ID: 324331
Sample Name:
Payment_Advice_pdf.exe
Cookbook: default.jbs
Time: 06:47:57
Date: 29/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

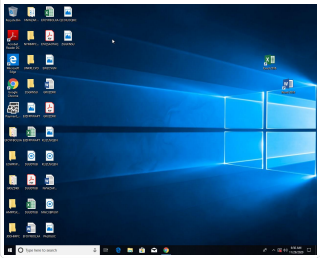
Analysis Report Payment_Advice_pdf.exe

Overview

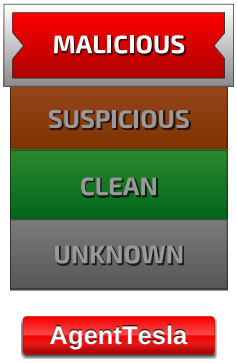
General Information

Sample Name:	Payment_Advice_pdf.exe
Analysis ID:	324331
MD5:	536cf4ed17eba1b.
SHA1:	72e062dd7a10d8..
SHA256:	c8ad1b5688fbbc3..
Tags:	Agenttesla exe

Most interesting Screenshot:



Detection

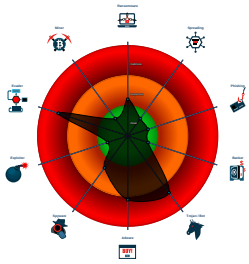


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- .NET source code contains very larg…
- Adds a directory exclusion to Windo…
- Connects to a pastebin service (like…
- Creates an undocumented autostart …
- Creates autostart registry keys with …
- Creates multiple autostart registry ke…
- Drops PE files to the startup folder
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Queries sensitive BIOS Information

Classification



Startup

- **System is w10x64**
- Payment_Advice_pdf.exe (PID: 4392 cmdline: 'C:\Users\user\Desktop\Payment_Advice_pdf.exe' MD5: 536CF4ED17EBA1BF41EF70FAAA2054A4)
  - timeout.exe (PID: 4488 cmdline: timeout 4 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
    - conhost.exe (PID: 4616 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6924 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Payment_Advice_pdf.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6932 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6948 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Payment_Advice_pdf.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 7016 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 7008 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Payment_Advice_pdf.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 7056 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 7104 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\Payment_Advice_pdf.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5792 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Payment_Advice_pdf.exe (PID: 6728 cmdline: C:\Users\user\Desktop\Payment_Advice_pdf.exe MD5: 536CF4ED17EBA1BF41EF70FAAA2054A4)
- Payment_Advice_pdf.exe (PID: 5600 cmdline: 'C:\Users\user\Desktop\Payment_Advice_pdf.exe' MD5: 536CF4ED17EBA1BF41EF70FAAA2054A4)
- Payment_Advice_pdf.exe (PID: 6944 cmdline: 'C:\Users\user\Desktop\Payment_Advice_pdf.exe' MD5: 536CF4ED17EBA1BF41EF70FAAA2054A4)
  - timeout.exe (PID: 4404 cmdline: timeout 4 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
    - conhost.exe (PID: 5772 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- Payment_Advice_pdf.exe (PID: 5360 cmdline: 'C:\Users\user\Desktop\Payment_Advice_pdf.exe' MD5: 536CF4ED17EBA1BF41EF70FAAA2054A4)
- Payment_Advice_pdf.exe (PID: 5916 cmdline: 'C:\Users\user\Desktop\Payment_Advice_pdf.exe' MD5: 536CF4ED17EBA1BF41EF70FAAA2054A4)
- Payment_Advice_pdf.exe (PID: 5536 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Payment_Advice_pdf.exe' MD5: 536CF4ED17EBA1BF41EF70FAAA2054A4)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000016.00000002.509306076.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000016.00000002.532140773.0000000002C41000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000016.00000002.532140773.0000000002C41000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Process Memory Space: Payment_Advice_pdf.exe PID: 6728	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: Payment_Advice_pdf.exe PID: 6728	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

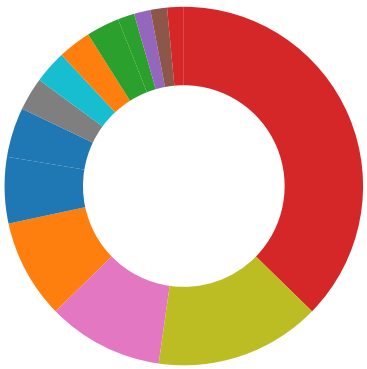
Unpacked PEs

Source	Rule	Description	Author	Strings
22.2.Payment_Advice_pdf.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

- AV Detection
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- 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

AV Detection:

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Networking:

Connects to a pastebin service (likely for C&C)

System Summary:

.NET source code contains very large strings

Initial sample is a PE file and has a suspicious name

Boot Survival:

- Creates an undocumented autostart registry key
- Creates autostart registry keys with suspicious names
- Creates multiple autostart registry keys
- Drops PE files to the startup folder

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)

HIPS / PFW / Operating System Protection Evasion:

- Adds a directory exclusion to Windows Defender
- Injects a PE file into a foreign processes

Stealing of Sensitive Information:

- Yara detected AgentTesla

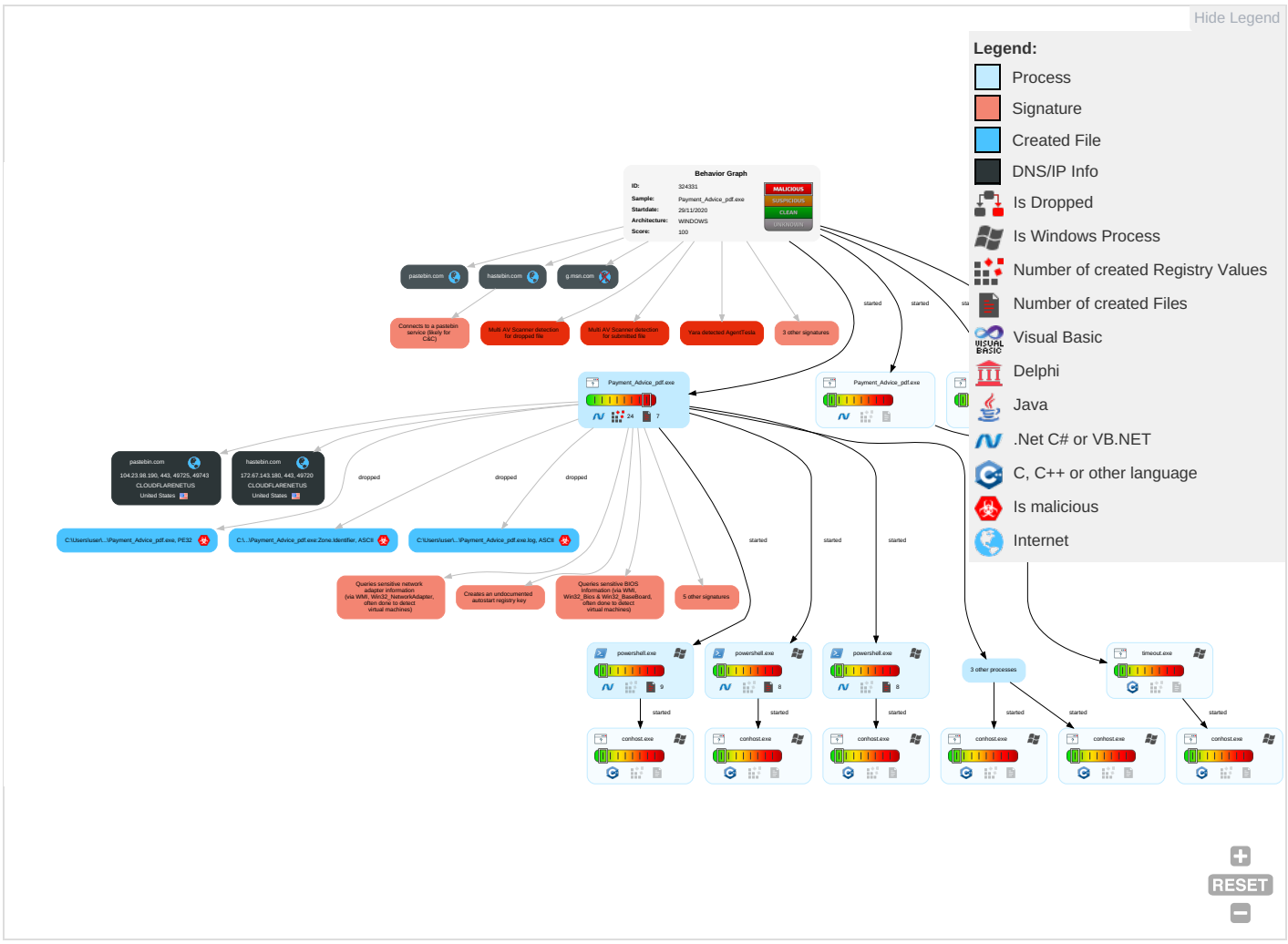
Remote Access Functionality:

- 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	Startup Items 1	Startup Items 1	Masquerading 1	Input Capture 1	Query Registry 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Web Service 1
Default Accounts	Scheduled Task/Job	Registry Run Keys / Startup Folder 4 2 1	Process Injection 1 1 2	Virtualization/Sandbox Evasion 1 4	LSASS Memory	Security Software Discovery 2 2 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Encrypted Channel 1 2
Domain Accounts	At (Linux)	Logon Script (Windows)	Registry Run Keys / Startup Folder 4 2 1	Disable or Modify Tools 1 1	Security Account Manager	Virtualization/Sandbox Evasion 1 4	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 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 Communicati
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	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 1 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protoc

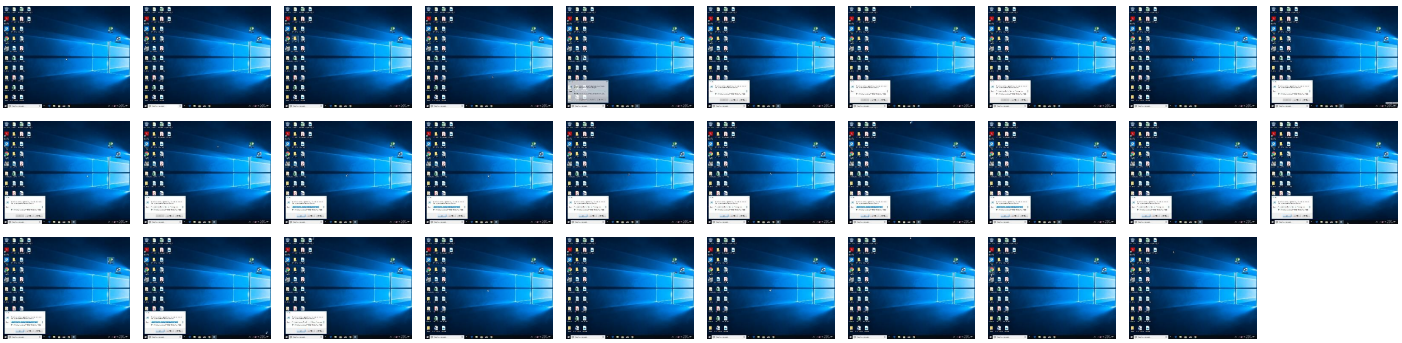
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Payment_Advice_pdf.exe	39%	Virustotal		Browse
Payment_Advice_pdf.exe	19%	Metadefender		Browse
Payment_Advice_pdf.exe	48%	ReversingLabs	ByteCode-MSIL.Trojan.Generic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Payment_Advice_pdf.exe	19%	Metadefender		Browse
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Payment_Advice_pdf.exe	48%	ReversingLabs	ByteCode-MSIL.Trojan.Generic	

Unpacked PE Files

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

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://ocsp.digp	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://hastebin.comD8	0%	Avira URL Cloud	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://www.digicert.co	0%	Virustotal		Browse
http://https://www.digicert.co	0%	Avira URL Cloud	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.pngTG	0%	Avira URL Cloud	safe	
http://oTJwpq.com	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
hastebin.com	172.67.143.180	true	false		high
pastebin.com	104.23.98.190	true	false		high
g.msn.com	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation

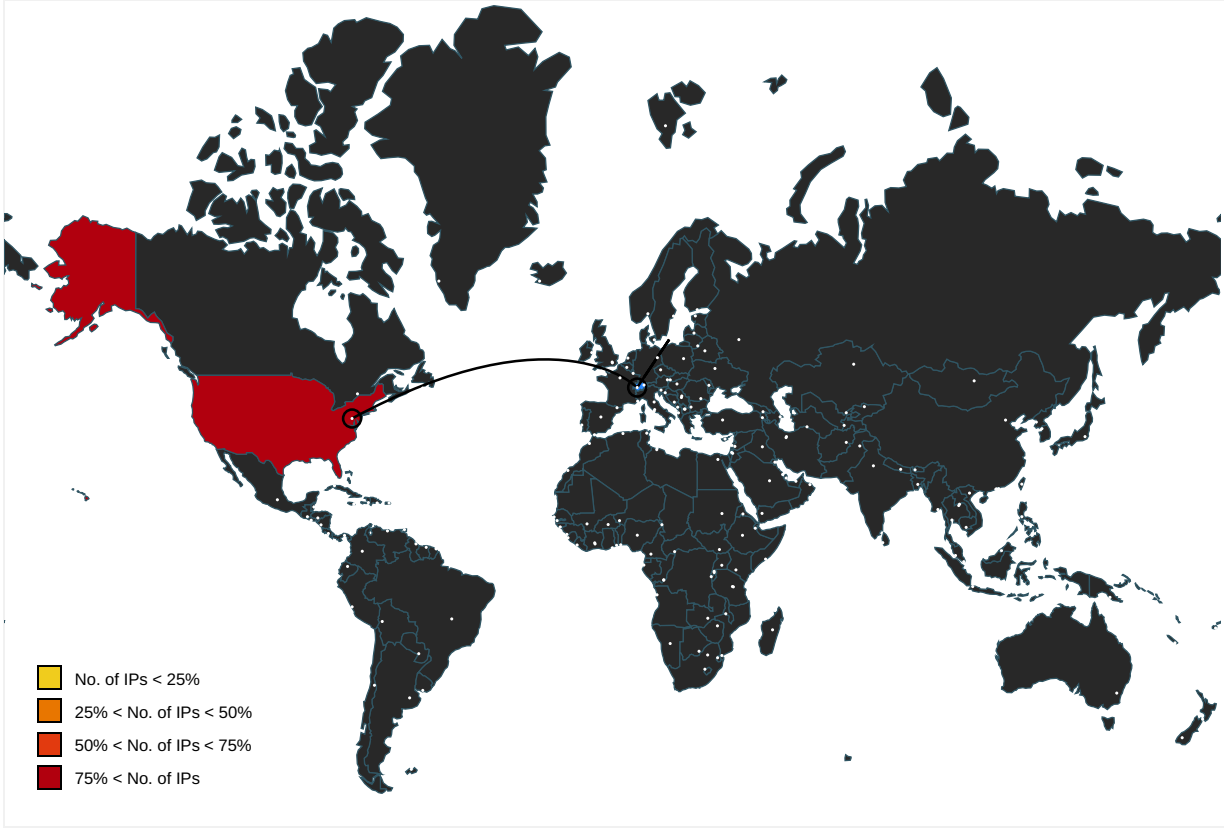
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://hastebin.com	Payment_Advice_pdf.exe, 000000 1B.00000002.532494643.00000000 028C1000.00000004.00000001.sdmp, Payment_Advice_pdf.exe, 000 0001C.00000002.532784461.00000 00003441000.00000004.00000001. sdmp, Payment_Advice_pdf.exe, 00000020.00000002.532690166.00 00000003051000.00000004.000000 01.sdmp	false		high
http://127.0.0.1:HTTP/1.1	Payment_Advice_pdf.exe, 000000 16.00000002.532140773.00000000 02C41000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://nuget.org/NuGet.exe	powershell.exe, 00000013.00000 002.601790285.0000000005BB5000 .00000004.00000001.sdmp	false		high
http://ocsp.digp	Payment_Advice_pdf.exe, 000000 00.00000003.309198205.00000000 011E9000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://DynDns.comDynDNS	Payment_Advice_pdf.exe, 000000 16.00000002.532140773.00000000 02C41000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://hastebin.com/raw/foqosepayu	Payment_Advice_pdf.exe, 000000 19.00000002.529670733.00000000 0324E000.00000004.00000001.sdmp, Payment_Advice_pdf.exe, 000 0001B.00000002.532494643.00000 000028C1000.00000004.00000001. sdmp, Payment_Advice_pdf.exe, 0000001C.00000002.532784461.00 00000003441000.00000004.000000 01.sdmp, Payment_Advice_pdf.exe, 00000020.00000002.532690166 .0000000003051000.00000004.000 00001.sdmp	false		high
http://https://hastebin.com/raw/noqadobanu	Payment_Advice_pdf.exe, 000000 19.00000002.529670733.00000000 0324E000.00000004.00000001.sdmp, Payment_Advice_pdf.exe, 000 0001B.00000002.532494643.00000 000028C1000.00000004.00000001. sdmp, Payment_Advice_pdf.exe, 0000001C.00000002.532784461.00 00000003441000.00000004.000000 01.sdmp, Payment_Advice_pdf.exe, 00000020.00000002.532690166 .0000000003051000.00000004.000 00001.sdmp	false		high
http://https://hastebin.com/raw/zegivutiko	Payment_Advice_pdf.exe, 000000 19.00000002.529670733.00000000 0324E000.00000004.00000001.sdmp, Payment_Advice_pdf.exe, 000 0001B.00000002.532494643.00000 000028C1000.00000004.00000001. sdmp, Payment_Advice_pdf.exe, 0000001C.00000002.532784461.00 00000003441000.00000004.000000 01.sdmp, Payment_Advice_pdf.exe, 00000020.00000002.532690166 .0000000003051000.00000004.000 00001.sdmp	false		high
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000013.00000 002.537783198.0000000004C8E000 .00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/soap/encoding/	powershell.exe, 0000000D.00000 002.535392577.000000000498D000 .00000004.00000001.sdmp, power shell.exe, 0000000F.00000002.5 35899338.0000000004BC1000.0000 0004.00000001.sdmp, powershell.exe, 00000013.00000002.537783198.000000 0004C8E000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://hastebin.com/raw/walodekari	Payment_Advice_pdf.exe, 00000019.00000002.529670733.00000000324E000.00000004.00000001.sdmp, Payment_Advice_pdf.exe, 00000001B.00000002.532494643.00000000028C1000.00000004.00000001.sdmp, Payment_Advice_pdf.exe, 0000001C.00000002.532784461.0000000003441000.00000004.00000001.sdmp, Payment_Advice_pdf.exe, 00000020.00000002.532690166.0000000003051000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	Payment_Advice_pdf.exe, 00000016.00000002.532140773.0000000002C41000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000013.00000002.537783198.0000000004C8E000.00000004.00000001.sdmp	false		high
http://https://hastebin.com/raw/yafimefexo	Payment_Advice_pdf.exe, 00000019.00000002.529670733.00000000324E000.00000004.00000001.sdmp, Payment_Advice_pdf.exe, 00000001B.00000002.532494643.00000000028C1000.00000004.00000001.sdmp, Payment_Advice_pdf.exe, 0000001C.00000002.532784461.0000000003441000.00000004.00000001.sdmp, Payment_Advice_pdf.exe, 00000020.00000002.532690166.0000000003051000.00000004.00000001.sdmp	false		high
http://https://contoso.com/License	powershell.exe, 00000013.00000002.601790285.0000000005BB5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://contoso.com/Icon	powershell.exe, 00000013.00000002.601790285.0000000005BB5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://hastebin.com/raw/onikuyajar	Payment_Advice_pdf.exe, 00000019.00000002.529670733.00000000324E000.00000004.00000001.sdmp, Payment_Advice_pdf.exe, 00000001B.00000002.532494643.00000000028C1000.00000004.00000001.sdmp, Payment_Advice_pdf.exe, 0000001C.00000002.532784461.0000000003441000.00000004.00000001.sdmp, Payment_Advice_pdf.exe, 00000020.00000002.532690166.0000000003051000.00000004.00000001.sdmp	false		high
http://https://hastebin.comD8	Payment_Advice_pdf.exe, 00000001B.00000002.536730759.0000000002A8C000.00000004.00000001.sdmp, Payment_Advice_pdf.exe, 0000001C.00000002.537590651.00000000036B9000.00000004.00000001.sdmp, Payment_Advice_pdf.exe, 00000020.00000002.533702642.00000000030C3000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://hastebin.com/raw/caqubavere	Payment_Advice_pdf.exe, 00000019.00000002.529670733.00000000324E000.00000004.00000001.sdmp, Payment_Advice_pdf.exe, 00000001B.00000002.532494643.00000000028C1000.00000004.00000001.sdmp, Payment_Advice_pdf.exe, 0000001C.00000002.532784461.0000000003441000.00000004.00000001.sdmp, Payment_Advice_pdf.exe, 00000020.00000002.532690166.0000000003051000.00000004.00000001.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 00000013.00000002.537783198.0000000004C8E000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://hastebin.com/raw/fufufevuxa	Payment_Advice_pdf.exe, 00000019.00000002.529670733.00000000324E000.00000004.00000001.sdmp, Payment_Advice_pdf.exe, 00000001B.00000002.532494643.00000000028C1000.00000004.00000001.sdmp, Payment_Advice_pdf.exe, 0000001C.00000002.532784461.00000000003441000.00000004.00000001.sdmp, Payment_Advice_pdf.exe, 00000020.00000002.532690166.0000000003051000.00000004.00000001.sdmp	false		high
http://https://hastebin.com/raw/saconikone	Payment_Advice_pdf.exe, 00000019.00000002.529670733.00000000324E000.00000004.00000001.sdmp, Payment_Advice_pdf.exe, 00000001B.00000002.532494643.00000000028C1000.00000004.00000001.sdmp, Payment_Advice_pdf.exe, 0000001C.00000002.532784461.00000000003441000.00000004.00000001.sdmp, Payment_Advice_pdf.exe, 00000020.00000002.532690166.0000000003051000.00000004.00000001.sdmp	false		high
http://https://api.ipify.orgGETMozilla/5.0	Payment_Advice_pdf.exe, 00000016.00000002.532140773.00000000002C41000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://hastebin.com/raw/asixarufey	Payment_Advice_pdf.exe, 00000019.00000002.529670733.00000000324E000.00000004.00000001.sdmp, Payment_Advice_pdf.exe, 00000001B.00000002.532494643.00000000028C1000.00000004.00000001.sdmp, Payment_Advice_pdf.exe, 0000001C.00000002.532784461.00000000003441000.00000004.00000001.sdmp, Payment_Advice_pdf.exe, 00000020.00000002.532690166.0000000003051000.00000004.00000001.sdmp	false		high
http://https://www.digicert.co	Payment_Advice_pdf.exe, 00000001B.00000002.527256543.00000000000C44000.00000004.00000020.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://api.telegram.org/bot%telegramapi%/	Payment_Advice_pdf.exe, 00000016.00000002.509306076.00000000000402000.00000040.00000001.sdmp	false		high
http://schemas.xmlsoap.org/wsdl/	powershell.exe, 0000000D.00000002.535392577.000000000498D000.00000004.00000001.sdmp, powershell.exe, 0000000F.00000002.535899338.0000000004BC1000.00000004.00000001.sdmp, powershell.exe, 00000013.00000002.537783198.0000000004C8E000.00000004.00000001.sdmp	false		high
http://https://contoso.com/	powershell.exe, 00000013.00000002.601790285.0000000005BB5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/Pester/PesterTG	powershell.exe, 0000000F.00000002.535899338.0000000004BC1000.00000004.00000001.sdmp	false		high
http://https://nuget.org/nuget.exe	powershell.exe, 00000013.00000002.601790285.0000000005BB5000.00000004.00000001.sdmp	false		high
http://pesterbdd.com/images/Pester.pngTG	powershell.exe, 0000000F.00000002.535899338.0000000004BC1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.htmlTG	powershell.exe, 0000000F.00000002.535899338.0000000004BC1000.00000004.00000001.sdmp	false		high
http://oTJwpq.com	Payment_Advice_pdf.exe, 00000016.00000002.532140773.00000000002C41000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 0000000D.00000002.532936323.0000000004761000.00000004.00000001.sdmp, powershell.exe, 0000000F.00000002.532691170.0000000004A81000.00000004.00000001.sdmp, powershell.exe, 00000010.00000002.585877442.0000000004761000.00000004.00000001.sdmp, powershell.exe, 00000013.00000002.535729267.0000000004B51000.00000004.00000001.sdmp, Payment_Advice_pdf.exe, 0000001B.00000002.532494643.00000000028C1000.00000004.00000001.sdmp, Payment_Advice_pdf.exe, 0000001C.00000002.532784461.000000000344100 0.00000004.00000001.sdmp, Payment_Advice_pdf.exe, 00000020.00000002.532690166.000000000305 1000.00000004.00000001.sdmp	false		high
http://https://api.telegram.org/bot%telegramapi%/sendDocumentdocument----------x	Payment_Advice_pdf.exe, 00000016.00000002.532140773.0000000002C41000.00000004.00000001.sdmp	false		high
http://https://hastebin.com/raw/oqigugirew	Payment_Advice_pdf.exe, 00000019.00000002.529670733.000000000324E000.00000004.00000001.sdmp, Payment_Advice_pdf.exe, 0000001B.00000002.532494643.00000000028C1000.00000004.00000001.sdmp, Payment_Advice_pdf.exe, 0000001C.00000002.532784461.000000003441000.00000004.00000001.sdmp, Payment_Advice_pdf.exe, 00000020.00000002.532690166.0000000003051000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	Payment_Advice_pdf.exe, 00000016.00000002.509306076.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://hastebin.com/raw/yimijojino	Payment_Advice_pdf.exe, 00000019.00000002.529670733.000000000324E000.00000004.00000001.sdmp, Payment_Advice_pdf.exe, 0000001B.00000002.532494643.00000000028C1000.00000004.00000001.sdmp, Payment_Advice_pdf.exe, 0000001C.00000002.532784461.000000003441000.00000004.00000001.sdmp, Payment_Advice_pdf.exe, 00000020.00000002.532690166.0000000003051000.00000004.00000001.sdmp	false		high
http://https://hastebin.com/raw/userirulod	Payment_Advice_pdf.exe, 00000019.00000002.529670733.000000000324E000.00000004.00000001.sdmp, Payment_Advice_pdf.exe, 0000001B.00000002.532494643.00000000028C1000.00000004.00000001.sdmp, Payment_Advice_pdf.exe, 0000001C.00000002.532784461.000000003441000.00000004.00000001.sdmp, Payment_Advice_pdf.exe, 00000020.00000002.532690166.0000000003051000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.23.98.190	unknown	United States		13335	CLOUDFLARENETUS	false
172.67.143.180	unknown	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	324331
Start date:	29.11.2020
Start time:	06:47:57
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Payment_Advice_pdf.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	37
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.adwa.evad.winEXE@26/15@13/2

EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.6% (good quality ratio 0.6%) • Quality average: 93.8% • Quality standard deviation: 7.8%
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 168.61.161.212, 104.43.193.48, 2.20.84.85, 51.11.168.160, 20.54.26.129, 51.103.5.159, 52.142.114.176, 92.122.213.194, 92.122.213.247, 51.104.144.132, 52.155.217.156 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, arc.msn.com.nsatc.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, wns.notify.windows.com.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, g-msn-com-nsatc.trafficmanager.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, par02p.wns.notify.windows.com.akadns.net, emea1.notify.windows.com.akadns.net, blobcollector.events.data.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
06:49:35	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run <Unknown> C:\Users\user\Desktop\Payment_Advice_pdf.exe
06:49:40	API Interceptor	17x Sleep call for process: Payment_Advice_pdf.exe modified
06:49:44	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Payment_Advice_pdf.exe C:\Users\user\Desktop\Payment_Advice_pdf.exe
06:49:53	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run <Unknown> C:\Users\user\Desktop\Payment_Advice_pdf.exe
06:50:02	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Payment_Advice_pdf.exe C:\Users\user\Desktop\Payment_Advice_pdf.exe
06:50:11	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Payment_Advice_pdf.exe
06:50:51	API Interceptor	25x Sleep call for process: powershell.exe modified
06:51:10	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run newapp C:\Users\user\AppData\Roaming\newapp\newapp.exe
06:51:19	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run newapp C:\Users\user\AppData\Roaming\newapp\newapp.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.23.98.190	b095b966805abb7df4ffddf183def880.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	E1Q0TjeN32.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	6YCl3ATKJw.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	Hjnb15Nuc3.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	JDgYMW0LHW.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	4av8Sn32by.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	5T4Ykc0VSK.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	afvhKak0Ir.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	T6OcyQsUsY.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	1KITgJnGbI.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	PxwWcmbMC5.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	XnAJZR4NcN.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	PbTwrajNMX.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	22NO7gVJ7r.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	rE7DwszvrX.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	VjPHSJkwr6.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	wf86K0dpOP.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	VrR9J0FnSG.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	6C1MYmrVl1.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
	aTZQZVVriQ.exe	Get hash	malicious	Browse	• pastebin.com/raw/XMKKNkb0
172.67.143.180	OVERDUE INVOICE.xls	Get hash	malicious	Browse	
	Purchase Order.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Mal.Generic-S.26042.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Siggen11.48004.19433.exe	Get hash	malicious	Browse	
	CSq58hA6nO.exe	Get hash	malicious	Browse	
	Order Catalogue Specifications.xlsx	Get hash	malicious	Browse	
	IFEvMPuK1t.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO91666. pdf.exe	Get hash	malicious	Browse	
	8DHgG635TK.exe	Get hash	malicious	Browse	
	NdAonNMuzm.exe	Get hash	malicious	Browse	
	9fv6IffZmA.exe	Get hash	malicious	Browse	
	plvSd6AoLp.exe	Get hash	malicious	Browse	
	w6r8DJTtvF.exe	Get hash	malicious	Browse	
	B67aSzPX6F.exe	Get hash	malicious	Browse	
	3230_pdf.exe	Get hash	malicious	Browse	
	P.O pdf pdf pdf pdf pdf ori40 ony.exe	Get hash	malicious	Browse	
	Shipping Details_PDF.exe	Get hash	malicious	Browse	
	#INVBEBON095834.pdf.exe	Get hash	malicious	Browse	
	#INVBEBON095835.pdf.exe	Get hash	malicious	Browse	
	xE08uG0aqO.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
pastebin.com	BWPh61ydQN.exe	Get hash	malicious	Browse	• 104.23.99.190
	fAhW3JEGaZ.exe	Get hash	malicious	Browse	• 104.23.99.190
	HIp08HPg20.exe	Get hash	malicious	Browse	• 104.23.98.190
	OVERDUE INVOICE.xls	Get hash	malicious	Browse	• 104.23.98.190
	Venom.exe	Get hash	malicious	Browse	• 104.23.99.190
	PO348578.jar	Get hash	malicious	Browse	• 104.23.99.190
	Purchase Order.exe	Get hash	malicious	Browse	• 104.23.98.190
	SecuriteInfo.com.Trojan.Siggen11.49316.15393.exe	Get hash	malicious	Browse	• 104.23.98.190
	SecuriteInfo.com.Trojan.Nanocore.23.20965.exe	Get hash	malicious	Browse	• 104.23.98.190
	SecuriteInfo.com.Mal.Generic-S.26042.exe	Get hash	malicious	Browse	• 104.23.98.190
	SecuriteInfo.com.BehavesLike.Win32.VirRansom.rm.exe	Get hash	malicious	Browse	• 104.23.99.190
	SecuriteInfo.com.Trojan.KillProc2.14740.25300.exe	Get hash	malicious	Browse	• 104.23.99.190
	due-invoice.xlsm	Get hash	malicious	Browse	• 104.23.98.190
	Order 51897.exe	Get hash	malicious	Browse	• 104.23.99.190
	Statement Of Account.exe	Get hash	malicious	Browse	• 104.23.98.190
	http://ancien-site-joomla.fr/build2.exe	Get hash	malicious	Browse	• 104.23.98.190
	BTNCRKWd.exe	Get hash	malicious	Browse	• 104.23.98.190
	Shipment Details.exe	Get hash	malicious	Browse	• 104.23.98.190
	7iZX0KCH4C.exe	Get hash	malicious	Browse	• 104.23.98.190
	IFEvMPuK1t.exe	Get hash	malicious	Browse	• 104.23.98.190
hastebin.com	OVERDUE INVOICE.xls	Get hash	malicious	Browse	• 172.67.143.180
	Venom.exe	Get hash	malicious	Browse	• 104.24.127.89
	Purchase Order.exe	Get hash	malicious	Browse	• 172.67.143.180
	SecuriteInfo.com.Mal.Generic-S.26042.exe	Get hash	malicious	Browse	• 104.24.126.89
	due-invoice.xlsm	Get hash	malicious	Browse	• 104.24.127.89
	SecuriteInfo.com.Gen.NN.ZemsilF.34658.m0@a8V1yrei.exe	Get hash	malicious	Browse	• 104.24.126.89
	Order 51897.exe	Get hash	malicious	Browse	• 104.24.127.89
	AsyncClient.exe	Get hash	malicious	Browse	• 104.24.126.89
	Statement Of Account.exe	Get hash	malicious	Browse	• 104.24.127.89
	http://ancien-site-joomla.fr/build2.exe	Get hash	malicious	Browse	• 104.24.126.89
	SecuriteInfo.com.ArtemisTrojan.exe	Get hash	malicious	Browse	• 104.24.126.89
	SecuriteInfo.com.BackDoor.SpyBotNET.25.30157.exe	Get hash	malicious	Browse	• 104.24.127.89
	C03N224Hbu.exe	Get hash	malicious	Browse	• 104.24.126.89
	P.O_ 39134.xlsx	Get hash	malicious	Browse	• 104.24.127.89
	EME.39134.xlsx	Get hash	malicious	Browse	• 104.24.127.89
	SecuriteInfo.com.Trojan.Siggen11.48004.19433.exe	Get hash	malicious	Browse	• 172.67.143.180
	Order List.xlsx	Get hash	malicious	Browse	• 104.24.127.89
	CSq58hA6nO.exe	Get hash	malicious	Browse	• 172.67.143.180
	Order Catalogue Specifications.xlsx	Get hash	malicious	Browse	• 172.67.143.180
	Shipping Details_PDF.exe	Get hash	malicious	Browse	• 104.24.127.89

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	case4092.xls	Get hash	malicious	Browse	• 104.31.86.113
	case4092.xls	Get hash	malicious	Browse	• 104.31.86.113
	SecuriteInfo.com.Exploit.Siggen3.2597.23127.xls	Get hash	malicious	Browse	• 172.67.212.16

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Exploit.Siggen3.2597.23127.xls	Get hash	malicious	Browse	• 172.67.212.16
	Quote.exe	Get hash	malicious	Browse	• 172.67.188.154
	DWG AND PO SPECIFICATION.xls	Get hash	malicious	Browse	• 104.20.138.65
	DWG AND PO SPECIFICATION.xls	Get hash	malicious	Browse	• 104.20.139.65
	egGgMixHNS.exe	Get hash	malicious	Browse	• 172.67.219.32
	BWPh61ydQN.exe	Get hash	malicious	Browse	• 162.159.135.233
	DWG AND PO SPECIFICATION.xls	Get hash	malicious	Browse	• 104.20.138.65
	egGgMixHNS.exe	Get hash	malicious	Browse	• 104.24.123.22
	5KYnVcv9cf.exe	Get hash	malicious	Browse	• 104.24.123.22
	5KYnVcv9cf.exe	Get hash	malicious	Browse	• 104.24.122.22
	DHL invoice VNYI564714692.exe	Get hash	malicious	Browse	• 162.159.135.232
	Order-Poland.exe	Get hash	malicious	Browse	• 162.159.134.233
	Novi poredak.exe	Get hash	malicious	Browse	• 162.159.135.233
	Customer Remittance Advice 9876627262822662.exe	Get hash	malicious	Browse	• 162.159.134.233
	94039330.exe	Get hash	malicious	Browse	• 162.159.134.233
	P1001094.EXE	Get hash	malicious	Browse	• 162.159.134.233
	ompbSaRiK0.exe	Get hash	malicious	Browse	• 104.18.53.239
CLOUDFLARENETUS	case4092.xls	Get hash	malicious	Browse	• 104.31.86.113
	case4092.xls	Get hash	malicious	Browse	• 104.31.86.113
	SecuriteInfo.com.Exploit.Siggen3.2597.23127.xls	Get hash	malicious	Browse	• 172.67.212.16
	SecuriteInfo.com.Exploit.Siggen3.2597.23127.xls	Get hash	malicious	Browse	• 172.67.212.16
	Quote.exe	Get hash	malicious	Browse	• 172.67.188.154
	DWG AND PO SPECIFICATION.xls	Get hash	malicious	Browse	• 104.20.138.65
	DWG AND PO SPECIFICATION.xls	Get hash	malicious	Browse	• 104.20.139.65
	egGgMixHNS.exe	Get hash	malicious	Browse	• 172.67.219.32
	BWPh61ydQN.exe	Get hash	malicious	Browse	• 162.159.135.233
	DWG AND PO SPECIFICATION.xls	Get hash	malicious	Browse	• 104.20.138.65
	egGgMixHNS.exe	Get hash	malicious	Browse	• 104.24.123.22
	5KYnVcv9cf.exe	Get hash	malicious	Browse	• 104.24.123.22
	5KYnVcv9cf.exe	Get hash	malicious	Browse	• 104.24.122.22
	DHL invoice VNYI564714692.exe	Get hash	malicious	Browse	• 162.159.135.232
	Order-Poland.exe	Get hash	malicious	Browse	• 162.159.134.233
	Novi poredak.exe	Get hash	malicious	Browse	• 162.159.135.233
	Customer Remittance Advice 9876627262822662.exe	Get hash	malicious	Browse	• 162.159.134.233
	94039330.exe	Get hash	malicious	Browse	• 162.159.134.233
	P1001094.EXE	Get hash	malicious	Browse	• 162.159.134.233
	ompbSaRiK0.exe	Get hash	malicious	Browse	• 104.18.53.239

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
3b5074b1b5d032e5620f69f9f700ff0e	ompbSaRiK0.exe	Get hash	malicious	Browse	• 104.23.98.190 • 172.67.143.180
	XcOxlmOz4D.exe	Get hash	malicious	Browse	• 104.23.98.190 • 172.67.143.180
	Venom.exe	Get hash	malicious	Browse	• 104.23.98.190 • 172.67.143.180
	module.exe	Get hash	malicious	Browse	• 104.23.98.190 • 172.67.143.180
	SecuriteInfo.com.Trojan.MulDrop15.61980.13868.exe	Get hash	malicious	Browse	• 104.23.98.190 • 172.67.143.180
	SecuriteInfo.com.Trojan.PWS.Stealer.29618.24275.exe	Get hash	malicious	Browse	• 104.23.98.190 • 172.67.143.180
	Purchase Order.exe	Get hash	malicious	Browse	• 104.23.98.190 • 172.67.143.180

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Trojan.MulDrop15.61981.23282.exe	Get hash	malicious	Browse	• 104.23.98.190 • 172.67.143.180
	ORDER.exe	Get hash	malicious	Browse	• 104.23.98.190 • 172.67.143.180
	Mixtec New Order And Price List Requsting Form_pdf.exe	Get hash	malicious	Browse	• 104.23.98.190 • 172.67.143.180
	swift copy.exe	Get hash	malicious	Browse	• 104.23.98.190 • 172.67.143.180
	26-11-20_Dhl_Signed_document-pdf.exe	Get hash	malicious	Browse	• 104.23.98.190 • 172.67.143.180
	Arrivalnotice2020pdf.exe	Get hash	malicious	Browse	• 104.23.98.190 • 172.67.143.180
	SecuriteInfo.com.Mal.Generic-S.26042.exe	Get hash	malicious	Browse	• 104.23.98.190 • 172.67.143.180
	guy1.exe	Get hash	malicious	Browse	• 104.23.98.190 • 172.67.143.180
	guy2.exe	Get hash	malicious	Browse	• 104.23.98.190 • 172.67.143.180
	Exodus.exe	Get hash	malicious	Browse	• 104.23.98.190 • 172.67.143.180
	INV-6367-20_pdf.exe	Get hash	malicious	Browse	• 104.23.98.190 • 172.67.143.180
	#A06578987.xlsm	Get hash	malicious	Browse	• 104.23.98.190 • 172.67.143.180
	Order 51897.exe	Get hash	malicious	Browse	• 104.23.98.190 • 172.67.143.180

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Payment_Advice_pdf.exe.log	
Process:	C:\Users\user\Desktop\Payment_Advice_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLU84qpE4Ks2wKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7GE4Kx1qE4KE4j:Mgv2HKXwYHKhQnoPtHoxHhAHKzvGHKxx
MD5:	6601BE2C4834904CD917BA61AE5C10E2
SHA1:	2AB6A81BFA9DC031F5D2538AB94FC99074AD5241
SHA-256:	85212C0C71D214CD899B0E3FDD41A1D149E44FEFA5DD42B419B2299BC6FCC34F
SHA-512:	2F825EC08F2A34A6540F862EDD948E5674D66C94E371C9EF3CDA0AA657E0A8EB8F6260A9EE7A582A1EC30C16CC8094ECC60F3406D2904A9AA0B38918205C5E 6
Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutra

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_24fphy4r.0gs.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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_24fphy4r.0gs.ps1	
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_52egkfrp.jkl.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_bppwvxmq.v5t.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_clsntrj5.a1a.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_fwsc2twm.abg.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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_fwsc2twm.abg.ps1	
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_lv3izpro.emd.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_mmdcdr4n.tid.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_vxulzjog.0pn.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\Microsoft\Windows\Start Menu\Programs\Startup\Payment_Advice_pdf.exe	
Process:	C:\Users\user\Desktop\Payment_Advice_pdf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	631776
Entropy (8bit):	5.351954264003962
Encrypted:	false
SSDEEP:	6144:9ktH7smB3jEe4PPDRQLv6DPc/cYeYUzz/OBOf7242COfS:mson4PL4vezOBOD242C0S
MD5:	536CF4ED17EBA1BF41EF70FAAA2054A4

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Payment_Advice_pdf.exe	
SHA1:	72E062DD7A10D8B9E66732D5037C5156A9741D30
SHA-256:	C8AD1B5688FBBC359EE4256D3C7FBCA2D09BDD4968000DC8FFB86BB9964AC213
SHA-512:	67BF10D1EA495B97EF8DB595BE0A1E363E2FF4B1E2EB6B55048C8AFDAF95CCC6AF443AE55070EDF22E1B0964B08099ABBE20E52301061B48C041240FD47471E
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 19%, Browse • Antivirus: ReversingLabs, Detection: 48%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....N.^.....''...0..... .....@.. .....K.. ..`.....O..... ..... ..H.....text..... ..... ..`.rsrc.....@..@.reloc..... .....@..B.....H.....(...d.....P .....*. ...*.. ...90...(....9.....r...p....(....(....*.....(....*....*..(....*.0.....D....U.... ....(.....#.....(....& ....(.....#.....(....& ....(.....#.....(....& ....(..... ....(.....#.....(....& ....(.....#.....(....&

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Payment_Advice_pdf.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Payment_Advice_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20201129\PowerShell_transcript.103386.JJDrYbN8.20201129064938.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):	690
Entropy (8bit):	5.374884313341398
Encrypted:	false
SSDEEP:	12:57DtSA6N4xYiTH3fBTj5oy/x2DOzzUjjIneSuVReTA64WoVPw6jewGxMKjX4CIyv:BxSAMiDvBBt/x2DOXUWeSuVReM64W8Hy
MD5:	EF7B79CA905D042D66413FBDCF5DCDBF
SHA1:	66857605BB4F8B535CD14C9EF58356B7A64B40BA
SHA-256:	EA4E25DF8980DECDD46A1F43C64433A52C9F28ECFF87491622F9446F5B788600
SHA-512:	7BC7AA96989DB17BF3255F72BBE074F552FCD6082892C6BD18B87A197353671A88261936716FEA777E1F9FF7D40684102B40609C26016995BEB8301B627FC0A5
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20201129065027..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 103386 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\Payment_Advice_pdf.exe -Force..Process ID: 7104..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..**********..

C:\Users\user\Documents\20201129\PowerShell_transcript.103386.VthBuP45.20201129064936.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):	744
Entropy (8bit):	5.386572842518841
Encrypted:	false
SSDEEP:	12:57DtSA6N4xXTH3fBTj5oy/x2DOzzUjjIneSuSHSuVM1t2X9TA64WoEPw6jewGxMy:BxSADDvBBt/x2DOXUWeSuvuVMyM64WNS
MD5:	B61E1B38F5A52C9C70308B3313727171
SHA1:	70CEA769F553FD5D183CC384D8BA35DBC02CFE2A
SHA-256:	3B342B75D223229FD4C12ED07611CC69C177CFD7452BAE9C28E860052EBB42BD
SHA-512:	985CA19BA3318E267D0F5CC823195A836B0FC60053345EDCB5C89DB3B293EA17874D88438A119D732B3692300DDC346D2B144FFD8D800ED2104DF1B0F1A73D0
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20201129065032..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 103386 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Payment_Advice_pdf.exe -Force..Process ID: 7008..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..**********..

C:\Users\user\Documents\20201129\PowerShell_transcript.103386.loZpncW0.20201129064934.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):	972
Entropy (8bit):	5.340417633985651
Encrypted:	false
SSDEEP:	24:BxSAO1DvBBt/x2DOXUWeSuvuVMyM64WEUHjeTKKjX4CIym1ZJXPuvuVMyM6k:BZCv/toO+SsuJblqDYB1ZNsuJk
MD5:	F15BE5A6925D17D92F9A119AA38CA51F
SHA1:	2608202B911882C6088D93169D4F1FA10E037FB1
SHA-256:	ADAC5C16AF66849262785A58D4A99C9EA9FEAADE4091A489CCCA041A1D2128BD
SHA-512:	90536976CCFC4E2B27F2FA1F60C44CA07007050F7273FC0F7DF73991A72245D909E89923482E876584EACA92B243BD4C397A5186FDA23404A9234131B97ACCD8
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20201129065013..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 103386 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Payment_Advice_pdf.exe -Force..Process ID: 6924..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: 20201129065014..********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Payment_Advice_pdf.exe -Force..

C:\Users\user\Documents\20201129\PowerShell_transcript.103386.z_ziTDYA.20201129064937.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):	744
Entropy (8bit):	5.3922837398219405
Encrypted:	false
SSDEEP:	12:57DtSA6N4xiTH3fBTj5oy/x2DOzzUjjIneSuSHSuVM1t2X9TA64WofyPw6jewGx9:BxSAODvBBt/x2DOXUWeSuvuVMyM64WaD
MD5:	FDFA077639A382123DC963D7DB1589C0
SHA1:	D98CDEAA8B6FC7243E40D80D52F53C995BF0B413
SHA-256:	2FE16B41DBFEBD40DF624B046CBBFEB051F98EF96998FDBF7F8797F31FB55CD3
SHA-512:	DBE91F7DA2DF097E0B5CF6F5192C7A1A4B5A1AF2FC0DE357F47A16F64A197DB8703D43EE0A567B863E0554DE6090D722F2B59F5CE339063711A2E29BA50F5A35
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20201129065031..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 103386 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Payment_Advice_pdf.exe -Force..Process ID: 6948..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..**********..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.351954264003962
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.98% • Win32 Executable (generic) a (10002005/4) 49.93% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	Payment_Advice_pdf.exe
File size:	631776
MD5:	536cf4ed17eba1bf41ef70faaa2054a4
SHA1:	72e062dd7a10d8b9e66732d5037c5156a9741d30
SHA256:	c8ad1b5688fbbc359ee4256d3c7fbca2d09bdd4968000dc8ffb86bb9964ac213
SHA512:	67bf10d1ea495b97ef8db595be0a1e363e2ff4b1e2eb6b55048c8afdaf95ccc6af443ae55070edf22e1b0964b08099abbe20e52301061b48c041240fd47471ee
SSDEEP:	6144:9ktH7smB3jEe4PPDRQLv6DPc/cYeYUzz/OBOf7242COfS:mson4PL4vezOBOD242C0S

General

File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....N.^.....".0..... .....@.. .....K.... `.....

File Icon

Icon Hash:	5414746b4a511de8

Static PE Info

General

Entrypoint:	0x48d2de
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT, HIGH_ENTROPY_VA
Time Stamp:	0x5EA34EB2 [Fri Apr 24 20:40:18 2020 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=US, L=New York, OU=Beebbecbbffabffdbbffedcdeecdb, O=Fadddee, CN=Eddcbdabcadbaebb
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	• 11/26/2020 2:31:29 PM 11/26/2021 2:31:29 PM
Subject Chain	• C=US, L=New York, OU=Beebbecbbffabffdbbffedcdeecdb, O=Fadddee, CN=Eddcbdabcadbaebb
Version:	3
Thumbprint MD5:	DEFA3690708D3682B3E4D95E30B1BDE9
Thumbprint SHA-1:	78B16D9ABE3F03A2D7907298352F0447D308BA24
Thumbprint SHA-256:	1CF24A216D49C60783F64E313500C987149D11738D40B8EC45F2E3E20914B0EF
Serial:	009CB9CAA3873FF2621FE2496AE8C17F7F

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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8d28c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x8e000	0xd7d8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x99000	0x13e0	.rsrc
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	0x8b2e4	0x8b400	False	0.177788725875	data	5.16846171058	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x8e000	0xd7d8	0xd800	False	0.240993923611	data	4.46718133319	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_ICON	0x8e370	0x9a4	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x8ed14	0x668	data	English	United States
RT_ICON	0x8f37c	0x2e8	dBase IV DBT of @.DBF, block length 512, next free block index 40, next free block 2004318071, next used block 4286054399	English	United States
RT_ICON	0x8f664	0x128	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x8f78c	0xed9	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x90668	0xea8	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_ICON	0x91510	0x8a8	dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x91db8	0x568	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x92320	0xee9	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x9320c	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 64767, next used block 0	English	United States
RT_ICON	0x97434	0x25a8	data	English	United States
RT_ICON	0x999dc	0x10a8	data	English	United States
RT_ICON	0x9aa84	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_GROUP_ICON	0x9aeec	0xbc	data	English	United States
RT_VERSION	0x9afa8	0x440	data	English	United States
RT_MANIFEST	0x9b3e8	0x3ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators	English	United States

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Assembly Version	16.0.0.0
LegalCopyright	Microsoft Corporation. All rights reserved.
InternalName	witadmin.exe
FileVersion	16.166.30024.1 built by: releases/dev16/16.6-preview5 (77caed4305)
CompanyName	Microsoft Corporation
Comments	6b2f20d4
ProductName	Microsoft Visual Studio Azure DevOps Server
ProductVersion	16.166.30024.1
FileDescription	witadmin.exe
OriginalFilename	witadmin.exe
Translation	0x0409 0x04b0

Possible Origin

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

Network Behavior

Network Port Distribution

Total Packets: 53

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 06:49:06.858720064 CET	49720	443	192.168.2.5	172.67.143.180
Nov 29, 2020 06:49:06.885519028 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:06.885683060 CET	49720	443	192.168.2.5	172.67.143.180
Nov 29, 2020 06:49:06.922310114 CET	49720	443	192.168.2.5	172.67.143.180
Nov 29, 2020 06:49:06.948971033 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:06.951082945 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:06.951127052 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:06.951248884 CET	49720	443	192.168.2.5	172.67.143.180
Nov 29, 2020 06:49:06.963032961 CET	49720	443	192.168.2.5	172.67.143.180
Nov 29, 2020 06:49:06.989978075 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:06.990125895 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.036216974 CET	49720	443	192.168.2.5	172.67.143.180
Nov 29, 2020 06:49:07.066555977 CET	49720	443	192.168.2.5	172.67.143.180
Nov 29, 2020 06:49:07.093046904 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.265099049 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.265120983 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.265131950 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.265144110 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.265152931 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.265167952 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.265183926 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.265196085 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.265211105 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.265225887 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.265237093 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.265252113 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.265270948 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.265286922 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.265297890 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.265310049 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.265345097 CET	49720	443	192.168.2.5	172.67.143.180
Nov 29, 2020 06:49:07.265405893 CET	49720	443	192.168.2.5	172.67.143.180
Nov 29, 2020 06:49:07.338573933 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.338589907 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.338603020 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.338627100 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.338630915 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.338634968 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.338650942 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.338661909 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.338670969 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.338748932 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.338773966 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.338777065 CET	49720	443	192.168.2.5	172.67.143.180
Nov 29, 2020 06:49:07.338792086 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.338809013 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.338824034 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.338866949 CET	49720	443	192.168.2.5	172.67.143.180
Nov 29, 2020 06:49:07.338916063 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.338936090 CET	49720	443	192.168.2.5	172.67.143.180
Nov 29, 2020 06:49:07.338963985 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.338979959 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.338996887 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.339011908 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.339031935 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.339032888 CET	49720	443	192.168.2.5	172.67.143.180
Nov 29, 2020 06:49:07.339046001 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.339092970 CET	49720	443	192.168.2.5	172.67.143.180
Nov 29, 2020 06:49:07.339143991 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.339160919 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.339175940 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.339191914 CET	443	49720	172.67.143.180	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 06:49:07.339211941 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.339212894 CET	49720	443	192.168.2.5	172.67.143.180
Nov 29, 2020 06:49:07.339270115 CET	49720	443	192.168.2.5	172.67.143.180
Nov 29, 2020 06:49:07.339318037 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.339370966 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.339386940 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.339421988 CET	49720	443	192.168.2.5	172.67.143.180
Nov 29, 2020 06:49:07.380106926 CET	49720	443	192.168.2.5	172.67.143.180
Nov 29, 2020 06:49:07.412678003 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.412694931 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.412707090 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.412719011 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.412727118 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.412739038 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.412746906 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.412758112 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.412775993 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.412791014 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.412802935 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.412863016 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.412879944 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.412894964 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.412905931 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.412951946 CET	49720	443	192.168.2.5	172.67.143.180
Nov 29, 2020 06:49:07.413042068 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.413073063 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.413105965 CET	49720	443	192.168.2.5	172.67.143.180
Nov 29, 2020 06:49:07.413110971 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.413155079 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.413162947 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.413165092 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.413172007 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.413180113 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.413197041 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.413197041 CET	49720	443	192.168.2.5	172.67.143.180
Nov 29, 2020 06:49:07.413213968 CET	443	49720	172.67.143.180	192.168.2.5
Nov 29, 2020 06:49:07.413275957 CET	49720	443	192.168.2.5	172.67.143.180
Nov 29, 2020 06:49:07.413336039 CET	443	49720	172.67.143.180	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 06:48:49.592431068 CET	54757	53	192.168.2.5	8.8.8.8
Nov 29, 2020 06:48:49.619355917 CET	53	54757	8.8.8.8	192.168.2.5
Nov 29, 2020 06:48:50.452881098 CET	49992	53	192.168.2.5	8.8.8.8
Nov 29, 2020 06:48:50.479872942 CET	53	49992	8.8.8.8	192.168.2.5
Nov 29, 2020 06:48:52.347913980 CET	60075	53	192.168.2.5	8.8.8.8
Nov 29, 2020 06:48:52.383404016 CET	53	60075	8.8.8.8	192.168.2.5
Nov 29, 2020 06:49:06.794851065 CET	55016	53	192.168.2.5	8.8.8.8
Nov 29, 2020 06:49:06.833525896 CET	53	55016	8.8.8.8	192.168.2.5
Nov 29, 2020 06:49:07.933543921 CET	64345	53	192.168.2.5	8.8.8.8
Nov 29, 2020 06:49:07.972069979 CET	53	64345	8.8.8.8	192.168.2.5
Nov 29, 2020 06:49:14.015892982 CET	57128	53	192.168.2.5	8.8.8.8
Nov 29, 2020 06:49:15.006133080 CET	57128	53	192.168.2.5	8.8.8.8
Nov 29, 2020 06:49:16.072524071 CET	57128	53	192.168.2.5	8.8.8.8
Nov 29, 2020 06:49:16.099591017 CET	53	57128	8.8.8.8	192.168.2.5
Nov 29, 2020 06:49:31.701009989 CET	54791	53	192.168.2.5	8.8.8.8
Nov 29, 2020 06:49:31.744827032 CET	53	54791	8.8.8.8	192.168.2.5
Nov 29, 2020 06:49:36.824596882 CET	50463	53	192.168.2.5	8.8.8.8
Nov 29, 2020 06:49:36.860050917 CET	53	50463	8.8.8.8	192.168.2.5
Nov 29, 2020 06:49:38.577140093 CET	50394	53	192.168.2.5	8.8.8.8
Nov 29, 2020 06:49:38.615976095 CET	53	50394	8.8.8.8	192.168.2.5
Nov 29, 2020 06:49:42.247489929 CET	58530	53	192.168.2.5	8.8.8.8
Nov 29, 2020 06:49:42.274691105 CET	53	58530	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 06:49:50.300962925 CET	53813	53	192.168.2.5	8.8.8.8
Nov 29, 2020 06:49:50.351768017 CET	53	53813	8.8.8.8	192.168.2.5
Nov 29, 2020 06:50:01.251828909 CET	63732	53	192.168.2.5	8.8.8.8
Nov 29, 2020 06:50:01.289098024 CET	53	63732	8.8.8.8	192.168.2.5
Nov 29, 2020 06:50:25.678795099 CET	57344	53	192.168.2.5	8.8.8.8
Nov 29, 2020 06:50:25.705877066 CET	53	57344	8.8.8.8	192.168.2.5
Nov 29, 2020 06:51:06.451838017 CET	54450	53	192.168.2.5	8.8.8.8
Nov 29, 2020 06:51:06.452275991 CET	59261	53	192.168.2.5	8.8.8.8
Nov 29, 2020 06:51:06.460237026 CET	57151	53	192.168.2.5	8.8.8.8
Nov 29, 2020 06:51:06.489944935 CET	53	59261	8.8.8.8	192.168.2.5
Nov 29, 2020 06:51:06.492084026 CET	53	54450	8.8.8.8	192.168.2.5
Nov 29, 2020 06:51:06.495630026 CET	53	57151	8.8.8.8	192.168.2.5
Nov 29, 2020 06:51:14.662991047 CET	59413	53	192.168.2.5	8.8.8.8
Nov 29, 2020 06:51:14.701637983 CET	53	59413	8.8.8.8	192.168.2.5
Nov 29, 2020 06:51:21.824026108 CET	60516	53	192.168.2.5	8.8.8.8
Nov 29, 2020 06:51:21.826122999 CET	51649	53	192.168.2.5	8.8.8.8
Nov 29, 2020 06:51:21.859415054 CET	53	60516	8.8.8.8	192.168.2.5
Nov 29, 2020 06:51:21.863610029 CET	53	51649	8.8.8.8	192.168.2.5
Nov 29, 2020 06:51:22.658529997 CET	65086	53	192.168.2.5	8.8.8.8
Nov 29, 2020 06:51:22.693871975 CET	53	65086	8.8.8.8	192.168.2.5
Nov 29, 2020 06:51:30.456788063 CET	56432	53	192.168.2.5	8.8.8.8
Nov 29, 2020 06:51:30.492680073 CET	53	56432	8.8.8.8	192.168.2.5
Nov 29, 2020 06:51:31.626458883 CET	52929	53	192.168.2.5	8.8.8.8
Nov 29, 2020 06:51:31.662272930 CET	53	52929	8.8.8.8	192.168.2.5
Nov 29, 2020 06:51:34.100285053 CET	64317	53	192.168.2.5	8.8.8.8
Nov 29, 2020 06:51:34.135688066 CET	53	64317	8.8.8.8	192.168.2.5
Nov 29, 2020 06:51:38.658795118 CET	61004	53	192.168.2.5	8.8.8.8
Nov 29, 2020 06:51:38.694324970 CET	53	61004	8.8.8.8	192.168.2.5
Nov 29, 2020 06:51:40.229526997 CET	56895	53	192.168.2.5	8.8.8.8
Nov 29, 2020 06:51:40.265198946 CET	53	56895	8.8.8.8	192.168.2.5
Nov 29, 2020 06:51:40.482561111 CET	62372	53	192.168.2.5	8.8.8.8
Nov 29, 2020 06:51:40.518327951 CET	53	62372	8.8.8.8	192.168.2.5
Nov 29, 2020 06:51:41.393907070 CET	61515	53	192.168.2.5	8.8.8.8
Nov 29, 2020 06:51:41.429419041 CET	53	61515	8.8.8.8	192.168.2.5
Nov 29, 2020 06:51:42.054263115 CET	56675	53	192.168.2.5	8.8.8.8
Nov 29, 2020 06:51:42.090038061 CET	53	56675	8.8.8.8	192.168.2.5
Nov 29, 2020 06:51:48.654684067 CET	57172	53	192.168.2.5	8.8.8.8
Nov 29, 2020 06:51:48.690429926 CET	53	57172	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 29, 2020 06:49:06.794851065 CET	192.168.2.5	8.8.8.8	0xfc83	Standard query (0)	hastebin.com	A (IP address)	IN (0x0001)
Nov 29, 2020 06:49:36.824596882 CET	192.168.2.5	8.8.8.8	0x3952	Standard query (0)	pastebin.com	A (IP address)	IN (0x0001)
Nov 29, 2020 06:49:50.300962925 CET	192.168.2.5	8.8.8.8	0xc052	Standard query (0)	g.msn.com	A (IP address)	IN (0x0001)
Nov 29, 2020 06:51:06.451838017 CET	192.168.2.5	8.8.8.8	0x7226	Standard query (0)	hastebin.com	A (IP address)	IN (0x0001)
Nov 29, 2020 06:51:06.452275991 CET	192.168.2.5	8.8.8.8	0x71be	Standard query (0)	hastebin.com	A (IP address)	IN (0x0001)
Nov 29, 2020 06:51:06.460237026 CET	192.168.2.5	8.8.8.8	0xb643	Standard query (0)	hastebin.com	A (IP address)	IN (0x0001)
Nov 29, 2020 06:51:14.662991047 CET	192.168.2.5	8.8.8.8	0x8d0d	Standard query (0)	hastebin.com	A (IP address)	IN (0x0001)
Nov 29, 2020 06:51:21.824026108 CET	192.168.2.5	8.8.8.8	0x727	Standard query (0)	pastebin.com	A (IP address)	IN (0x0001)
Nov 29, 2020 06:51:21.826122999 CET	192.168.2.5	8.8.8.8	0xbb93	Standard query (0)	pastebin.com	A (IP address)	IN (0x0001)
Nov 29, 2020 06:51:22.658529997 CET	192.168.2.5	8.8.8.8	0xc7e8	Standard query (0)	pastebin.com	A (IP address)	IN (0x0001)
Nov 29, 2020 06:51:31.626458883 CET	192.168.2.5	8.8.8.8	0xb638	Standard query (0)	hastebin.com	A (IP address)	IN (0x0001)
Nov 29, 2020 06:51:40.229526997 CET	192.168.2.5	8.8.8.8	0x5ccc	Standard query (0)	hastebin.com	A (IP address)	IN (0x0001)
Nov 29, 2020 06:51:41.393907070 CET	192.168.2.5	8.8.8.8	0x4c60	Standard query (0)	pastebin.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 29, 2020 06:49:06.833525896 CET	8.8.8.8	192.168.2.5	0xfc83	No error (0)	hastebin.com		172.67.143.180	A (IP address)	IN (0x0001)
Nov 29, 2020 06:49:06.833525896 CET	8.8.8.8	192.168.2.5	0xfc83	No error (0)	hastebin.com		104.24.127.89	A (IP address)	IN (0x0001)
Nov 29, 2020 06:49:06.833525896 CET	8.8.8.8	192.168.2.5	0xfc83	No error (0)	hastebin.com		104.24.126.89	A (IP address)	IN (0x0001)
Nov 29, 2020 06:49:36.860050917 CET	8.8.8.8	192.168.2.5	0x3952	No error (0)	pastebin.com		104.23.98.190	A (IP address)	IN (0x0001)
Nov 29, 2020 06:49:36.860050917 CET	8.8.8.8	192.168.2.5	0x3952	No error (0)	pastebin.com		104.23.99.190	A (IP address)	IN (0x0001)
Nov 29, 2020 06:49:50.351768017 CET	8.8.8.8	192.168.2.5	0xc052	No error (0)	g.msn.com	g-msn-com-nsatc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Nov 29, 2020 06:51:06.489944935 CET	8.8.8.8	192.168.2.5	0x71be	No error (0)	hastebin.com		104.24.126.89	A (IP address)	IN (0x0001)
Nov 29, 2020 06:51:06.489944935 CET	8.8.8.8	192.168.2.5	0x71be	No error (0)	hastebin.com		104.24.127.89	A (IP address)	IN (0x0001)
Nov 29, 2020 06:51:06.489944935 CET	8.8.8.8	192.168.2.5	0x71be	No error (0)	hastebin.com		172.67.143.180	A (IP address)	IN (0x0001)
Nov 29, 2020 06:51:06.492084026 CET	8.8.8.8	192.168.2.5	0x7226	No error (0)	hastebin.com		104.24.126.89	A (IP address)	IN (0x0001)
Nov 29, 2020 06:51:06.492084026 CET	8.8.8.8	192.168.2.5	0x7226	No error (0)	hastebin.com		104.24.127.89	A (IP address)	IN (0x0001)
Nov 29, 2020 06:51:06.492084026 CET	8.8.8.8	192.168.2.5	0x7226	No error (0)	hastebin.com		172.67.143.180	A (IP address)	IN (0x0001)
Nov 29, 2020 06:51:06.495630026 CET	8.8.8.8	192.168.2.5	0xb643	No error (0)	hastebin.com		104.24.126.89	A (IP address)	IN (0x0001)
Nov 29, 2020 06:51:06.495630026 CET	8.8.8.8	192.168.2.5	0xb643	No error (0)	hastebin.com		104.24.127.89	A (IP address)	IN (0x0001)
Nov 29, 2020 06:51:06.495630026 CET	8.8.8.8	192.168.2.5	0xb643	No error (0)	hastebin.com		172.67.143.180	A (IP address)	IN (0x0001)
Nov 29, 2020 06:51:14.701637983 CET	8.8.8.8	192.168.2.5	0x8d0d	No error (0)	hastebin.com		104.24.126.89	A (IP address)	IN (0x0001)
Nov 29, 2020 06:51:14.701637983 CET	8.8.8.8	192.168.2.5	0x8d0d	No error (0)	hastebin.com		104.24.127.89	A (IP address)	IN (0x0001)
Nov 29, 2020 06:51:14.701637983 CET	8.8.8.8	192.168.2.5	0x8d0d	No error (0)	hastebin.com		172.67.143.180	A (IP address)	IN (0x0001)
Nov 29, 2020 06:51:21.859415054 CET	8.8.8.8	192.168.2.5	0x727	No error (0)	pastebin.com		104.23.99.190	A (IP address)	IN (0x0001)
Nov 29, 2020 06:51:21.859415054 CET	8.8.8.8	192.168.2.5	0x727	No error (0)	pastebin.com		104.23.98.190	A (IP address)	IN (0x0001)
Nov 29, 2020 06:51:21.863610029 CET	8.8.8.8	192.168.2.5	0xbb93	No error (0)	pastebin.com		104.23.99.190	A (IP address)	IN (0x0001)
Nov 29, 2020 06:51:21.863610029 CET	8.8.8.8	192.168.2.5	0xbb93	No error (0)	pastebin.com		104.23.98.190	A (IP address)	IN (0x0001)
Nov 29, 2020 06:51:22.693871975 CET	8.8.8.8	192.168.2.5	0xc7e8	No error (0)	pastebin.com		104.23.98.190	A (IP address)	IN (0x0001)
Nov 29, 2020 06:51:22.693871975 CET	8.8.8.8	192.168.2.5	0xc7e8	No error (0)	pastebin.com		104.23.99.190	A (IP address)	IN (0x0001)
Nov 29, 2020 06:51:31.662272930 CET	8.8.8.8	192.168.2.5	0xb638	No error (0)	hastebin.com		104.24.126.89	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 29, 2020 06:51:31.662272930 CET	8.8.8.8	192.168.2.5	0xb638	No error (0)	hastebin.com		104.24.127.89	A (IP address)	IN (0x0001)
Nov 29, 2020 06:51:31.662272930 CET	8.8.8.8	192.168.2.5	0xb638	No error (0)	hastebin.com		172.67.143.180	A (IP address)	IN (0x0001)
Nov 29, 2020 06:51:40.265198946 CET	8.8.8.8	192.168.2.5	0x5ccc	No error (0)	hastebin.com		104.24.126.89	A (IP address)	IN (0x0001)
Nov 29, 2020 06:51:40.265198946 CET	8.8.8.8	192.168.2.5	0x5ccc	No error (0)	hastebin.com		104.24.127.89	A (IP address)	IN (0x0001)
Nov 29, 2020 06:51:40.265198946 CET	8.8.8.8	192.168.2.5	0x5ccc	No error (0)	hastebin.com		172.67.143.180	A (IP address)	IN (0x0001)
Nov 29, 2020 06:51:41.429419041 CET	8.8.8.8	192.168.2.5	0x4c60	No error (0)	pastebin.com		104.23.99.190	A (IP address)	IN (0x0001)
Nov 29, 2020 06:51:41.429419041 CET	8.8.8.8	192.168.2.5	0x4c60	No error (0)	pastebin.com		104.23.98.190	A (IP address)	IN (0x0001)

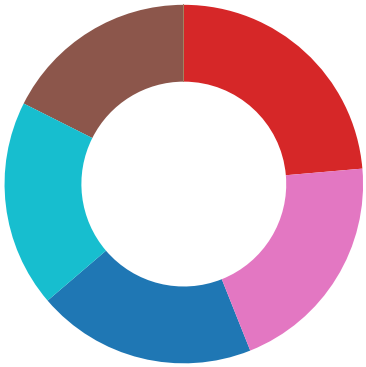
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 29, 2020 06:49:06.951127052 CET	172.67.143.180	443	192.168.2.5	49720	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Sat Jul 25 02:00:00 CEST 2020	Sun Jul 25 14:00:00 CEST 2021	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	3b5074b1b5d032e5620f69f9f700ff0e
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Nov 29, 2020 06:49:36.902630091 CET	104.23.98.190	443	192.168.2.5	49725	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Aug 17 02:00:00 CEST 2020	Tue Aug 17 14:00:00 CEST 2021	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	3b5074b1b5d032e5620f69f9f700ff0e
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Nov 29, 2020 06:51:22.807216883 CET	104.23.98.190	443	192.168.2.5	49743	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Aug 17 02:00:00 CEST 2020	Tue Aug 17 14:00:00 CEST 2021	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	3b5074b1b5d032e5620f69f9f700ff0e
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Code Manipulations

Statistics

Behavior



- Payment_Advice_pdf.exe
- timeout.exe
- conhost.exe
- powershell.exe
- conhost.exe
- powershell.exe
- powershell.exe
- conhost.exe
- conhost.exe
- powershell.exe
- conhost.exe
- Payment_Advice_pdf.exe
- Payment_Advice_pdf.exe
- Payment_Advice_pdf.exe
- Payment_Advice_pdf.exe
- Payment_Advice_pdf.exe
- Payment_Advice_pdf.exe
- timeout.exe
- conhost.exe

Click to jump to process

System Behavior

Analysis Process: Payment_Advice_pdf.exe PID: 4392 Parent PID: 5724

General

Start time:	06:48:54
Start date:	29/11/2020
Path:	C:\Users\user\Desktop\Payment_Advice_pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Payment_Advice_pdf.exe'
Imagebase:	0xa20000
File size:	631776 bytes
MD5 hash:	536CF4ED17EBA1BF41EF70FAAA2054A4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DB9CF06	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	6DB9CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Payment_Advice_pdf.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	6C9EDD66	CopyFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Payment_Advice_pdf.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C9EDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\642ea71a-359c-4338-a04f-1ead15fc1a7a	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C9EBEFF	CreateDirectoryW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Payment_Advice_pdf.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DEAC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Payment_Advice_pdf.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 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 b2 4e a3 5e 00 00 00 00 00 00 00 00 e0 00 22 00 0b 01 30 00 00 b4 08 00 00 da 00 00 00 00 00 00 de d2 08 00 00 20 00 00 00 e0 08 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 00 e0 09 00 00 02 00 00 ae 4b 0a 00 02 00 60 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L....N.^.......... "...0................. ....@.. ....K....`................	success or wait	3	6C9EDD66	CopyFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Payment_Advice_pdf.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	6C9EDD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Payment_Advice_pdf.exe.log	unknown	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0	success or wait	1	6DEAC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DB75705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DAD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB7CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DAD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DAD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DAD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DAD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DB75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C9E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C9E1B4F	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender	success or wait	1	6C9E5F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions	success or wait	1	6C9E5F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions\Paths	success or wait	1	6C9E5F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Real-Time Protection	success or wait	1	6C9E5F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Spynet	success or wait	1	6C9E5F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Features	success or wait	1	6C9E5F3C	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	<Unknown>	unicode	C:\Users\user\Desktop\Payment_Advice_pdf.exe	success or wait	1	6C9E646A	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions\Paths	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Payment_Advice_pdf.exe	dword	0	success or wait	1	6C9EC075	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon	shell	unicode	explorer.exe,"C:\Users\user\Desktop\Payment_Advice_pdf.exe"	success or wait	1	6C9E646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	Payment_Advice_pdf.exe	unicode	C:\Users\user\Desktop\Payment_Advice_pdf.exe	success or wait	1	6C9E646A	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions\Paths	C:\Users\user\Desktop\Payment_Advice_pdf.exe	dword	0	success or wait	1	6C9EC075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Real-Time Protection	DisableRealtimeMonitoring	dword	1	success or wait	1	6C9EC075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Spynet	SpyNetReporting	dword	0	success or wait	1	6C9EC075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Spynet	SubmitSamplesConsent	dword	0	success or wait	1	6C9EC075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Features	TamperProtection	dword	0	success or wait	1	6C9EC075	RegSetValueExW

Analysis Process: timeout.exe PID: 4488 Parent PID: 4392

General

Start time:	06:48:59
Start date:	29/11/2020
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 4
Imagebase:	0x350000
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: conhost.exe PID: 4616 Parent PID: 4488

General

Start time:	06:49:00
Start date:	29/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true

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

Analysis Process: powershell.exe PID: 6924 Parent PID: 4392

General

Start time:	06:49:32
Start date:	29/11/2020
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Payment_Advice_pdf.exe' -Force
Imagebase:	0x12e0000
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	6DB9CF06	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	6DB9CF06	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	6C945B28	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	6C945B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_clsntrj5.a1a.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C9E1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_vxulzjog.0pn.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C9E1E60	CreateFileW
C:\Users\user\Documents\20201129	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C9EBEFF	CreateDirectoryW
C:\Users\user\Documents\20201129\PowerShell_transcript.103386.loZpncW0.20201129064934.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C9E1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_clsntrj5.a1a.ps1	success or wait	1	6C9E6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_vxulzjog.0pn.psm1	success or wait	1	6C9E6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_clsntrj5.a1a.ps1	unknown	1	31	1	success or wait	1	6C9E1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_vxulzjog.0pn.psm1	unknown	1	31	1	success or wait	1	6C9E1B4F	WriteFile
C:\Users\user\Documents\20201129\PowerShell_transcript.103386.loZpncW0.20201129064934.txt	unknown	3	ef bb bf	...	success or wait	1	6C9E1B4F	WriteFile
C:\Users\user\Documents\20201129\PowerShell_transcript.103386.loZpncW0.20201129064934.txt	unknown	741	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 30 31 31 32 39 30 36 35 30 31 33 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 31 30 33 33 38 36 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c	**********..Windows PowerShell transcript start..Start time: 20201129065013..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 103386 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\	success or wait	5	6C9E1B4F	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	6DB75705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DB75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DB75705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DAD03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DB7CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DB7CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB7CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DAD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DAD03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DB75705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DB75705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DB75705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DB75705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DAD03DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf4 9f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DAD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DB75705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6DB81F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21268	success or wait	1	6DB8203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DAD03DE	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	6C9E1B4F	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	6C9E1B4F	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	6C9E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6C9E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6C9E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6C9E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C9E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C9E1B4F	ReadFile

Analysis Process: conhost.exe PID: 6932 Parent PID: 6924

General

Start time:	06:49:32
Start date:	29/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: 6948 Parent PID: 4392

General

Start time:	06:49:32
Start date:	29/11/2020
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -Ex clusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs \Startup\Payment_Advice_pdf.exe' -Force
Imagebase:	0x12e0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

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	6DB9CF06	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	6DB9CF06	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_bppwvxmq.v5t.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C9E1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_lv3izpro.emd.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C9E1E60	CreateFileW
C:\Users\user\Documents\20201129\PowerShell_transcript.103386.z_ziTDYA.20201129064937.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C9E1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_bppwvxmq.v5t.ps1	success or wait	1	6C9E6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_lv3izpro.emd.psm1	success or wait	1	6C9E6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_bppwvxmq.v5t.ps1	unknown	1	31	1	success or wait	1	6C9E1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_lv3izpro.emd.psm1	unknown	1	31	1	success or wait	1	6C9E1B4F	WriteFile
C:\Users\user\Documents\20201129\PowerShell_transcript.103386.z_ziTDYA.20201129064937.txt	unknown	3	ef bb bf	...	success or wait	1	6C9E1B4F	WriteFile
C:\Users\user\Documents\20201129\PowerShell_transcript.103386.z_ziTDYA.20201129064937.txt	unknown	741	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 30 31 31 32 39 30 36 35 30 33 31 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 31 30 33 33 38 36 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c	**********..Windows PowerShell transcript start..Start time: 20201129065031..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 103386 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\	success or wait	1	6C9E1B4F	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	6DB75705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DB75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DB75705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DAD03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DB7CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DB7CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB7CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DAD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DAD03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DB75705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DB75705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DB75705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DB75705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DAD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf4 9f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DAD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DB75705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6DB81F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21268	success or wait	1	6DB8203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DAD03DE	ReadFile

Analysis Process: powershell.exe PID: 7008 Parent PID: 4392

General

Start time:	06:49:33
Start date:	29/11/2020
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -Ex clusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs \Startup\Payment_Advice_pdf.exe' -Force
Imagebase:	0x12e0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

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	6DB9CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DB9CF06	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	6C945B28	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	6C945B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_fwsc2twm.abg.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C9E1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_mmdcdr4n.tid.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C9E1E60	CreateFileW
C:\Users\user\Documents\20201129\PowerShell_transcr ipt.103386.VthBuP45.20201129064936.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C9E1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_fwsc2twm.abg.ps1	success or wait	1	6C9E6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_mmdcdr4n.tid.psm1	success or wait	1	6C9E6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscr iptPolicyTest_fwsc2twm.abg.ps1	unknown	1	31	1	success or wait	1	6C9E1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscr iptPolicyTest_mmdcdr4n.tid.psm1	unknown	1	31	1	success or wait	1	6C9E1B4F	WriteFile
C:\Users\user\Documents\20201129\PowerShell_transcr ipt.103386.VthBuP45.20201129064936.txt	unknown	3	ef bb bf	...	success or wait	1	6C9E1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20201129\PowerShell_transcript.103386.VthBuP45.20201129064936.txt	unknown	741	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 30 31 31 32 39 30 36 35 30 33 32 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 31 30 33 33 38 36 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c	**********..Windows PowerShell transcript start..Start time: 20201129065032..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 103386 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\	success or wait	1	6C9E1B4F	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	6DB75705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DB75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DB75705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DAD03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DB7CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DB7CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB7CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DAD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DAD03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DB75705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DB75705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DB75705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DB75705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DAD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DB75705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DAD03DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6DB81F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21268	success or wait	1	6DB8203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DAD03DE	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	6C9E1B4F	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	6C9E1B4F	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	6C9E1B4F	ReadFile

Analysis Process: conhost.exe PID: 7016 Parent PID: 6948

General

Start time:	06:49:33
Start date:	29/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 7056 Parent PID: 7008

General

Start time:	06:49:33
Start date:	29/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 7104 Parent PID: 4392

General

Start time:	06:49:33
Start date:	29/11/2020
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\Payment_Advice_pdf.exe' -Force
Imagebase:	0x12e0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DB9CF06	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	6DB9CF06	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	6C945B28	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	6C945B28	unknown
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_24fphy4r.0gs.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C9E1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_52egkfrp.jkl.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C9E1E60	CreateFileW
C:\Users\user\Documents\20201129\PowerShell_transcript.103386.JJDrYbN8.20201129064938.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C9E1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_24fphy4r.0gs.ps1	success or wait	1	6C9E6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_52egkfrp.jkl.psm1	success or wait	1	6C9E6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_24fphy4r.0gs.ps1	unknown	1	31	1	success or wait	1	6C9E1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_52egkfrp.jkl.psm1	unknown	1	31	1	success or wait	1	6C9E1B4F	WriteFile
C:\Users\user\Documents\20201129\PowerShell_transcript.103386.JJDrYbN8.20201129064938.txt	unknown	3	ef bb bf	...	success or wait	1	6C9E1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20201129\PowerShell_transcript.103386.JJDrYbN8.20201129064938.txt	unknown	687	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 30 31 31 32 39 30 36 35 30 32 37 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 31 30 33 33 38 36 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c	********..Windows PowerShell transcript start..Start time: 20201129065027..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 103386 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\	success or wait	1	6C9E1B4F	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	6DB75705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DB75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DB75705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DAD03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DB7CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DB7CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB7CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DAD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DAD03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DB75705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DB75705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DB75705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DB75705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DAD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DAD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DB75705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6DB81F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21268	success or wait	1	6DB8203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DAD03DE	ReadFile

Analysis Process: conhost.exe PID: 5792 Parent PID: 7104

General

Start time:	06:49:34
Start date:	29/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: Payment_Advice_pdf.exe PID: 6728 Parent PID: 4392

General

Start time:	06:49:39
Start date:	29/11/2020
Path:	C:\Users\user\Desktop\Payment_Advice_pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Payment_Advice_pdf.exe
Imagebase:	0x840000
File size:	631776 bytes
MD5 hash:	536CF4ED17EBA1BF41EF70FAAA2054A4
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: 00000016.00000002.509306076.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000016.00000002.532140773.0000000002C41000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000016.00000002.532140773.0000000002C41000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: Payment_Advice_pdf.exe PID: 5600 Parent PID: 3472

General

Start time:	06:49:44
Start date:	29/11/2020
Path:	C:\Users\user\Desktop\Payment_Advice_pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Payment_Advice_pdf.exe'
Imagebase:	0xdb0000
File size:	631776 bytes
MD5 hash:	536CF4ED17EBA1BF41EF70FAAA2054A4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: Payment_Advice_pdf.exe PID: 6944 Parent PID: 3472

General

Start time:	06:49:53
Start date:	29/11/2020
Path:	C:\Users\user\Desktop\Payment_Advice_pdf.exe

Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Payment_Advice_pdf.exe'
Imagebase:	0xe50000
File size:	631776 bytes
MD5 hash:	536CF4ED17EBA1BF41EF70FAAA2054A4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: Payment_Advice_pdf.exe PID: 5360 Parent PID: 3472

General

Start time:	06:50:02
Start date:	29/11/2020
Path:	C:\Users\user\Desktop\Payment_Advice_pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Payment_Advice_pdf.exe'
Imagebase:	0x370000
File size:	631776 bytes
MD5 hash:	536CF4ED17EBA1BF41EF70FAAA2054A4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: Payment_Advice_pdf.exe PID: 5916 Parent PID: 3472

General

Start time:	06:50:11
Start date:	29/11/2020
Path:	C:\Users\user\Desktop\Payment_Advice_pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Payment_Advice_pdf.exe'
Imagebase:	0xe60000
File size:	631776 bytes
MD5 hash:	536CF4ED17EBA1BF41EF70FAAA2054A4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: Payment_Advice_pdf.exe PID: 5536 Parent PID: 3472

General

Start time:	06:50:20
Start date:	29/11/2020
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Payment_Advice_pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Payment_Advice_pdf.exe'
Imagebase:	0xbb0000
File size:	631776 bytes
MD5 hash:	536CF4ED17EBA1BF41EF70FAAA2054A4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Antivirus matches:	• Detection: 19%, Metadefender, Browse • Detection: 48%, ReversingLabs

Analysis Process: timeout.exe PID: 4404 Parent PID: 6944

General

Start time:	06:50:53
Start date:	29/11/2020
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 4
Imagebase:	0x350000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 5772 Parent PID: 4404

General

Start time:	06:50:54
Start date:	29/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis