ID: 680371
Sample Name: PAYMENT-ADVICE.exe
Cookbook: default.jbs
Time: 13:47:07
Date: 08/08/2022
Version: 35.0.0 Citrine

Table of Contents

Table of Contents 2
Windows Analysis Report PAYMENT-ADVICE.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Agenttesla 4
Yara Signatures 4
Initial Sample 4
Dropped Files 5
Memory Dumps 5
Unpacked PEs 5
Sigma Signatures 5
Snort Signatures 6
Joe Sandbox Signatures 6
AV Detection 6
Networking 6
Spam, unwanted Advertisements and Ransom Demands 6
System Summary 6
Boot Survival 6
Malware Analysis System Evasion 6
HIPS / PFW / Operating System Protection Evasion 6
Lowering of HIPS / PFW / Operating System Security Settings 6
Stealing of Sensitive Information 6
Remote Access Functionality 7
Mitre Att&ck Matrix 7
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 9
URLs 9
Domains and IPs 11
Contacted Domains 11
URLs from Memory and Binaries 11
World Map of Contacted IPs 21
Public IPs 21
General Information 21
Warnings 22
Simulations 22
Behavior and APIs 22
Joe Sandbox View / Context 22
IPs 22
Domains 22
ASNs 22
JA3 Fingerprints 22
Dropped Files 23
Created / dropped Files 23
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506 23
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506 23
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PAYMENT-ADVICE.exe.log 23
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive 24
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_g4bf5eyu.ra0.psm1 24
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_p02vnukr.mky.ps1 24
C:\Users\user\AppData\Local\Temp\tmpA427.tmp 25
C:\Users\user\AppData\Roaming\rNFzixmDCD.exe 25
C:\Users\user\AppData\Roaming\rNFzixmDCD.exe:Zone.Identifier 25
C:\Users\user\Documents\20220808\PowerShell_transcript.114127.7_bzaf+H.20220808134820.txt 25
C:\Windows\System32\drivers\etc\hosts 26
Static File Info 26
General 26
File Icon 26
Static PE Info 27
General 27
Entrypoint Preview 27
Data Directories 27
Sections 28
Resources 28

Imports 28
Network Behavior 28
Network Port Distribution 28
TCP Packets 28
UDP Packets 29
DNS Queries 29
DNS Answers 30
SMTP Packets 30
Statistics 30
Behavior 30
System Behavior 31
Analysis Process: PAYMENT-ADVICE.exePID: 5664, Parent PID: 5356 31
General 31
File Activities 31
Analysis Process: BackgroundTransferHost.exePID: 1504, Parent PID: 756 31
General 31
File Activities 31
Analysis Process: powershell.exePID: 2404, Parent PID: 5664 31
General 31
File Activities 32
File Created 32
File Deleted 32
File Written 32
File Read 34
Analysis Process: conhost.exePID: 5744, Parent PID: 2404 38
General 38
Analysis Process: schtasks.exePID: 5416, Parent PID: 5664 38
General 38
File Activities 38
File Read 38
Analysis Process: conhost.exePID: 4480, Parent PID: 5416 38
General 38
Analysis Process: PAYMENT-ADVICE.exePID: 3156, Parent PID: 5664 39
General 39
Analysis Process: PAYMENT-ADVICE.exePID: 1504, Parent PID: 5664 39
General 39
File Activities 39
File Created 39
File Written 40
File Read 40
Disassembly 40

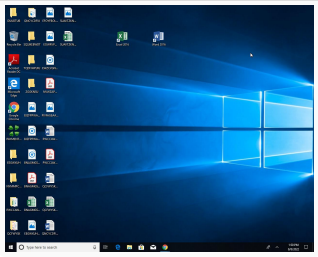
Windows Analysis Report

PAYMENT-ADVICE.exe

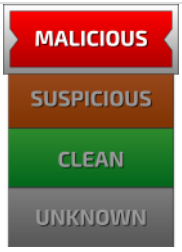
Overview

General Information

Sample Name:	PAYMENT-ADVICE.exe
Analysis ID:	680371
MD5:	2d9f2c92d70a25..
SHA1:	ca8fb29bd41999..
SHA256:	001709cadc8a0a..
Tags:	exe
Infos:	



Detection



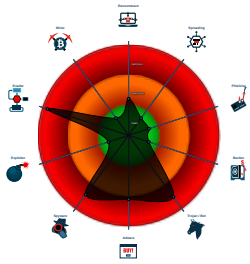
AgentTesla

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

Signatures

- Malicious sample detected (through…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Tries to steal Mail credentials (via fi…
- Initial sample is a PE file and has a…
- Tries to harvest and steal Putty / W…
- Tries to harvest and steal ftp login c…
- Modifies the hosts file
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- Injects a PE file into a foreign proce…
- Yara detected Generic Downloader

Classification



Process Tree

- **System is w10x64**
- PAYMENT-ADVICE.exe (PID: 5664 cmdline: "C:\Users\user\Desktop\PAYMENT-ADVICE.exe" MD5: 2D9F2C92D70A25AD42FE3602D7F932B1)
  - BackgroundTransferHost.exe (PID: 1504 cmdline: "BackgroundTransferHost.exe" -ServerName:BackgroundTransferHost.1 MD5: 02BA81746B929ECC9DB6665589B68335)
  - powershell.exe (PID: 2404 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\rNFzixmDCD.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5744 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 5416 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\rNFzixmDCD" /XML "C:\Users\user\AppData\Local\Temp\tmpA427.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4480 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - PAYMENT-ADVICE.exe (PID: 3156 cmdline: C:\Users\user\Desktop\PAYMENT-ADVICE.exe MD5: 2D9F2C92D70A25AD42FE3602D7F932B1)
  - PAYMENT-ADVICE.exe (PID: 1504 cmdline: C:\Users\user\Desktop\PAYMENT-ADVICE.exe MD5: 2D9F2C92D70A25AD42FE3602D7F932B1)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "vikas@waytogochile.com",
  "Password": "Vikas2020",
  "Host": "mail.waytogochile.com"
}
```

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
PAYMENT-ADVICE.exe	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Roaming\rNFzixmDCD.exe	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000000.280352342.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000009.00000000.280352342.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000009.00000000.280352342.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x301b2:$a13: get_DnsResolver • 0x2e993:$a20: get_LastAccessed • 0x30b30:$a27: set_InternalServerPort • 0x30e4f:$a30: set_GuidMasterKey • 0x2ea9a:$a33: get_Clipboard • 0x2eaa8:$a34: get_Keyboard • 0x2fdcd:$a35: get_ShiftKeyDown • 0x2fdde:$a36: get_AltKeyDown • 0x2eab5:$a37: get_Password • 0x2f57d:$a38: get_PasswordHash • 0x305b2:$a39: get_DefaultCredentials
00000000.00000002.288114287.0000000003665000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.288114287.0000000003665000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 11 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.PAYMENT-ADVICE.exe.36d09d0.5.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.PAYMENT-ADVICE.exe.36d09d0.5.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.PAYMENT-ADVICE.exe.36d09d0.5.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x30e7b:$s10: logins • 0x308e2:$s11: credential • 0x2ce9a:$g1: get_Clipboard • 0x2cea8:$g2: get_Keyboard • 0x2ceb5:$g3: get_Password • 0x2e1bd:$g4: get_CtrlKeyDown • 0x2e1cd:$g5: get_ShiftKeyDown • 0x2e1de:$g6: get_AltKeyDown
0.2.PAYMENT-ADVICE.exe.36d09d0.5.unpack	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x2e5b2:$a13: get_DnsResolver • 0x2cd93:$a20: get_LastAccessed • 0x2ef30:$a27: set_InternalServerPort • 0x2f24f:$a30: set_GuidMasterKey • 0x2ce9a:$a33: get_Clipboard • 0x2cea8:$a34: get_Keyboard • 0x2e1cd:$a35: get_ShiftKeyDown • 0x2e1de:$a36: get_AltKeyDown • 0x2ceb5:$a37: get_Password • 0x2d97d:$a38: get_PasswordHash • 0x2e9b2:$a39: get_DefaultCredentials
9.0.PAYMENT-ADVICE.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 23 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

Yara detected Generic Downloader

Spam, unwanted Advertisements and Ransom Demands

Modifies the hosts file

System Summary

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

.NET source code contains very large array initializations

Boot Survival

Uses schtasks.exe or at.exe to add and modify task schedules

Malware Analysis System Evasion

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

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

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

HIPS / PFW / Operating System Protection Evasion

Modifies the hosts file

Injects a PE file into a foreign processes

Adds a directory exclusion to Windows Defender

Lowering of HIPS / PFW / Operating System Security Settings

Modifies the hosts file

Stealing of Sensitive Information

Yara detected AgentTesla

Tries to steal Mail credentials (via file / registry access)

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal ftp login credentials

Tries to harvest and steal browser information (history, passwords, etc)

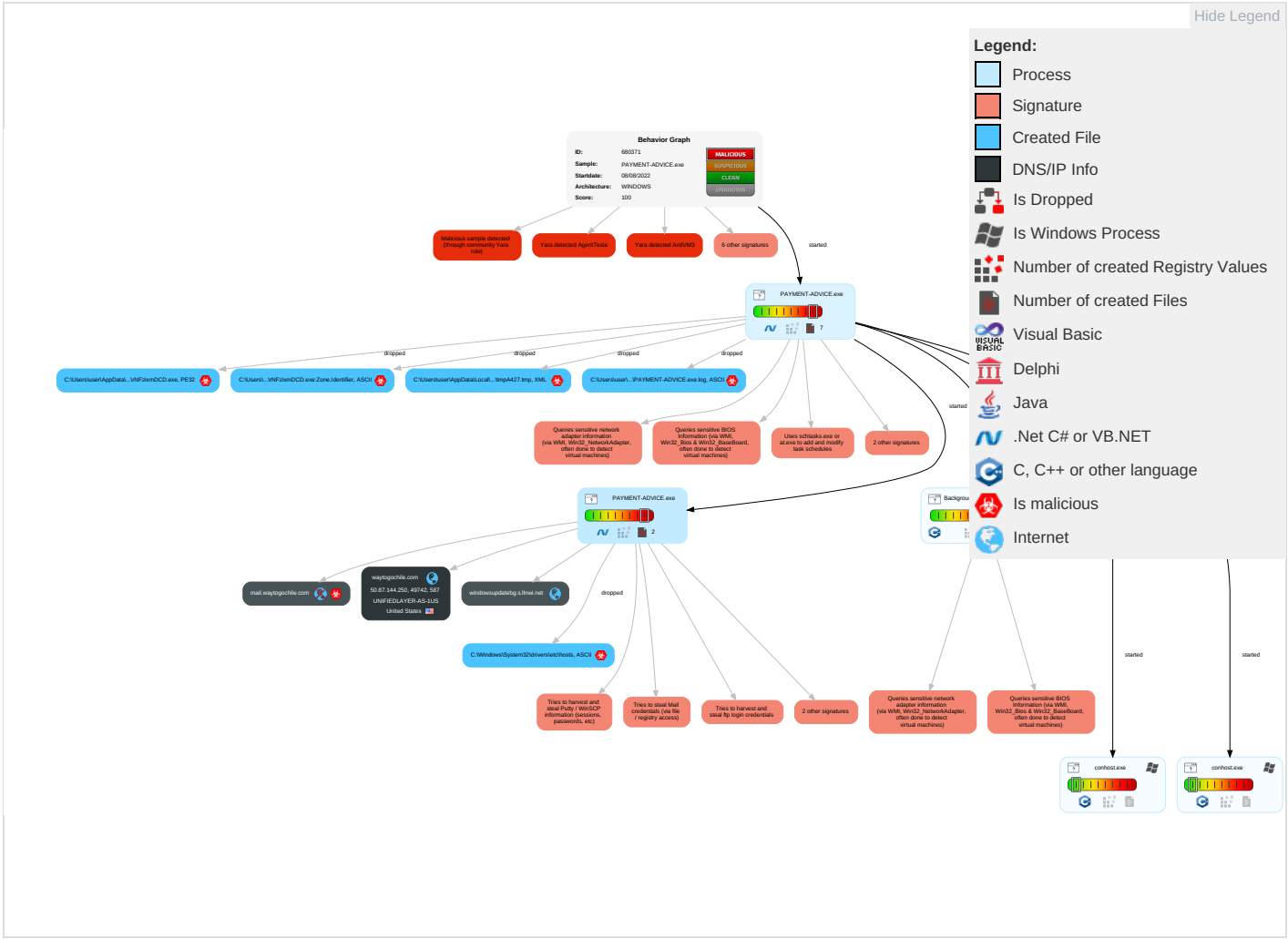
Remote Access Functionality

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	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	1 Scheduled Task/Job	1 1 1 Process Injection	1 File and Directory Permissions Modification	2 OS Credential Dumping	1 Account Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Scheduled Task/Job	1 1 Disable or Modify Tools	1 Input Capture	1 File and Directory Discovery	Remote Desktop Protocol	2 Data from Local System	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Deobfuscate/Decode Files or Information	1 Credentials in Registry	1 1 4 System Information Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	2 Obfuscated Files or Information	NTDS	1 Query Registry	Distributed Component Object Model	1 Input Capture	Scheduled Transfer	1 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	3 Software Packing	LSA Secrets	2 1 1 Security Software Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Masquerading	Cached Domain Credentials	1 Process Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 3 1 Virtualization/Sandbox Evasion	DCSync	1 3 1 Virtualization/Sandbox Evasion	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 1 1 Process Injection	Proc Filesystem	1 Application Window Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	1 System Owner/User Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	1 Remote System Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

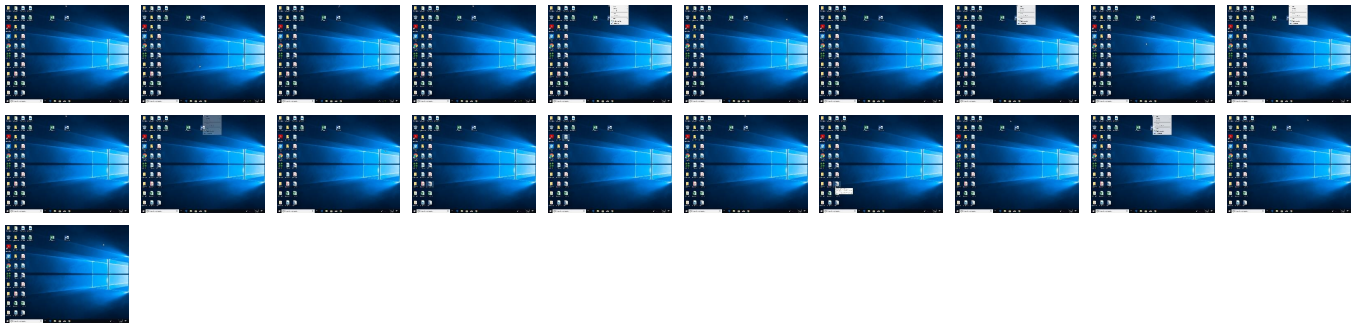
Behavior Graph



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.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\rNFzixmDCD.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
9.0.PAYMENT-ADVICE.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
waytogochile.com	1%	Virustotal		Browse
windowsupdatebg.s.llnwi.net	0%	Virustotal		Browse
mail.waytogochile.com	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	0%	URL Reputation	safe	
http://www.fontbureau.comituoj	0%	Avira URL Cloud	safe	
http://www.certplus.com/CRL/class3.crl0	0%	URL Reputation	safe	
http://ocsp.suscerte.gob.ve0	0%	URL Reputation	safe	
http://www.fontbureau.comessedc	0%	Avira URL Cloud	safe	
http://crl.dhimyotis.com/certignarootca.crl0	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://www.carterandcone.comno	0%	Avira URL Cloud	safe	
http://ca2.mtin.es/mtin/crl/MTINAutoridadRaiz0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-c/cacrl.crl0	0%	URL Reputation	safe	
http://ca.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://www.suscerte.gob.ve/dpc0	0%	URL Reputation	safe	
http://www.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://policy.camerfirma.com0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y	0%	URL Reputation	safe	
http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf0?	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/V	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-b/cacrl.crl0	0%	URL Reputation	safe	
http://microsoft.co	0%	URL Reputation	safe	
http://www.uce.gub.uy/informacion-tecnica/politicas/cp_acrn.pdf0G	0%	URL Reputation	safe	
http://https://wwww.certigna.fr/autorites/0m	0%	URL Reputation	safe	
http://www.ica.co.il/repository/cps/PersonalID_Practice_Statement.pdf0	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	URL Reputation	safe	
http://crl.microsfCC	0%	Avira URL Cloud	safe	
http://www.globaltrust.info0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/D	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://ac.economia.gob.mx/last.crl0G	0%	URL Reputation	safe	
http://www.fontbureau.coma2	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Y0/	0%	URL Reputation	safe	
http://www.carterandcone.comw	0%	URL Reputation	safe	
http://crl.oces.trust2408.com/oces.crl0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/j	0%	URL Reputation	safe	
http://www.fontbureau.comals	0%	URL Reputation	safe	
http://certs.oaticerts.com/repository/OATICA2.crl	0%	URL Reputation	safe	
http://certs.oati.net/repository/OATICA2.crt0	0%	URL Reputation	safe	
http://www.accv.es00	0%	URL Reputation	safe	
http://www.fontbureau.comFV	0%	Avira URL Cloud	safe	
http://web.ncdc.gov.sa/crl/nrcaparta1.crl	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.acabogacia.org0	0%	URL Reputation	safe	
http://www.fontbureau.comgritaY	0%	Avira URL Cloud	safe	
http://www.founder.c	0%	URL Reputation	safe	
http://https://api.ipify.org%%startupfolder%	0%	URL Reputation	safe	
http://crl.securetrust.com/SGCA.crl0	0%	URL Reputation	safe	
http://www.agesic.gub.uy/acrn/acrn.crl0)	0%	URL Reputation	safe	
http://acraiz.icpbrasil.gov.br/LCRacraizv1.crl	0%	Avira URL Cloud	safe	
http://www.carterandcone.comB	0%	URL Reputation	safe	
http://www.rcsc.lt/repository0	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.zhongyicts.com.cnTC	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.carterandcone.comE	0%	URL Reputation	safe	
http://x1.c.lencr.org/0	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://x1.i.lencr.org/0	0%	URL Reputation	safe	
http://www.correo.com.uy/correocert/cps.pdf0	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htmf	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://waytogochile.com	0%	Avira URL Cloud	safe	
http://certs.oaticerts.com/repository/OATICA2.crt08	0%	URL Reputation	safe	
http://cps.chambersign.org/cps/chambersignroot.html0	0%	URL Reputation	safe	
http://www.oaticerts.com/repository.	0%	URL Reputation	safe	
http://www.ancert.com/cps0	0%	URL Reputation	safe	
http://ocsp.accv.es0	0%	URL Reputation	safe	
http://acraiz.icpbrasil.gov.br/LCRacraizv2.crl0	0%	URL Reputation	safe	
http://www.echoworx.com/ca/root2/cps.pdf0	0%	URL Reputation	safe	
http://cSdGYD.com	0%	Avira URL Cloud	safe	
http://ca.mtin.es/mtin/crl/MTINAutoridadRaiz03	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://acraiz.icpbrasil.gov.br/LCRacraizv1.crl0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
waytogochile.com	50.87.144.250	true	false	• 1%, Virustotal, Browse	unknown
windowsupdatebg.s.llnwi.net	178.79.225.0	true	false	• 0%, Virustotal, Browse	unknown
mail.waytogochile.com	unknown	unknown	true	• 1%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	PAYMENT-ADVICE.exe, 00000009.00000003.316775640.0000000006A51000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000009.00000003.317999412.0000000006A52000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comituoj	PAYMENT-ADVICE.exe, 00000000.00000003.245541059.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.245612940.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.245939337.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.245737324.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.245697904.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.245893190.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.245915879.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.245770538.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.245675149.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.245966630.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.245820046.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.245990326.0000000005390000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.certplus.com/CRL/class3.crl0	PAYMENT-ADVICE.exe, 00000009.00000003.317885982.0000000006C3A000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ocsp.suscerte.gob.ve0	PAYMENT-ADVICE.exe, 00000009.00000003.317135049.0000000006CF2000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000009.00000003.318051121.0000000006C32000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comessedc	PAYMENT-ADVICE.exe, 00000000.00000003.245541059.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.245612940.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.245939337.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.245737324.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.245697904.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.245893190.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.245915879.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.245770538.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.245675149.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.245503899.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.245464381.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.245820046.0000000005390000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.dhimyotis.com/certignarootca.crl0	PAYMENT-ADVICE.exe, 00000009.00000003.316952523.00000000069EE000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://sertifikati.ca.posta.rs/crl/PostaCARoot.crl0	PAYMENT-ADVICE.exe, 00000009.00000003.318051121.0000000006C32000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000009.00000003.446747240.0000000006C37000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.chambersign.org1	PAYMENT-ADVICE.exe, 00000009.00000003.317293236.0000000006CC3000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000009.00000003.317075496.0000000006CFC000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://repository.swisssign.com/0	PAYMENT-ADVICE.exe, 00000009.00000003.318051121.0000000006C32000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000009.00000003.317176096.0000000006CE4000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000009.00000003.317480011.0000000006CB0000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers	PAYMENT-ADVICE.exe, 00000000.00000003.244266150.0000000005390000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.comno	PAYMENT-ADVICE.exe, 00000000.00000003.242187057.0000000005367000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.241919573.0000000005364000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.242690202.000000000536B000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.242509856.0000000005365000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ca2.mtin.es/mtin/crl/MTINAutoridadRaiz0	PAYMENT-ADVICE.exe, 00000009.00000003.317293236.0000000006CC3000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.ssc.lt/root-c/cacrl.crl0	PAYMENT-ADVICE.exe, 00000009.00000003.316952523.00000000069EE000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ca.disig.sk/ca/crl/ca_disig.crl0	PAYMENT-ADVICE.exe, 00000009.00000003.317293236.0000000006CC3000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000009.00000003.445945425.00000006CDB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.suscerte.gob.ve/dpc0	PAYMENT-ADVICE.exe, 00000009.00000003.317135049.0000000006CF2000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000009.00000003.318051121.00000006C32000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.disig.sk/ca/crl/ca_disig.crl0	PAYMENT-ADVICE.exe, 00000009.00000003.317293236.0000000006CC3000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000009.00000003.445945425.00000006CDB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	PAYMENT-ADVICE.exe, 00000000.00000002.292161681.00000000065F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html5	PAYMENT-ADVICE.exe, 00000000.00000003.245227416.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.245043521.00000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.244602175.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.244869097.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.244529636.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.244785379.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.244574340.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.245196092.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.244957508.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.245070927.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.244641952.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.244727855.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.244553519.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.244841565.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.244927047.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.245173045.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.244990804.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.244810442.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.244761242.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.244620054.0000000005390000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.zhongyicts.com.cn	PAYMENT-ADVICE.exe, 00000000.00000003.241093875.000000000538F000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000002.292161681.00000000065F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	PAYMENT-ADVICE.exe, 00000000.00000002.285145322.000000000255B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://api.ipify.org%	PAYMENT-ADVICE.exe, 00000009.00000002.506133681.0000000002E71000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://pki.registradores.org/normativa/index.htm0	PAYMENT-ADVICE.exe, 00000009.00000003.316952523.00000000069EE000.00000004.00000800.00020000.00000000.sdmp	false		high
http://policy.camerfirma.com0	PAYMENT-ADVICE.exe, 00000009.00000003.317293236.0000000006CC3000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000009.00000003.317176096.0000000006CE4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y	PAYMENT-ADVICE.exe, 00000000.00000003.242056881.000000000538E000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.242132857.000000000538E000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.241998865.0000000005394000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.242223653.000000000538E000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.241951986.000000000538E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.anf.es/es/address-direccion.html	PAYMENT-ADVICE.exe, 00000009.00000003.317176096.0000000006CE4000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.anf.es/address/)1(0&	PAYMENT-ADVICE.exe, 00000009.00000003.317885982.0000000006C3A000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000009.00000003.317570045.0000000006C3F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf0?	PAYMENT-ADVICE.exe, 00000009.00000003.317293236.0000000006CC3000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000009.00000003.317550868.0000000006CD3000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000009.00000003.317480011.0000000006CB0000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/V	PAYMENT-ADVICE.exe, 00000000.00000003.242056881.000000000538E000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.242132857.000000000538E000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.241998865.0000000005394000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.242573887.000000000538E000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.242298115.000000000538E000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.242621313.000000000538E000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.242405955.000000000538E000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.242821504.0000000005395000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.242223653.000000000538E000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.242596197.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.242718773.000000000538E000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.242445517.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.242651071.000000000538E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://cps.letsencrypt.org0	PAYMENT-ADVICE.exe, 00000009.00000002.511603322.00000000031D3000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.ssc.lt/root-b/cacrl.crl0	PAYMENT-ADVICE.exe, 00000009.00000003.317135049.0000000006CF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://microsoft.co	PAYMENT-ADVICE.exe, 00000009.00000003.445543359.0000000006A51000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.certicamara.com/dpc/0Z	PAYMENT-ADVICE.exe, 00000009.00000003.317570045.0000000006C3F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.uce.gub.uy/informacion-tecnica/politicas/cp_acrn.pdf0G	PAYMENT-ADVICE.exe, 00000009.00000003.317293236.0000000006CC3000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.pki.wellsfargo.com/wsprca.crl0	PAYMENT-ADVICE.exe, 00000009.00000003.316775640.0000000006A51000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000009.00000003.317999412.0000000006A52000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://wwww.certigna.fr/autorites/0m	PAYMENT-ADVICE.exe, 00000009.00000003.316952523.00000000069EE000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.ica.co.il/repository/cps/PersonalID_Practice_Statement.pdf0	PAYMENT-ADVICE.exe, 00000009.00000003.317135049.0000000006CF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	PAYMENT-ADVICE.exe, 00000009.00000002.506133681.0000000002E71000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.anf.es/AC/ANFServerCA.crl0	PAYMENT-ADVICE.exe, 00000009.00000003.317570045.0000000006C3F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://crl.microsfCC	PAYMENT-ADVICE.exe, 00000009.00000003.445543359.0000000006A51000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.globaltrust.info0	PAYMENT-ADVICE.exe, 00000009.00000002.515403329.00000000069CD000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/D	PAYMENT-ADVICE.exe, 00000000.00000003.242056881.000000000538E000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.242132857.0000000000538E000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.242573887.000000000538E000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.242298115.000000000538E000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.242621313.000000000538E000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.242405955.000000000538E000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.242821504.0000000005395000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.242223653.000000000538E000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.242596197.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.242718773.000000000538E000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.242445517.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.242651071.000000000538E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/V	PAYMENT-ADVICE.exe, 00000000.00000003.243968794.0000000005394000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.coml	PAYMENT-ADVICE.exe, 00000000.00000002.292161681.00000000065F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ac.economia.gob.mx/last.crl0G	PAYMENT-ADVICE.exe, 00000009.00000003.317075496.0000000006CFC000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.coma2	PAYMENT-ADVICE.exe, 00000000.00000003.250249996.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.244356405.00000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.244393260.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.244308922.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.244451182.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.249004082.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.244338184.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.249191383.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.249400543.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.244288016.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.249285616.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.244471028.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.249085609.0000000005394000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.244502148.0000000005390000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1.crt0	PAYMENT-ADVICE.exe, 00000009.00000003.317480011.0000000006CB0000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/Y0/	PAYMENT-ADVICE.exe, 00000000.00000003.242298115.000000000538E000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.242405955.000000000538E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comw	PAYMENT-ADVICE.exe, 00000000.00000003.241434338.0000000005390000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.oces.trust2408.com/oces.crl0	PAYMENT-ADVICE.exe, 00000009.00000003.317176096.0000000006CE4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/j	PAYMENT-ADVICE.exe, 00000000.00000003.242298115.000000000538E000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.242621313.000000000538E000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.242405955.000000000538E000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.242821504.0000000005395000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.242596197.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.242718773.000000000538E000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.242651071.000000000538E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://eca.hinet.net/repository0	PAYMENT-ADVICE.exe, 00000009.00000003.317293236.0000000006CC3000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comals	PAYMENT-ADVICE.exe, 00000000.00000003.24 5541059.0000000005390000.00000004.000008 00.00020000.00000000.sdmp, PAYMENT-ADVIC E.exe, 00000000.00000003.245612940.00000 0005390000.00000004.00000800.00020000.0 0000000.sdmp, PAYMENT-ADVICE.exe, 000000 00.00000003.245939337.0000000005390000.0 0000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.2 45227416.0000000005390000.00000004.00000 800.00020000.00000000.sdmp, PAYMENT-ADVI CE.exe, 00000000.00000003.245737324.0000 000005390000.00000004.00000800.00020000. 00000000.sdmp, PAYMENT-ADVICE.exe, 00000 000.00000003.245697904.0000000005390000. 00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003. 245893190.0000000005390000.00000004.0000 0800.00020000.00000000.sdmp, PAYMENT-ADV ICE.exe, 00000000.00000003.245915879.000 0000005390000.00000004.00000800.00020000 .00000000.sdmp, PAYMENT-ADVICE.exe, 0000 0000.00000003.245770538.0000000005390000 .00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003 .245196092.0000000005390000.00000004.000 00800.00020000.00000000.sdmp, PAYMENT-AD VICE.exe, 00000000.00000003.245443702.00 00000005390000.00000004.00000800.0002000 0.00000000.sdmp, PAYMENT-ADVICE.exe, 000 00000.00000003.245675149.000000000539000 0.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.0000000 3.245070927.0000000005390000.00000004.00 000800.00020000.00000000.sdmp, PAYMENT-A DVICE.exe, 00000000.00000003.245402109.0 0000000005390000.00000004.00000800.000200 00.00000000.sdmp, PAYMENT-ADVICE.exe, 00 000000.00000003.245256302.0000000005390 00.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.000000 03.245503899.0000000005390000.00000004.0 0000800.00020000.00000000.sdmp, PAYMENT- ADVICE.exe, 00000000.00000003.245173045. 0000000005390000.00000004.00000800.00020 000.00000000.sdmp, PAYMENT-ADVICE.exe, 0 0000000.00000003.245464381.0000000005390 000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.245820 046.0000000005390000.00000004.00000800.0 0020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://certs.oaticerts.com/repository/OATICA2.crl	PAYMENT-ADVICE.exe, 00000009.00000003.31 7176096.0000000006CE4000.00000004.000008 00.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://certs.oati.net/repository/OATICA2.crt0	PAYMENT-ADVICE.exe, 00000009.00000003.31 7176096.0000000006CE4000.00000004.000008 00.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.accv.es00	PAYMENT-ADVICE.exe, 00000009.00000003.31 7480011.0000000006CB0000.00000004.000008 00.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http:// www.pki.admin.ch/policy/CPS_2_16_756_1_17_3_21_ 1.pdf0	PAYMENT-ADVICE.exe, 00000009.00000003.31 7293236.0000000006CC3000.00000004.000008 00.00020000.00000000.sdmp	false		high

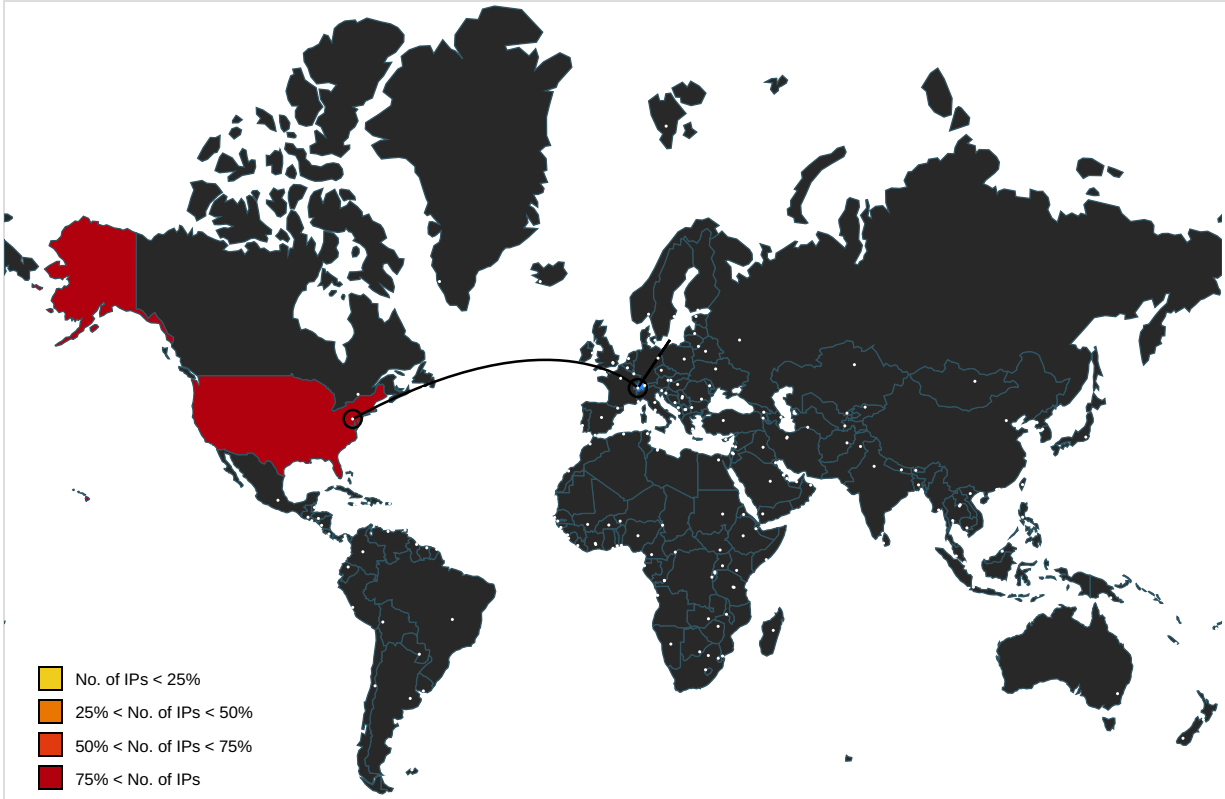
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comFV	PAYMENT-ADVICE.exe, 00000000.00000003.24 5541059.0000000005390000.00000004.000008 00.00020000.00000000.sdmp, PAYMENT-ADVIC E.exe, 00000000.00000003.245612940.00000 00005390000.00000004.00000800.00020000.0 0000000.sdmp, PAYMENT-ADVICE.exe, 000000 00.00000003.245939337.0000000005390000.0 0000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.2 45227416.0000000005390000.00000004.00000 800.00020000.00000000.sdmp, PAYMENT-ADVI CE.exe, 00000000.00000003.245737324.0000 000005390000.00000004.00000800.00020000. 00000000.sdmp, PAYMENT-ADVICE.exe, 00000 000.00000003.245697904.0000000005390000. 00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003. 245893190.0000000005390000.00000004.0000 0800.00020000.00000000.sdmp, PAYMENT-ADV ICE.exe, 00000000.00000003.245915879.000 0000005390000.00000004.00000800.00020000 .00000000.sdmp, PAYMENT-ADVICE.exe, 0000 0000.00000003.245770538.0000000005390000 .00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003 .245196092.0000000005390000.00000004.000 00800.00020000.00000000.sdmp, PAYMENT-AD VICE.exe, 00000000.00000003.245443702.00 00000005390000.00000004.00000800.0002000 0.00000000.sdmp, PAYMENT-ADVICE.exe, 000 00000.00000003.245675149.000000005390000 0.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.0000000 3.245966630.0000000005390000.00000004.00 000800.00020000.00000000.sdmp, PAYMENT-A DVICE.exe, 00000000.00000003.245402109.0 000000005390000.00000004.00000800.000200 00.00000000.sdmp, PAYMENT-ADVICE.exe, 00 000000.00000003.245256302.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.000000 03.245503899.0000000005390000.00000004.0 0000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.245173045. 0000000005390000.00000004.00000800.00020 000.00000000.sdmp, PAYMENT-ADVICE.exe, 0 0000000.00000003.245464381.0000000005390 000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.245820 046.0000000005390000.00000004.00000800.0 0020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.245990326.000000000 5390000.00000004.00000800.00020000.00000 000.sdmp	false	• Avira URL Cloud: safe	unknown
http://web.ncdc.gov.sa/crl/nrcaparta1.crl	PAYMENT-ADVICE.exe, 00000009.00000003.31 7293236.0000000006CC3000.00000004.000008 00.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.datev.de/zertifikat-policy-int0	PAYMENT-ADVICE.exe, 00000009.00000003.31 7176096.0000000006CE4000.00000004.000008 00.00020000.00000000.sdmp, PAYMENT-ADVIC E.exe, 00000009.00000003.317480011.00000 00006CB0000.00000004.00000800.00020000.0 0000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	PAYMENT-ADVICE.exe, 00000000.00000002.29 2161681.00000000065F2000.00000004.000008 00.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://boards.4chan.org/b/	PAYMENT-ADVICE.exe, rNFzixmDCD.exe.0.dr	false		high
http://www.acabogacia.org0	PAYMENT-ADVICE.exe, 00000009.00000003.31 7293236.0000000006CC3000.00000004.000008 00.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.firmaprofesional.com/cps0	PAYMENT-ADVICE.exe, 00000009.00000003.31 7570045.0000000006C3F000.00000004.000008 00.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comgritaY	PAYMENT-ADVICE.exe, 00000000.00000003.250249996.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.282918228.00000005394000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.249004082.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.249191383.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.249400543.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.249285616.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.249085609.0000000005394000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.c	PAYMENT-ADVICE.exe, 00000000.00000003.240620543.000000000538E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.ipify.org%%startupfolder%	PAYMENT-ADVICE.exe, 00000009.00000002.506133681.0000000002E71000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://crl.securetrust.com/SGCA.crl0	PAYMENT-ADVICE.exe, 00000009.00000003.317293236.0000000006CC3000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.agesic.gub.uy/acrn/acrn.crl0)	PAYMENT-ADVICE.exe, 00000009.00000003.317293236.0000000006CC3000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://acraiz.icpbrasil.gov.br/LCRacraizv1.crl	PAYMENT-ADVICE.exe, 00000009.00000003.317550868.0000000006CD3000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comB	PAYMENT-ADVICE.exe, 00000000.00000003.241239656.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.241179726.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.241220651.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.241332459.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.241287867.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.241495178.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.241311661.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.241434338.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.241268186.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.241479619.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.241200143.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.241464737.0000000005390000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.rcsc.lt/repository0	PAYMENT-ADVICE.exe, 00000009.00000003.317480011.0000000006CB0000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	PAYMENT-ADVICE.exe, 00000000.00000002.292161681.00000000065F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cnTC	PAYMENT-ADVICE.exe, 00000000.00000003.241093875.000000000538F000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	PAYMENT-ADVICE.exe, 00000000.00000002.292161681.00000000065F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://web.certicamara.com/marco-legal0Z	PAYMENT-ADVICE.exe, 00000009.00000003.317176096.0000000006CE4000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.comE	PAYMENT-ADVICE.exe, 00000000.00000003.241434338.0000000005390000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.quovadisglobal.com/cps0	PAYMENT-ADVICE.exe, 00000009.00000003.316952523.00000000069EE000.00000004.00000800.00020000.00000000.sdmp	false		high
http://x1.c.lencr.org/0	PAYMENT-ADVICE.exe, 00000009.00000002.511603322.00000000031D3000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://x1.i.lencr.org/0	PAYMENT-ADVICE.exe, 00000009.00000002.511603322.00000000031D3000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.correo.com.uy/correocert/cps.pdf0	PAYMENT-ADVICE.exe, 00000009.00000003.316775640.0000000006A51000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htmf	PAYMENT-ADVICE.exe, 00000000.00000003.246677015.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.246650218.0000000005390000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	PAYMENT-ADVICE.exe, 00000009.00000002.506133681.0000000002E71000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	PAYMENT-ADVICE.exe, 00000000.00000002.292161681.00000000065F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	PAYMENT-ADVICE.exe, 00000000.00000002.292161681.00000000065F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://waytogochile.com	PAYMENT-ADVICE.exe, 00000009.00000002.511603322.00000000031D3000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://certs.oaticerts.com/repository/OATICA2.crt08	PAYMENT-ADVICE.exe, 00000009.00000003.317176096.0000000006CE4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://cps.chambersign.org/cps/chambersignroot.html0	PAYMENT-ADVICE.exe, 00000009.00000003.317075496.0000000006CFC000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.anf.es/AC/RC/ocsp0c	PAYMENT-ADVICE.exe, 00000009.00000003.317570045.0000000006C3F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.oaticerts.com/repository.	PAYMENT-ADVICE.exe, 00000009.00000003.317176096.0000000006CE4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.ancert.com/cps0	PAYMENT-ADVICE.exe, 00000009.00000003.316952523.00000000069EE000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ocsp.accv.es0	PAYMENT-ADVICE.exe, 00000009.00000003.317480011.0000000006CB0000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://acraiz.icpbrasil.gov.br/LCRacraizv2.crl0	PAYMENT-ADVICE.exe, 00000009.00000003.317480011.0000000006CB0000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.echoworx.com/ca/root2/cps.pdf0	PAYMENT-ADVICE.exe, 00000009.00000003.317570045.0000000006C3F000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://rca.e-szigno.hu/ocsp0-	PAYMENT-ADVICE.exe, 00000009.00000003.316952523.00000000069EE000.00000004.00000800.00020000.00000000.sdmp	false		high
http://cSdGYD.com	PAYMENT-ADVICE.exe, 00000009.00000002.506133681.0000000002E71000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ca.mtin.es/mtin/crl/MTINAutoridadRaiz03	PAYMENT-ADVICE.exe, 00000009.00000003.317293236.0000000006CC3000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://eca.hinet.net/repository/CRL2/CA.crl0	PAYMENT-ADVICE.exe, 00000009.00000003.317293236.0000000006CC3000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.datev.de/zertifikat-policy-std0	PAYMENT-ADVICE.exe, 00000009.00000003.317936131.0000000006CAF000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000009.00000003.316952523.00000000069EE000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000009.00000003.317655861.0000000006CAE000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000009.00000002.516201934.0000000006CAE000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/jp/	PAYMENT-ADVICE.exe, 00000000.00000003.242445517.0000000005390000.00000004.00000800.00020000.00000000.sdmp, PAYMENT-ADVICE.exe, 00000000.00000003.242651071.0000000000538E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://acraiz.icpbrasil.gov.br/LCRacraizv1.crl0	PAYMENT-ADVICE.exe, 00000009.00000003.317293236.0000000006CC3000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
50.87.144.250	waytogochile.com	United States		46606	UNIFIEDLAYER-AS-1US	false

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	680371
Start date and time: 08/08/202213:47:07	2022-08-08 13:47:07 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PAYMENT-ADVICE.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:	33
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.spyw.evad.winEXE@12/11@2/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 92% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 178.79.225.0, 209.197.3.8
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, store-images.s-microsoft.com-c.edgekey.net, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, arc.msn.com, wu-bg-shim.trafficmanager.net, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
13:48:13	API Interceptor	688x Sleep call for process: PAYMENT-ADVICE.exe modified
13:48:22	API Interceptor	44x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Users\user\Desktop\PAYMENT-ADVICE.exe
File Type:	Microsoft Cabinet archive data, 61712 bytes, 1 file
Category:	dropped
Size (bytes):	61712
Entropy (8bit):	**7.995044632446497**
Encrypted:	**true**
SSDEEP:	1536:gzjJiDImMsrjCtGLaexX/zL09mX/lZHIxs:gPJiDI/sr0Hexv/0S/zx
MD5:	589C442FC7A0C70DCA927115A700D41E
SHA1:	66A07DACE3AFBFD1AA07A47E6875BEAB62C4BB31
SHA-256:	2E5CB72E9EB43BAAFB6C6BFCC573AAC92F49A8064C483F9D378A9E8E781A526A
SHA-512:	1B5FA79E52BE495C42CF49618441FB7012E28C02E7A08A91DA9213DB3AB810F0E83485BC1DD5F625A47D0BA7CFCDD5EA50ACC9A8DCEBB39F048C40F01E94155B
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF.....,.....I.....y.....Tf. .authroot.stl..W.`.4..CK..8U[...q.yL'sf!d.D..."2.2g.<dVI.!.....$).\...!2s..(...[.T7..{}...g....g.....w.km$.&|..qe.n.8+..&...O...`...+..C.....`h!0.I.(C..1Q*L.p..".s..B.....H.....fUP@..5...(X#.t.2lX.>.y|D.0Z0...M....I(.#.-... ...(.J....2..`.hO..{l+.bd7y.j..u.....3....<.....3....s.T...._.'...%{v...s.....KgV.0..X=.A.9w9.Ea.x.....\.=.e.C2.....9.....`.o... .....@pm.. a.....-M.....{...s.mW.....;.+...A.....0.g..L9#.v.&O>./xSH.S.....GH.6.j...`2.(0g..... Lt.....h4.iQ?....[.K.....uI.....}.....d....M.....6q.Q~.0.\.'U^)`..u.....-.....d..7...2.-.2+3.....A./.%Q...k...Q.,...H.B.%..O..x..5\...Hk.....B.';"Ym.'....X.l.E.6..a8.6..nq..x.r4..1t.....,..u.O..O.L...Uf...X.u.F .(.(.....".q...n{%U.-u....l6!....Z....~o0.}Q'.s.i....7...>4x...A.h.Mk].O.z.].6...53...b^;..>e..x.'1..\p.O.k..B1w..|..K.R.....2.e0..X.^...I...w..!.v5B]x..z.6.G^uF..].b.W...'..I.;..p..@L{.E..@W..3.&...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Users\user\Desktop\PAYMENT-ADVICE.exe
File Type:	data
Category:	modified
Size (bytes):	290
Entropy (8bit):	2.9447851908702747
Encrypted:	false
SSDEEP:	3:kkFklK9E/ltfllXlE/6hpllGhlR6pFRltB+SliQlP8F+RlTRe86A+iRlERMta9bP:kK/+N+SkQlPlEGYRMY9z+4KlDA3RUe/
MD5:	1C14DE57307A1B51C7B11F7ED0B0ED6C
SHA1:	5D5542D686F4938EF7C1660470235765EF2708D9
SHA-256:	B9CBA7CC9ABCF706140DDC49727E92E182C855BB1A86FD29CCC737B3235895AC
SHA-512:	39C4E8933E0470127B5D82B17CF68D9129FF50CBB58A66F873303F6A83CEEB7B04B34891CF35758E9C24760E61A1F4EEBA06A8895CE87F0032E8401D770B8A50
Malicious:	false
Reputation:	low
Preview:	p..... .....m...(..... ....L.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PAYMENT-ADVICE.exe.log

Process:	C:\Users\user\Desktop\PAYMENT-ADVICE.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84FsXE8:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzu
MD5:	2E016B886BDB8389D2DD0867BE55F87B
SHA1:	25D28EF2ACBB41764571E06E11BF4C05DD0E2F8B
SHA-256:	1D037CF00A8849E6866603297F85D3DABE09535E72EDD2636FB7D0F6C7DA3427

SHA-512:	C100729153954328AA2A77EECB2A3CBD03CB7E8E23D736000F890B17AAA50BA87745E30FB9E2B0D61E16DCA45694C79B4CE09B9F4475220BEB38CAEA546CFC2A
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",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..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",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\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22248
Entropy (8bit):	5.601355512915253
Encrypted:	false
SSDEEP:	384:6PtCDT00R+dgN3SBKnNSjultIti7Y9gdSJ3xu1BMrmHZ1AV7mjcWwQ64l+iSY:Udw34K4CltS2dcN+4ajZA
MD5:	4735FDB06E86095FE7B6C1A487F76917
SHA1:	BC7A67AEE462A0EA89D644E49D58310B73CFD652
SHA-256:	D6FE2E815F67742E43AC2E1234AE4C765376E605AD8F3E52D2B20B282B0BD032
SHA-512:	87D6CB0D44C59B722E5398876157D0D0FFC3CF9550C8E2F506C1D98168E9EA21B3F7C68261FC89C5A59B39D437024BFE1CF1F75FC7D0513C08D26DF6434F1FF
Malicious:	false
Preview:	@...e.....s.....?.n.....@.....H.....<@.^.L."My...:R..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'...L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_g4bf5eyu.ra0.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_p02vnukr.mky.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\tmpA427.tmp

Process:	C:\Users\user\Desktop\PAYMENT-ADVICE.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1597
Entropy (8bit):	5.1515491367200426
Encrypted:	false
SSDEEP:	24:2di4+S2qh/Q1K1y1mokUnrKMhEMOFGpwOzNgU3ODOilQRvh7hwrgXuNt7xvn:cge4MYrFdOFzOzN33ODOiDdKrsuTlv
MD5:	B768D0ABC5ABA4635FD8227222020095
SHA1:	C666124BA7B44AD460636DC2321A48E88ADE0ECB
SHA-256:	53B7D65D28A3BE473DC3AB09FF2A9C8B30062AC1F1BE3969D384B7BD313F1FD6
SHA-512:	42004A3F3EE326CAEDE5731DFD5620CFDC1427015118444405F04A3AB799198247AFF85CEC8AF36947803947E9C8A6EAB615572BD8EC98E1330157B9112A0BC9
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>. <

C:\Users\user\AppData\Roaming\rNFzixmDCD.exe

Process:	C:\Users\user\Desktop\PAYMENT-ADVICE.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1024000
Entropy (8bit):	7.481605845274099
Encrypted:	false
SSDEEP:	12288:5CSXZj4rDO3Koc+FI64Ap+1MUo4p/L2R6hT/0yAEfirpHhOtfI/4eAwRXIbUDbL+:5CTFqZ+zJhT/0yAJrIfIAe9IbUDHDls
MD5:	2D9F2C92D70A25AD42FE3602D7F932B1
SHA1:	CA8FB29BD419998B7F2DA87C49F1EB7B2C0700A0
SHA-256:	001709CADC8A0A856D91B9E3C9C0753AC8469D3C6CF2F532FDD53AEDB3A268D6
SHA-512:	8D71362C4074423EE1E8F48FB11332A0BA58ADD496AD65E0B83331F34029D58D9D347BB70B7F496C11FF9B6482A679389CEAFF78B088D782936720E2CAC8E163
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_GenericDownloader_1, Description: Yara detected Generic Downloader, Source: C:\Users\user\AppData\Roaming\rNFzixmDCD.exe, Author: Joe Security
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....p.b.....0..... .....@.. ....@.....O..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....<+.....$.....0..V.....~....~*...(+.....,5.(....&r...p(,....+...r...p(....%.....~*...(+.....-..~.....(....&*...0..!... .....~....~*...(-.....,~.....(....&*....0..\.....s.....~....r/..p(/.....,..(0.....~....(1...o2...&.r1..po2...&..o2...&..o2...&.o3...(.....*:..r]..p(.....*..0..\.....s.....~....r/..p(/.....,..(0.....~....(1...o2. ..&.ra..po2...&..o2...&..o2...&.o3...(.....*:..r]..p(.....*..0..\.....s.....~

C:\Users\user\AppData\Roaming\rNFzixmDCD.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\PAYMENT-ADVICE.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:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20220808\PowerShell_transcript.114127.7_bzaf+H.20220808134820.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):	5789
Entropy (8bit):	5.402519732955
Encrypted:	false
SSDEEP:	96:BZ8hUN7qDo1ZBZRhUN7qDo1ZkUasjZLhUN7qDo1Z/dJ88EZP:S
MD5:	FA3066E2A7181FE4FCD73C6FA873E08D
SHA1:	5AE4181CA9BF0D2AE329A53D55D4A5AFC8B491DE
SHA-256:	E6AD590BEEE4C89503729349387C0450AD683BA4FCDDA8C91A9186DE3C16E79B
SHA-512:	A6B16C791A237EF34D1BC22763444022FCF3CD5C73DBFCDAE55FF7A815E33366E2804DBB8E797C2AF1DD5861EFDB29F3C85232B8B39C96B5235F448749124BI 5
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220808134822..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 114127 (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\rNFzixmDCD.exe..Process ID: 2404..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: 20220808134822..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\rNFzixmDCD.exe..**********..Windows PowerShell transcript start..Start time: 20220808135226..Username: computer\user..RunAs User: computer\hard

C:\Windows\System32\drivers\etc\hosts

Process:	C:\Users\user\Desktop\PAYMENT-ADVICE.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	835
Entropy (8bit):	4.694294591169137
Encrypted:	false
SSDEEP:	24:QWDZh+ragzMZfuMMs1L/JU5fFCkK8T1rTt8:vDZhyoZWM9rU5fFcP
MD5:	6EB47C1CF858E25486E42440074917F2
SHA1:	6A63F93A95E1AE831C393A97158C526A4FA0FAAE
SHA-256:	9B13A3EA948A1071A81787AAC1930B89E30DF22CE13F8FF751F31B5D83E79FFB
SHA-512:	08437AB32E7E905EB11335E670CDD5D999803390710ED39CBC31A2D3F05868D5D0E5D051CCD7B06A85BB466932F99A220463D27FAC29116D241E8ADAC495FA F
Malicious:	**true**
Preview:	# Copyright (c) 1993-2009 Microsoft Corp...#..# This is a sample HOSTS file used by Microsoft TCP/IP for Windows...#..# This file contains the mappings of IP addresses to host names. Each..# entry should be kept on an individual line. The IP address should..# be placed in the first column followed by the corresponding host name...# The IP address and the host name should be separated by at least one..# space...#..# Additionally, comments (such as these) may be inserted on individual..# lines or following the machine name denoted by a '#' symbol...#..# For example:..#..# 102.54.94.97 rhino.acme.com # source server..# 38.25.63.10 x.acme.com # x client host....# localhost name resolution is handled within DNS itself...#.127.0.0.1 localhost..#.::1 localhost....127.0.0.1

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.481605845274099
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	PAYMENT-ADVICE.exe
File size:	1024000
MD5:	2d9f2c92d70a25ad42fe3602d7f932b1
SHA1:	ca8fb29bd419998b7f2da87c49f1eb7b2c0700a0
SHA256:	001709cadc8a0a856d91b9e3c9c0753ac8469d3c6cf2f532fdd53aedb3a268d6
SHA512:	8d71362c4074423ee1e8f48fb11332a0ba58add496ad65e0b83331f34029d58d9d347bb70b7f496c11ff9b6482a679389ceaff78b088d782936720e2cac8e163
SSDEEP:	12288:5CSXZj4rDO3Koc+FI64Ap+1MUo4p/L2R6hT/0yAEfirpHhOtfI/4eAwRXIbUDbL+:5CTFqZ+zJhT/0yAJrIfIAe9IbUDHDls
TLSH:	0125AD17AFA47604E4F75BB8DC2B686183F63819617EE3792E905C9F2DFA301D40162B
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....p.b.....0..... .....@.. .....@.....

File Icon

Icon Hash:	c68ce86ecc8c8ac8

Static PE Info

General

Entrypoint:	0x4ed116
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x62F070B8 [Mon Aug 8 02:11:04 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
mov bh, 1Dh
rol dword ptr [esi+ebp*2], 3Bh
or byte ptr [ecx], FFFFFFD9h
inc ebx
or eax, 130476DCh
imul ebp, dword ptr [ebx-3Bh], 17h
mov dl, 4Dh
xchg byte ptr [edx], bl
add eax, B81E4750h
in eax, dx
or byte ptr [esi], ah

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xed0c4	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xf0000	0xd4bc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xfe000	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

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xec494	0xec600	False	0.7465595666975146	data	7.612937074384405	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xf0000	0xd4bc	0xd600	False	0.2765405957943925	data	3.7577588509475435	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xfe000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

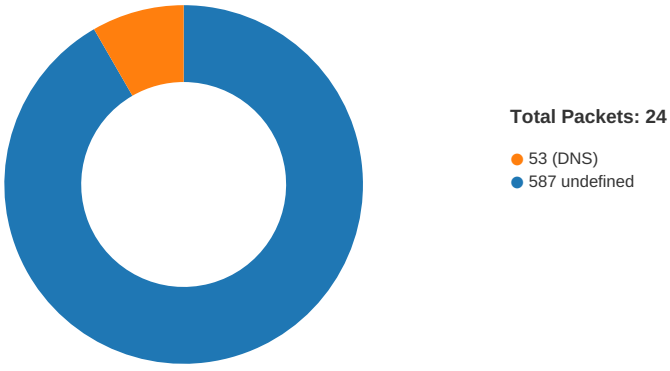
Name	RVA	Size	Type	Language	Country
RT_ICON	0xf0128	0x94a8	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0xf95e0	0x25a8	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0xfbb98	0x10a8	data		
RT_ICON	0xfcc50	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xfd0c8	0x3e	data		
RT_VERSION	0xfd118	0x3a0	data		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 13:48:39.032881021 CEST	49742	587	192.168.2.3	50.87.144.250
Aug 8, 2022 13:48:39.200524092 CEST	587	49742	50.87.144.250	192.168.2.3
Aug 8, 2022 13:48:39.203560114 CEST	49742	587	192.168.2.3	50.87.144.250
Aug 8, 2022 13:48:39.721107006 CEST	587	49742	50.87.144.250	192.168.2.3
Aug 8, 2022 13:48:39.721518993 CEST	49742	587	192.168.2.3	50.87.144.250
Aug 8, 2022 13:48:39.890348911 CEST	587	49742	50.87.144.250	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 13:48:39.890791893 CEST	49742	587	192.168.2.3	50.87.144.250
Aug 8, 2022 13:48:40.058064938 CEST	587	49742	50.87.144.250	192.168.2.3
Aug 8, 2022 13:48:40.095247984 CEST	49742	587	192.168.2.3	50.87.144.250
Aug 8, 2022 13:48:40.272490978 CEST	587	49742	50.87.144.250	192.168.2.3
Aug 8, 2022 13:48:40.272547007 CEST	587	49742	50.87.144.250	192.168.2.3
Aug 8, 2022 13:48:40.272586107 CEST	587	49742	50.87.144.250	192.168.2.3
Aug 8, 2022 13:48:40.272614002 CEST	587	49742	50.87.144.250	192.168.2.3
Aug 8, 2022 13:48:40.272774935 CEST	49742	587	192.168.2.3	50.87.144.250
Aug 8, 2022 13:48:40.274614096 CEST	587	49742	50.87.144.250	192.168.2.3
Aug 8, 2022 13:48:40.306319952 CEST	49742	587	192.168.2.3	50.87.144.250
Aug 8, 2022 13:48:40.473406076 CEST	587	49742	50.87.144.250	192.168.2.3
Aug 8, 2022 13:48:40.535706043 CEST	49742	587	192.168.2.3	50.87.144.250
Aug 8, 2022 13:48:43.449434996 CEST	49742	587	192.168.2.3	50.87.144.250
Aug 8, 2022 13:48:43.633064032 CEST	587	49742	50.87.144.250	192.168.2.3
Aug 8, 2022 13:48:43.636696100 CEST	49742	587	192.168.2.3	50.87.144.250
Aug 8, 2022 13:48:43.803231955 CEST	587	49742	50.87.144.250	192.168.2.3
Aug 8, 2022 13:48:43.804233074 CEST	49742	587	192.168.2.3	50.87.144.250
Aug 8, 2022 13:48:44.010504007 CEST	587	49742	50.87.144.250	192.168.2.3
Aug 8, 2022 13:48:44.029414892 CEST	587	49742	50.87.144.250	192.168.2.3
Aug 8, 2022 13:48:44.030265093 CEST	49742	587	192.168.2.3	50.87.144.250
Aug 8, 2022 13:48:44.196176052 CEST	587	49742	50.87.144.250	192.168.2.3
Aug 8, 2022 13:48:44.196244955 CEST	587	49742	50.87.144.250	192.168.2.3
Aug 8, 2022 13:48:44.196616888 CEST	49742	587	192.168.2.3	50.87.144.250
Aug 8, 2022 13:48:44.403211117 CEST	587	49742	50.87.144.250	192.168.2.3
Aug 8, 2022 13:48:44.463028908 CEST	587	49742	50.87.144.250	192.168.2.3
Aug 8, 2022 13:48:44.463500023 CEST	49742	587	192.168.2.3	50.87.144.250
Aug 8, 2022 13:48:44.629625082 CEST	587	49742	50.87.144.250	192.168.2.3
Aug 8, 2022 13:48:44.629676104 CEST	587	49742	50.87.144.250	192.168.2.3
Aug 8, 2022 13:48:44.630863905 CEST	49742	587	192.168.2.3	50.87.144.250
Aug 8, 2022 13:48:44.631122112 CEST	49742	587	192.168.2.3	50.87.144.250
Aug 8, 2022 13:48:44.631939888 CEST	49742	587	192.168.2.3	50.87.144.250
Aug 8, 2022 13:48:44.631995916 CEST	49742	587	192.168.2.3	50.87.144.250
Aug 8, 2022 13:48:44.796878099 CEST	587	49742	50.87.144.250	192.168.2.3
Aug 8, 2022 13:48:44.796945095 CEST	587	49742	50.87.144.250	192.168.2.3
Aug 8, 2022 13:48:44.797646999 CEST	587	49742	50.87.144.250	192.168.2.3
Aug 8, 2022 13:48:44.797688961 CEST	587	49742	50.87.144.250	192.168.2.3
Aug 8, 2022 13:48:44.798681974 CEST	587	49742	50.87.144.250	192.168.2.3
Aug 8, 2022 13:48:45.036043882 CEST	49742	587	192.168.2.3	50.87.144.250
Aug 8, 2022 13:48:45.189403057 CEST	587	49742	50.87.144.250	192.168.2.3
Aug 8, 2022 13:48:45.189567089 CEST	49742	587	192.168.2.3	50.87.144.250
Aug 8, 2022 13:50:18.638147116 CEST	49742	587	192.168.2.3	50.87.144.250
Aug 8, 2022 13:50:18.845161915 CEST	587	49742	50.87.144.250	192.168.2.3
Aug 8, 2022 13:50:19.189120054 CEST	587	49742	50.87.144.250	192.168.2.3
Aug 8, 2022 13:50:19.189923048 CEST	49742	587	192.168.2.3	50.87.144.250

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 13:48:38.640746117 CEST	55923	53	192.168.2.3	8.8.8.8
Aug 8, 2022 13:48:38.812478065 CEST	53	55923	8.8.8.8	192.168.2.3
Aug 8, 2022 13:48:38.851862907 CEST	57723	53	192.168.2.3	8.8.8.8
Aug 8, 2022 13:48:39.020261049 CEST	53	57723	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 8, 2022 13:48:38.640746117 CEST	192.168.2.3	8.8.8.8	0x9f59	Standard query (0)	mail.wayto gochile.com	A (IP address)	IN (0x0001)
Aug 8, 2022 13:48:38.851862907 CEST	192.168.2.3	8.8.8.8	0x6dcb	Standard query (0)	mail.wayto gochile.com	A (IP address)	IN (0x0001)

DNS Answers

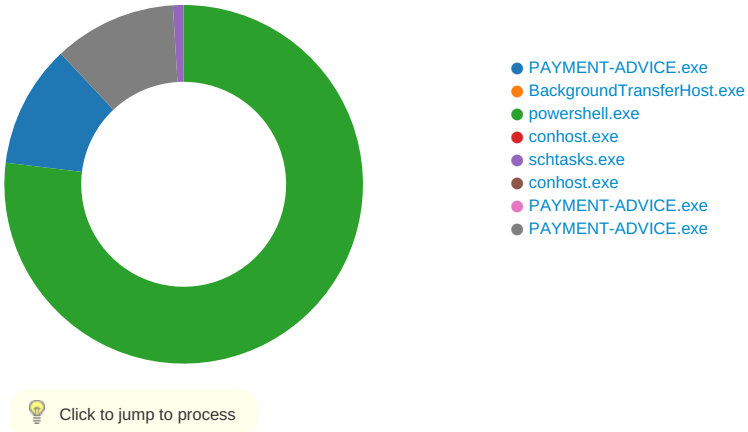
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 8, 2022 13:48:38.812478065 CEST	8.8.8.8	192.168.2.3	0x9f59	No error (0)	mail.waytogochile.com	waytogochile.com		CNAME (Canonical name)	IN (0x0001)
Aug 8, 2022 13:48:38.812478065 CEST	8.8.8.8	192.168.2.3	0x9f59	No error (0)	waytogochile.com		50.87.144.250	A (IP address)	IN (0x0001)
Aug 8, 2022 13:48:39.020261049 CEST	8.8.8.8	192.168.2.3	0x6dcb	No error (0)	mail.waytogochile.com	waytogochile.com		CNAME (Canonical name)	IN (0x0001)
Aug 8, 2022 13:48:39.020261049 CEST	8.8.8.8	192.168.2.3	0x6dcb	No error (0)	waytogochile.com		50.87.144.250	A (IP address)	IN (0x0001)
Aug 8, 2022 13:48:41.079037905 CEST	8.8.8.8	192.168.2.3	0xb186	No error (0)	windowsupdatebg.s.llnwi.net		178.79.225.0	A (IP address)	IN (0x0001)
Aug 8, 2022 13:48:41.079037905 CEST	8.8.8.8	192.168.2.3	0xb186	No error (0)	windowsupdatebg.s.llnwi.net		95.140.230.128	A (IP address)	IN (0x0001)
Aug 8, 2022 13:48:51.671696901 CEST	8.8.8.8	192.168.2.3	0x7f29	No error (0)	windowsupdatebg.s.llnwi.net		178.79.225.128	A (IP address)	IN (0x0001)
Aug 8, 2022 13:48:51.671696901 CEST	8.8.8.8	192.168.2.3	0x7f29	No error (0)	windowsupdatebg.s.llnwi.net		178.79.225.0	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Aug 8, 2022 13:48:39.721107006 CEST	587	49742	50.87.144.250	192.168.2.3	220-gator2004.hostgator.com ESMTP Exim 4.95 #2 Mon, 08 Aug 2022 06:48:39 -0500 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Aug 8, 2022 13:48:39.721518993 CEST	49742	587	192.168.2.3	50.87.144.250	EHLO 114127
Aug 8, 2022 13:48:39.890348911 CEST	587	49742	50.87.144.250	192.168.2.3	250-gator2004.hostgator.com Hello 114127 [102.129.143.3] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Aug 8, 2022 13:48:39.890791893 CEST	49742	587	192.168.2.3	50.87.144.250	STARTTLS
Aug 8, 2022 13:48:40.058064938 CEST	587	49742	50.87.144.250	192.168.2.3	220 TLS go ahead

Statistics

Behavior



System Behavior

Analysis Process: PAYMENT-ADVICE.exe PID: **5664**, Parent PID: **5356**

General

Target ID:	0
Start time:	13:48:04
Start date:	08/08/2022
Path:	C:\Users\user\Desktop\PAYMENT-ADVICE.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\PAYMENT-ADVICE.exe"
Imagebase:	0xe0000
File size:	1024000 bytes
MD5 hash:	2D9F2C92D70A25AD42FE3602D7F932B1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.288114287.0000000003665000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.288114287.0000000003665000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000000.00000002.288114287.0000000003665000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.287162918.00000000027CE000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.285145322.000000000255B000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Analysis Process: BackgroundTransferHost.exe PID: **1504**, Parent PID: **756**

General

Target ID:	2
Start time:	13:48:09
Start date:	08/08/2022
Path:	C:\Windows\System32\BackgroundTransferHost.exe
Wow64 process (32bit):	false
Commandline:	"BackgroundTransferHost.exe" -ServerName:BackgroundTransferHost.1
Imagebase:	0x7ff6d4350000
File size:	36864 bytes
MD5 hash:	02BA81746B929ECC9DB6665589B68335
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: **2404**, Parent PID: **5664**

General

Target ID:	4
Start time:	13:48:17
Start date:	08/08/2022
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\rNFzixmDCD.exe
Imagebase:	0x7ff73c930000
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	6D00CF06	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	6D00CF06	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_p02vnukr.mky.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6BE51E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_g4bf5eyu.ra0.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6BE51E60	CreateFileW
C:\Users\user\Documents\20220808	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6BE5BEFF	CreateDirectoryW
C:\Users\user\Documents\20220808\PowerShell_transcript.114127.7_bzaf+H.20220808134820.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6BE51E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_p02vnukr.mky.ps1	success or wait	1	6BE56A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_g4bf5eyu.ra0.psm1	success or wait	1	6BE56A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	16	19	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BDB5B28	unknown
unknown	35	21	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BDB5B28	unknown
unknown	56	16	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BDB5B28	unknown
unknown	72	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BDB5B28	unknown
unknown	80	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BDB5B28	unknown
unknown	89	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BDB5B28	unknown
unknown	97	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BDB5B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_p02vnukr.mky.ps1	0	1	31	1	success or wait	1	6BE51B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_g4bf5eyu.ra0.psm1	0	1	31	1	success or wait	1	6BE51B4F	WriteFile
C:\Users\user\Documents\20220808\PowerShell_transcript.114127.7_bzaf+H.20220808134820.txt	0	3	ff		success or wait	1	6BE51B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220808\PowerShell_transcript.114127.7_bzaf+H.20220808134820.txt	3	677	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 32 30 38 30 38 31 33 34 38 32 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 68 61 72 64 7a 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 31 31 34 31 32 37 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c 57 69	**********Windows PowerShell transcript startStart time: 20220808134822Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 114127 (Microsoft Windows NT 10.0.17134.0)Host Application: C:\Wi	success or wait	44	6BE51B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 73 14 00 00 18 00 00 00 fd 0e fd 04 12 0a 0e 0a fd 09 00 00 3f 01 6e 00 0a 00 fd 0e 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@es?n@	success or wait	1	6D2D76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 52 00 00 00 0e 00 20 00	H<@^L"My:R	success or wait	17	6D2D76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	17	6D2D76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	11	6D2D76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	00 08 00 03		success or wait	11	6D2D76FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1172	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 09 0c fd 00 54 01 40 00 fd 3e 40 01 fd 67 40 01 fd 01 40 00 fd 00 40 00 fd 00 00 00 56 01 00 00 48 01 00 00 58 01 00 00 5b 01 00 00 4e 54 00 01 48 54 00 01 fd 53 00 01 fd 53 00 01 68 54 00 01 fd 53 00 01 fd 53 00 01 fd 53 00 01 5c 01 00 00 00 54 00 01 02 54 00 01 40 58 00 01 3f 58 00 01 1c 54 00 01 fd 53 00 01 fd 53 00 01 1e 54 00 01 19 54 00 01 78 54 00 01 7a 54 00 01 fd 54 00 01 3d 4d 00 01 44 4d 00 01 3a 4d 00 01 22 4d 00 01 20 4d 00 01 21 4d 00 01 3b 4d 00 01 fd 44 00 01 fd 44 00 01 40 4d 00 01 3c 4d 00 01 24 4d 00 01 38 4d 00 01 3f 4d 00 01 42 4d 00 01 fd 44 00 01 6d 45 00 01 45 4d 00 01 fd 71 00 01 fd 71 00 01 fd 53 00 01 fd 25 00 01 fd 6e 00	T@>@g@@@VHX[NTHTSShTSSS\TT@X?XTSSTTxTzTT=MDM:M"MM!M;MDD@M<M$M8M?MBMDmEEMqqS%n	success or wait	11	6D2D76FC	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	6CFE5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CFE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CFE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CFE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CF403DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CFECA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CFECA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CFECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CF403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CF403DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CFE5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CFE5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CFE5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CFE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CF403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6CF403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CFE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CFE5705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6CFF1F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	22392	success or wait	1	6CFF203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CF403DE	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	6BE51B4F	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	6BE51B4F	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	6BE51B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6BE51B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6BE51B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6BE51B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6BE51B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6BE51B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6BE51B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	143	6BE51B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6BE51B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6BE51B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6CF403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CF403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CF403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CF403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CF403DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CFE5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CFE5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CFE5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CFE5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6BE51B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	6BE51B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	16	6BE51B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6BE51B4F	ReadFile

Analysis Process: conhost.exe PID: **5744**, Parent PID: **2404**

General

Target ID:	5
Start time:	13:48:17
Start date:	08/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
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: schtasks.exe PID: **5416**, Parent PID: **5664**

General

Target ID:	6
Start time:	13:48:18
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\rNFzixmDCD" /XML "C:\Users\user\AppData\Local\Temp\tmpA427.tmp
Imagebase:	0x900000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpA427.tmp	unknown	2	success or wait	1	90AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpA427.tmp	unknown	1598	success or wait	1	90ABD9	ReadFile

Analysis Process: conhost.exe PID: **4480**, Parent PID: **5416**

General

Target ID:	7
Start time:	13:48:22
Start date:	08/08/2022

Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
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: PAYMENT-ADVICE.exe PID: **3156**, Parent PID: **5664**

General

Target ID:	8
Start time:	13:48:24
Start date:	08/08/2022
Path:	C:\Users\user\Desktop\PAYMENT-ADVICE.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\PAYMENT-ADVICE.exe
Imagebase:	0x80000
File size:	1024000 bytes
MD5 hash:	2D9F2C92D70A25AD42FE3602D7F932B1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: PAYMENT-ADVICE.exe PID: **1504**, Parent PID: **5664**

General

Target ID:	9
Start time:	13:48:24
Start date:	08/08/2022
Path:	C:\Users\user\Desktop\PAYMENT-ADVICE.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\PAYMENT-ADVICE.exe
Imagebase:	0x800000
File size:	1024000 bytes
MD5 hash:	2D9F2C92D70A25AD42FE3602D7F932B1
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: 00000009.00000000.280352342.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000009.00000000.280352342.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000009.00000000.280352342.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000002.506133681.0000000002E71000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000009.00000002.506133681.0000000002E71000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D00CF06	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	6D00CF06	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\System32\drivers\etc\hosts	824	11	0d 0a 31 32 37 2e 30 2e 30 2e 31	127.0.0.1	success or wait	1	6BE51B4F	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	6CFE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CFE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CF403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CFECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CF403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CF403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CF403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CF403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CFE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CFE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6BE51B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6BE51B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6BE51B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\05b98e77-fe4c-4961-9081-bc8c3f45dec3	unknown	4096	success or wait	1	6BE51B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6BE51B4F	ReadFile

Disassembly

No disassembly