ID: 756110
Sample Name: SHIPMENT DOCUMENTS.exe
Cookbook: default.jbs
Time: 16:42:18
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

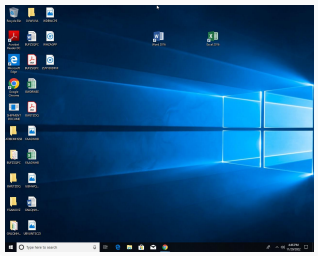
Windows Analysis Report

SHIPMENT DOCUMENTS.exe

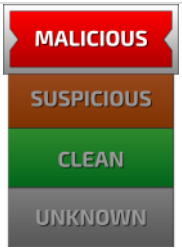
Overview

General Information

Sample Name:	SHIPMENT DOCUMENTS.exe
Analysis ID:	756110
MD5:	12dc06d3034a17..
SHA1:	9b68ae25498a12.
SHA256:	91826efe412b5c..
Tags:	AgentTesla exe
Infos:	



Detection



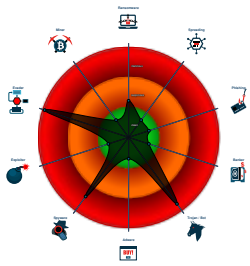
AgentTesla

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Sigma detected: Scheduled temp fil…
- Multi AV Scanner detection for drop…
- 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…
- .NET source code references suspic…
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w10x64**
- SHIPMENT DOCUMENTS.exe (PID: 3192 cmdline: C:\Users\user\Desktop\SHIPMENT DOCUMENTS.exe MD5: 12DC06D3034A17BE7A70A4AA45EDCE8D)
  - schtasks.exe (PID: 5900 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\cnWCiicEpxW" /XML "C:\Users\user\AppData\Local\Temp\tmp2A80.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 1632 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - SHIPMENT DOCUMENTS.exe (PID: 3244 cmdline: {path} MD5: 12DC06D3034A17BE7A70A4AA45EDCE8D)
- cnWCiicEpxW.exe (PID: 4444 cmdline: C:\Users\user\AppData\Roaming\cnWCiicEpxW.exe MD5: 12DC06D3034A17BE7A70A4AA45EDCE8D)
  - schtasks.exe (PID: 5740 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\cnWCiicEpxW" /XML "C:\Users\user\AppData\Local\Temp\tmpC7C9.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4512 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cnWCiicEpxW.exe (PID: 3132 cmdline: {path} MD5: 12DC06D3034A17BE7A70A4AA45EDCE8D)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Host": "mail.southernboilers.org",
  "Username": "info@southernboilers.org",
  "Password": "Sksmoke2018#"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000014.00000000.301553016.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000014.00000000.301553016.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000014.00000000.301553016.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x31ccf:$a13: get_DnsResolver • 0x303d4:$a20: get_LastAccessed • 0x326dc:$a27: set_InternalServerPort • 0x32a11:$a30: set_GuidMasterKey • 0x304e6:$a33: get_Clipboard • 0x304f4:$a34: get_Keyboard • 0x318ba:$a35: get_ShiftKeyDown • 0x318cb:$a36: get_AltKeyDown • 0x30501:$a37: get_Password • 0x31015:$a38: get_PasswordHash • 0x32110:$a39: get_DefaultCredentials
0000001B.00000002.528419495.0000000003164000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
0000001B.00000002.525674867.0000000003111000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 16 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
20.0.SHIPMENT DOCUMENTS.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
20.0.SHIPMENT DOCUMENTS.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
20.0.SHIPMENT DOCUMENTS.exe.400000.0.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x349c0:$s10: logins • 0x34440:$s11: credential • 0x306e6:$g1: get_Clipboard • 0x306f4:$g2: get_Keyboard • 0x30701:$g3: get_Password • 0x31aaa:$g4: get_CtrlKeyDown • 0x31aba:$g5: get_ShiftKeyDown • 0x31acb:$g6: get_AltKeyDown
20.0.SHIPMENT DOCUMENTS.exe.400000.0.unpack	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x31ecf:$a13: get_DnsResolver • 0x305d4:$a20: get_LastAccessed • 0x328dc:$a27: set_InternalServerPort • 0x32c11:$a30: set_GuidMasterKey • 0x306e6:$a33: get_Clipboard • 0x306f4:$a34: get_Keyboard • 0x31aba:$a35: get_ShiftKeyDown • 0x31acb:$a36: get_AltKeyDown • 0x30701:$a37: get_Password • 0x31215:$a38: get_PasswordHash • 0x32310:$a39: get_DefaultCredentials
0.2.SHIPMENT DOCUMENTS.exe.3d715a0.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 15 entries				

Sigma Signatures

Persistence and Installation Behavior

Sigma detected: Scheduled temp file as task from temp location

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

May check the online IP address of the machine

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

Data Obfuscation

.NET source code contains potential unpacker

.NET source code contains method to dynamically call methods (often used by packers)

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

.NET source code references suspicious native API functions

Injects a PE file into a foreign processes

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)

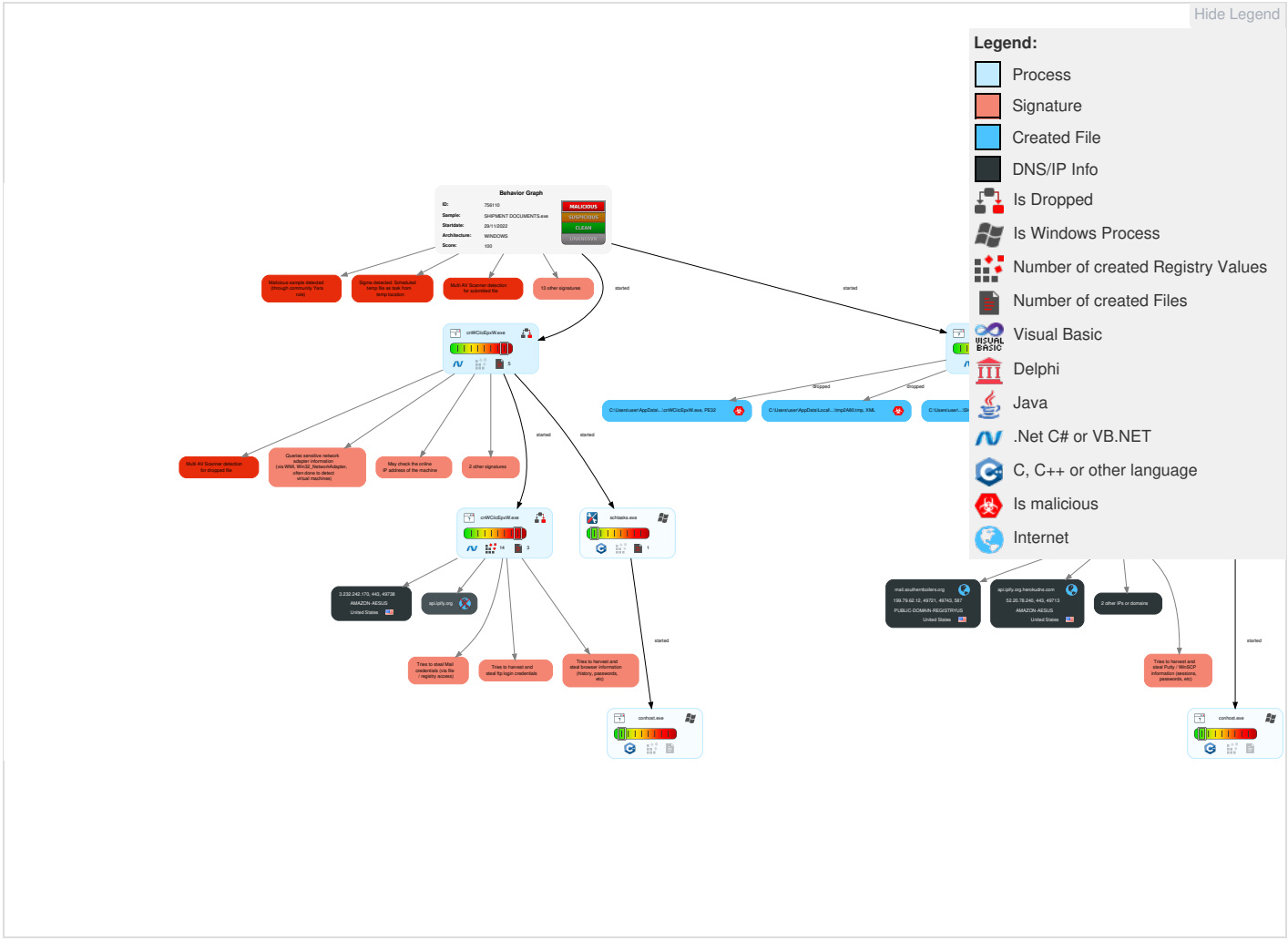
Remote Access Functionality

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 Disable or Modify Tools	2 OS Credential Dumping	1 File and Directory Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Native API	Boot or Logon Initialization Scripts	1 Scheduled Task/Job	1 Deobfuscate/Decode Files or Information	1 Credentials in Registry	1 1 4 System Information Discovery	Remote Desktop Protocol	2 Data from Local System	Exfiltration Over Bluetooth	1 1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Scheduled Task/Job	Logon Script (Windows)	Logon Script (Windows)	2 Obfuscated Files or Information	Security Account Manager	1 Query Registry	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	2 3 Software Packing	NTDS	3 1 1 Security Software Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Masquerading	LSA Secrets	1 Process Discovery	SSH	Keylogging	Data Transfer Size Limits	2 3 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 3 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	1 3 1 Virtualization/Sandbox Evasion	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 1 1 Process Injection	DCSync	1 Application Window Discovery	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	Indicator Removal from Tools	Proc Filesystem	1 Remote System 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 Network Configuration Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

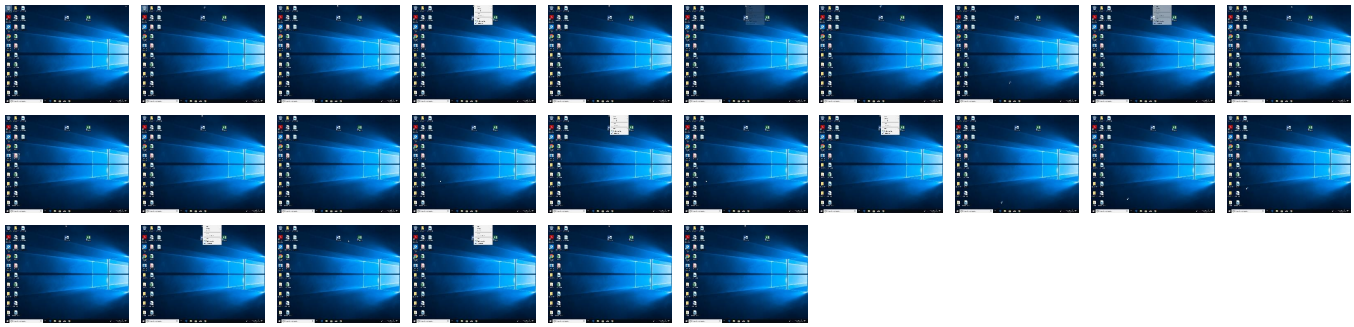
Behavior Graph



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
SHIPMENT DOCUMENTS.exe	36%	Virustotal		Browse
SHIPMENT DOCUMENTS.exe	32%	ReversingLabs	Win32.Trojan.Wore flint	
SHIPMENT DOCUMENTS.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\cnWCiicEpxW.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\cnWCiicEpxW.exe	32%	ReversingLabs	Win32.Trojan.Wore flint	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
20.0.SHIPMENT DOCUMENTS.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
mail.southernboilers.org	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.certplus.com/CRL/class3.crl0	0%	URL Reputation	safe	
http://www.e-me.lv/repository0	0%	URL Reputation	safe	
http://www.acabogacia.org/doc0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://ocsp.suscerte.gob.ve0	0%	URL Reputation	safe	
http://www.postsignum.cz/crl/psrootqca2.crl02	0%	URL Reputation	safe	
http://crl.dhimyotis.com/certignarootca.crl0	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://www.pkioverheid.nl/policies/root-policy0	0%	URL Reputation	safe	
http://www.suscerte.gob.ve/lcr0#	0%	URL Reputation	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://postsignum.ttc.cz/crl/psrootqca2.crl0	0%	URL Reputation	safe	
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	0%	URL Reputation	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://ca.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://crl1.comsign.co.il/crl/comsignglobalrootca.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3P.crl0	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.suscerte.gob.ve/dpc0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class2.crl0	0%	URL Reputation	safe	
http://www.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://www.defence.gov.au/pki0	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sk.ee/cps/0	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://policy.camerfirma.com0	0%	URL Reputation	safe	
http://www.ssc.lt/cps03	0%	URL Reputation	safe	
http://ocsp.pki.gva.es0	0%	URL Reputation	safe	
http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf0?	0%	URL Reputation	safe	
http://ca.mtin.es/mtin/ocsp0	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://web.ncdc.gov.sa/crl/nrcacomb1.crl0	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.dnie.es/dpc0	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://ca.mtin.es/mtin/DPCyPoliticas0	0%	URL Reputation	safe	
http://www.globaltrust.info0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3TS.crl0	0%	URL Reputation	safe	
http://crl.microsoft.	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://ac.economia.gob.mx/last.crl0G	0%	URL Reputation	safe	
http://https://www.catcert.net/verarrel	0%	URL Reputation	safe	
http://www.disig.sk/ca0f	0%	URL Reputation	safe	
http://www.globaltrust.info0=	0%	Avira URL Cloud	safe	
http://www.sk.ee/juur/crl/0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersignroot.crl0	0%	URL Reputation	safe	
http://crl.xrampsecurity.com/XGCA.crl0	0%	URL Reputation	safe	
http://certs.oati.net/repository/OATICA2.crl0	0%	URL Reputation	safe	
http://crl.oces.trust2408.com/oces.crl0	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.quovadis.bm0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-a/cacrl.crl0	0%	URL Reputation	safe	
http://certs.oaticerts.com/repository/OATICA2.crl	0%	URL Reputation	safe	
http://www.trustdst.com/certificates/policy/ACES-index.html0	0%	URL Reputation	safe	
http://certs.oati.net/repository/OATICA2.crt0	0%	URL Reputation	safe	
http://https://9psarY6l5Bj.org	0%	Avira URL Cloud	safe	
http://mail.southernboilers.org	0%	Avira URL Cloud	safe	
http://bvQtmz.com	0%	Avira URL Cloud	safe	
http://www.accv.es00	0%	URL Reputation	safe	
http://www.pkioverheid.nl/policies/root-policy-G20	0%	URL Reputation	safe	
http://https://www.netlock.net/docs	0%	URL Reputation	safe	
http://www.e-trust.be/CPS/QNcerts	0%	URL Reputation	safe	
http://ocsp.ncdc.gov.sa0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignCA.crl0	0%	URL Reputation	safe	
http://trustcenter-crl.certificat2.com/Keynectis/KEYNECTIS_ROOT_CA.crl0	0%	URL Reputation	safe	
http://web.ncdc.gov.sa/crl/nrcaparta1.crl	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.southernboilers.org	199.79.62.12	true	false	• 0%, Virustotal, Browse	unknown
api.ipify.org.herokudns.com	52.20.78.240	true	false		unknown
windowsupdatebg.s.llnwi.net	178.79.242.0	true	false		unknown
api.ipify.org	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	SHIPMENT DOCUMENTS.exe, 00000014.00000002.522417697.0000000002EF1000.00000004.00000800.00020000.00000000.sdmp, cnWCiicEpxW.exe, 0000001B.00000002.525674867.0000000003111000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.certplus.com/CRL/class3.crl0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.407487472.00000000070CC000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.e-me.lv/repository0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.398450527.0000000007136000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.acabogacia.org/doc0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.407487472.00000000070CC000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.398941782.00000000065B9000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.403651123.00000000065E4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.chambersign.org/chambersroot.crl0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.398941782.00000000065B9000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.403651123.00000000065E4000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000002.546353573.00000000065ED000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ocsp.suscerte.gob.ve0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.407487472.00000000070CC000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.398696766.0000000007129000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.postsignum.cz/crl/psrootqca2.crl02	SHIPMENT DOCUMENTS.exe, 00000014.00000003.398941782.00000000065B9000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.403942163.00000000065CD000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://mail.southernboilers.org	SHIPMENT DOCUMENTS.exe, 00000014.00000002.533736666.00000000031E6000.00000004.00000800.00020000.00000000.sdmp, cnWCiicExW.exe, 0000001B.00000002.534528527.00000000033EF000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.dhimyotis.com/certignarootca.crl0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.398450527.0000000007136000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://sertifikati.ca.posta.rs/crl/PostaCARoot.crl0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.407487472.00000000070CC000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.chambersign.org1	SHIPMENT DOCUMENTS.exe, 00000014.00000003.398941782.00000000065B9000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.403651123.00000000065E4000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.398696766.00000000007129000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000002.546353573.00000000065ED000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.pkioverheid.nl/policies/root-policy0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.398941782.00000000065B9000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.403853962.00000000065DA000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://repository.swisssign.com/0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.400439346.00000000065EF000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.407487472.00000000070CC000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.401332216.00000000065F2000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.398941782.00000000065B9000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.403942163.00000000065CD000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers	SHIPMENT DOCUMENTS.exe, 00000000.00000002.315590285.0000000006E62000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.pki.admin.ch/polic	SHIPMENT DOCUMENTS.exe, 00000014.00000003.403712232.00000000065F1000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000002.546377934.00000000065F0000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.suscerte.gob.ve/lcr0#	SHIPMENT DOCUMENTS.exe, 00000014.00000003.407487472.00000000070CC000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.398696766.0000000007129000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ca2.mtin.es/mtin/crl/MTINAutoridadRaiz0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.400439346.00000000065EF000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.401332216.00000000065F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.ssc.lt/root-c/cacrl.crl0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.398450527.0000000007136000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://postsignum.ttc.cz/crl/psrootqca2.crl0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.398941782.00000000065B9000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.403942163.00000000065CD000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	SHIPMENT DOCUMENTS.exe, 00000014.00000003.398941782.00000000065B9000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.403651123.00000000065E4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ca.disig.sk/ca/crl/ca_disig.crl0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.400439346.00000000065EF000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.403696848.00000000065EF000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl1.comsign.co.il/crl/comsignglobalrootca.crl0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.398941782.00000000065B9000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.407915366.00000000065B9000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.certplus.com/CRL/class3P.crl0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.398450527.0000000007136000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	SHIPMENT DOCUMENTS.exe, 00000000.00000002.315590285.0000000006E62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	SHIPMENT DOCUMENTS.exe, 00000000.00000002.315590285.0000000006E62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.suscerte.gob.ve/dpc0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.407487472.00000000070CC000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.398696766.0000000007129000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.certeurope.fr/reference/root2.crl0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.400776216.000000000660B000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.408594188.000000000660D000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.certplus.com/CRL/class2.crl0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.398941782.00000000065B9000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.403651123.00000000065E4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.disig.sk/ca/crl/ca_disig.crl0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.400439346.00000000065EF000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.403696848.00000000065EF000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://eca.hinet.net/repository/Certs/IssuedToThisCA.p7b05	SHIPMENT DOCUMENTS.exe, 00000014.00000003.398941782.00000000065B9000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.403651123.00000000065E4000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.defence.gov.au/pki0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.403880249.00000000065E1000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.398941782.00000000065B9000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.406958224.00000000065E3000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	SHIPMENT DOCUMENTS.exe, 00000000.00000002.315590285.0000000006E62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sk.ee/cps/0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.401258901.0000000007125000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.globaltrust.info0=	SHIPMENT DOCUMENTS.exe, 00000014.00000003.398696766.0000000007129000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.anf.es	SHIPMENT DOCUMENTS.exe, 00000014.00000003.400439346.00000000065EF000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.401332216.00000000065F2000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_1_0.pdf09	SHIPMENT DOCUMENTS.exe, 00000014.00000003.398941782.00000000065B9000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.403942163.00000000065CD000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.urwpp.deDPlease	SHIPMENT DOCUMENTS.exe, 00000000.00000002.315590285.0000000006E62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	SHIPMENT DOCUMENTS.exe, 00000000.00000002.315590285.0000000006E62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SHIPMENT DOCUMENTS.exe, 00000000.00000002.305232047.0000000002CA1000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000002.522417697.0000000002EF1000.00000004.00000800.00020000.00000000.sdmp, cnWCiicEpxW.exe, 00000015.00000002.415707967.0000000002B71000.00000004.00000800.00020000.00000000.sdmp, cnWCiicEpxW.exe, 0000001B.00000002.525674867.0000000003111000.00000004.00000800.00020000.00000000.sdmp	false		high
http://pki.registradores.org/normativa/index.htm0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.398450527.0000000007136000.00000004.00000800.00020000.00000000.sdmp	false		high
http://cps.root-x1.letsencrypt.org0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.393081850.00000000010F2000.00000004.00000020.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000002.518974908.00000000010F2000.00000004.00000020.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000002.516536811.000000000107D000.00000004.00000020.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.393347400.0000000006586000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000002.533736666.00000000031E6000.00000004.00000800.00020000.00000000.sdmp, cnWCiicEpxW.exe, 0000001B.00000002.520315185.00000000013A0000.00000004.00000020.00020000.00000000.sdmp, cnWCiicEpxW.exe, 0000001B.00000002.534582730.00000000033F5000.00000004.00000800.00020000.00000000.sdmp, cnWCiicEpxW.exe, 0000001B.00000002.520153626.0000000001396000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://policy.camerfirma.com0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.400439346.00000000065EF000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.408538851.0000000006603000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.401332216.00000000065F2000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.398941782.00000000065B9000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.403651123.00000000065E4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.ssc.lt/cps03	SHIPMENT DOCUMENTS.exe, 00000014.00000003.400439346.00000000065EF000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.401258901.0000000007125000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.401332216.00000000065F2000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.398450527.0000000007136000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ocsp.pki.gva.es0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.398941782.00000000065B9000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.403942163.00000000065CD000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

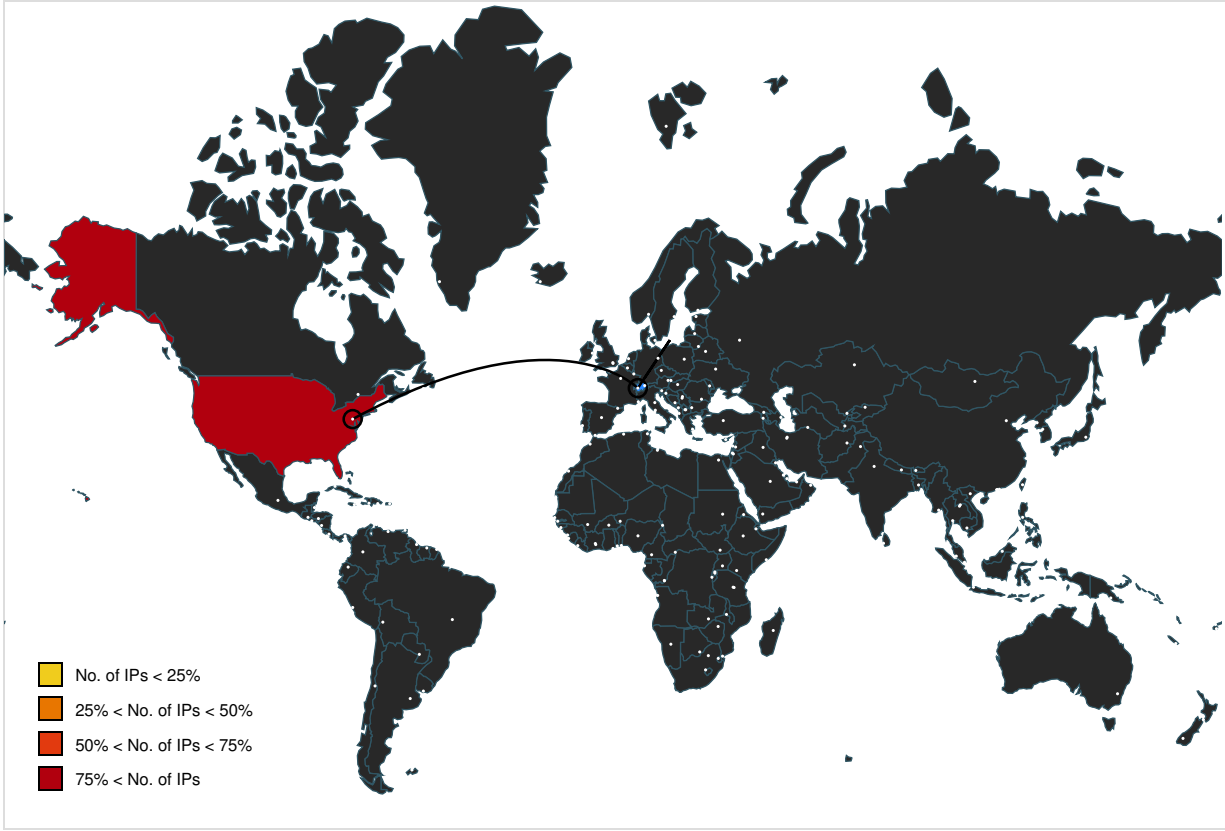
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.anf.es/es/address-direccion.html	SHIPMENT DOCUMENTS.exe, 00000014.00000003.400439346.00000000065EF000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.401332216.00000000065F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.anf.es/address/)1(0&	SHIPMENT DOCUMENTS.exe, 00000014.00000003.398836058.00000000065AD000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.407868660.00000000065AE000.00000004.00000800.00020000.00000000.sdmp	false		high
http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf0?	SHIPMENT DOCUMENTS.exe, 00000014.00000003.398941782.00000000065B9000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.403651123.00000000065E4000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.407915366.00000000065B9000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://bvQtmz.com	cnWCiicEpxW.exe, 0000001B.00000002.525674867.0000000003111000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ca.mtin.es/mtin/ocsp0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.400439346.00000000065EF000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.401332216.00000000065F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://cps.letsencrypt.org0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.392950428.00000000010D7000.00000004.00000020.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000002.516536811.000000000107D000.00000004.00000020.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.393347400.00000000006586000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000002.533736666.00000000031E6000.00000004.00000800.00020000.00000000.sdmp, cnWCiicEpxW.exe, 0000001B.00000002.520315185.00000000013A0000.00000004.00000020.00020000.00000000.sdmp, cnWCiicEpxW.exe, 0000001B.00000002.534582730.00000000033F5000.00000004.00000800.00020000.00000000.sdmp, cnWCiicEpxW.exe, 0000001B.00000002.519279531.000000000135D000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.ssc.lt/root-b/cacrl.crl0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.401258901.0000000007125000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://web.ncdc.gov.sa/crl/nrcacomb1.crl0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.403880249.00000000065E1000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.398941782.00000000065B9000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.406958224.00000000065E3000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.certicamara.com/dpc/0Z	SHIPMENT DOCUMENTS.exe, 00000014.00000003.398836058.00000000065AD000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.407868660.00000000065AE000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.uce.gub.uy/informacion-tecnica/politicas/cp_acrn.pdf0G	SHIPMENT DOCUMENTS.exe, 00000014.00000003.398941782.00000000065B9000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.403651123.00000000065E4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.pki.wellsfargo.com/wsprca.crl0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.408437609.00000000070C4000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://wwww.certigna.fr/autorites/0m	SHIPMENT DOCUMENTS.exe, 00000014.00000003.398450527.0000000007136000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.dnie.es/dpc0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.398941782.00000000065B9000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.407915366.00000000065B9000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.ica.co.il/repository/cps/PersonalID_Practice_Statement.pdf0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.401258901.0000000007125000.00000004.00000800.00020000.00000000.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	SHIPMENT DOCUMENTS.exe, 00000014.00000002.522417697.0000000002EF1000.00000004.00000800.00020000.00000000.sdmp, cnWCiicExpxW.exe, 0000001B.00000002.525674867.0000000003111000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ca.mtin.es/mtin/DPCyPoliticas0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.400439346.00000000065EF000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.401332216.00000000065F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.anf.es/AC/ANFServerCA.crl0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.398836058.00000000065AD000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.407868660.00000000065AE000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.globaltrust.info0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.398696766.0000000007129000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://certificates.starfieldtech.com/repository/1604	SHIPMENT DOCUMENTS.exe, 00000014.00000003.400439346.00000000065EF000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.401332216.00000000065F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://acedicom.edicomgroup.com/doc0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.408437609.00000000070C4000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.certplus.com/CRL/class3TS.crl0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.401023380.000000000662C000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.408697131.0000000006630000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.microsoft.	SHIPMENT DOCUMENTS.exe, 00000014.00000002.546472929.0000000006603000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://crl.anf.es/AC/ANFServerCA.crl0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.398836058.00000000065AD000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.407868660.00000000065AE000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.coml	SHIPMENT DOCUMENTS.exe, 00000000.00000002.315590285.0000000006E62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.certeurope.fr/reference/pc-root2.pdf0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.400776216.000000000660B000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.408594188.000000000660D000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://9psarY6l5Bj.org	cnWCiicEpxW.exe, 0000001B.00000002.528419495.0000000003164000.00000004.00000800.00020000.00000000.sdmp, cnWCiicEpxW.exe, 0000001B.00000002.534484751.00000000033EB000.00000004.00000800.00020000.00000000.sdmp, cnWCiicEpxW.exe, 0000001B.00000002.534582730.00000000033F5000.00000004.00000800.00020000.00000000.sdmp, cnWCiicEpxW.exe, 0000001B.00000002.533917798.00000000033AA000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ac.economia.gob.mx/last.crl0G	SHIPMENT DOCUMENTS.exe, 00000014.00000003.398696766.0000000007129000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	SHIPMENT DOCUMENTS.exe, 00000000.00000002.315590285.0000000006E62000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.catcert.net/verarrel	SHIPMENT DOCUMENTS.exe, 00000014.00000003.398450527.0000000007136000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.disig.sk/ca0f	SHIPMENT DOCUMENTS.exe, 00000014.00000003.400439346.00000000065EF000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.403696848.00000000065EF000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1.crt0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.398941782.00000000065B9000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.403942163.00000000065CD000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.e-szigno.hu/RootCA.crl	SHIPMENT DOCUMENTS.exe, 00000014.00000003.398450527.0000000007136000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sk.ee/juur/crl/0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.401258901.0000000007125000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.chambersign.org/chambersignroot.crl0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.398696766.0000000007129000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.xrampsecurity.com/XGCA.crl0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.408011972.00000000065C1000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.398941782.00000000065B9000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.407915366.00000000065B9000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://certs.oati.net/repository/OATICA2.crl0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.400439346.00000000065EF000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.401332216.00000000065F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.oces.trust2408.com/oces.crl0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.400439346.00000000065EF000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.401332216.00000000065F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.quovadis.bm0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.407487472.00000000070CC000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://eca.hinet.net/repository0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.398941782.00000000065B9000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.403651123.00000000065E4000.00000004.00000800.00020000.00000000.sdmp	false		high
http://crl.ssc.lt/root-a/cacrl.crl0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.400439346.00000000065EF000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.401332216.00000000065F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://certs.oaticerts.com/repository/OATICA2.crl	SHIPMENT DOCUMENTS.exe, 00000014.00000003.400439346.00000000065EF000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.401332216.00000000065F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.trustdst.com/certificates/policy/ACES-index.html0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.401258901.0000000007125000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://certs.oati.net/repository/OATICA2.crt0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.400439346.00000000065EF000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.401332216.00000000065F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.accv.es00	SHIPMENT DOCUMENTS.exe, 00000014.00000003.398941782.00000000065B9000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.403942163.00000000065CD000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.pkioverheid.nl/policies/root-policy-G20	SHIPMENT DOCUMENTS.exe, 00000014.00000003.400439346.00000000065EF000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.401332216.00000000065F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.netlock.net/docs	SHIPMENT DOCUMENTS.exe, 00000014.00000003.407915366.00000000065B9000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.pki.admin.ch/policy/CPS_2_16_756_1_17_3_21_1.pdf0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.400439346.00000000065EF000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.e-trust.be/CPS/QNcerts	SHIPMENT DOCUMENTS.exe, 00000014.00000003.398450527.0000000007136000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.398941782.00000000065B9000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.403651123.00000000065E4000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.407915366.00000000065B9000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000002.546037308.00000000065B9000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ocsp.ncdc.gov.sa0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.403880249.00000000065E1000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.398941782.00000000065B9000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.406958224.00000000065E3000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designersG	SHIPMENT DOCUMENTS.exe, 00000000.00000002.315590285.0000000006E62000.00000004.00000800.00020000.00000000.sdmp	false		high
http://fedir.comsign.co.il/crl/ComSignCA.crl0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.408437609.00000000070C4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	SHIPMENT DOCUMENTS.exe, 00000000.00000002.315590285.0000000006E62000.00000004.00000800.00020000.00000000.sdmp	false		high
http://trustcenter-crl.certificat2.com/Keynectis/KEYNECTIS_ROOT_CA.crl0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.398941782.00000000065B9000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.403942163.00000000065CD000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://web.ncdc.gov.sa/crl/nrcaparta1.crl	SHIPMENT DOCUMENTS.exe, 00000014.00000003.403880249.00000000065E1000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.398941782.00000000065B9000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.406958224.00000000065E3000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.datev.de/zertifikat-policy-int0	SHIPMENT DOCUMENTS.exe, 00000014.00000003.400439346.00000000065EF000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.401332216.00000000065F2000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.398941782.00000000065B9000.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.408391129.00000000065D800.00000004.00000800.00020000.00000000.sdmp, SHIPMENT DOCUMENTS.exe, 00000014.00000003.403942163.00000000065CD000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	SHIPMENT DOCUMENTS.exe, 00000000.00000002.315590285.0000000006E62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
199.79.62.12	mail.southernboilers.org	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false
3.232.242.170	unknown	United States		14618	AMAZON-AESUS	false
52.20.78.240	api.ipify.org.herokudns.com	United States		14618	AMAZON-AESUS	false

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756110
Start date and time:	2022-11-29 16:42:18 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 46s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SHIPMENT DOCUMENTS.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	34
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.spyw.evad.winEXE@12/7@6/3
EGA Information:	• Successful, ratio: 100%

HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, dllhost.exe, BackgroundTransferHost.exe, HxTsr.exe, RuntimeBroker.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 178.79.242.0, 209.197.3.8, 20.82.154.241, 20.82.228.9, 104.214.104.116, 20.65.78.40
- Excluded domains from analysis (whitelisted): www.bing.com, asf-ris-prod-scus-azsc.southcentralus.cloudapp.azure.com, fs.microsoft.com, eudb.ris.api.iris.microsoft.com, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, asf-ris-prod-eus2-azsc.eastus2.cloudapp.azure.com, arc.msn.com, wu-bg-shim.trafficmanager.net, neus1c-displaycatalog.frontdoor.bigcatalog.commerce.microsoft.com, ris.api.iris.microsoft.com, rp-consumer-prod-displaycatalog-geomap.trafficmanager.net, login.live.com, store-images.s-microsoft.com, neus2c-displaycatalog.frontdoor.bigcatalog.commerce.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, cdn.onenote.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, ris-prod-eudb.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size 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
16:44:15	API Interceptor	377x Sleep call for process: SHIPMENT DOCUMENTS.exe modified
16:44:29	Task Scheduler	Run new task: cnWCiicEpxW path: C:\Users\user\AppData\Roaming\cnWCiicEpxW.exe
16:44:49	API Interceptor	54x Sleep call for process: cnWCiicEpxW.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\SHIPMENT DOCUMENTS.exe

File Type:	Microsoft Cabinet archive data, Windows 2000/XP setup, 62919 bytes, 1 file, at 0x2c +A "authroot.stl", number 1, 6 datablocks, 0x1 compression
Category:	dropped
Size (bytes):	62919
Entropy (8bit):	**7.995280921994772**
Encrypted:	**true**
SSDEEP:	1536:d+OfVxHl7Wyf11lYom3xQcRVOtPHwQV4rP6Ji7:d+OxHxJlZcuPt4b6q
MD5:	3DCF580A93972319E82CAFBC047D34D5
SHA1:	8528D2A1363E5DE77DC3B1142850E51EAD0F4B6B
SHA-256:	40810E31F1B69075C727E6D557F9614D5880112895FF6F4DF1767E87AE5640D1
SHA-512:	98384BE7218340F95DAE88D1CB865F23A0B4E12855BEB6E74A3752274C9B4C601E493864DB777BCA677A370D0A9DBFFD68D94898A82014537F3A801CCE839C4
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF.....,.....I.....Q.....GU.\ .authroot.stl..O..5..CK..<Tk...c_.d....A.K...+.d.-;%.BJII!.QIR..$t)Kd.-QQ*...g.....^..~|N=...y....{. .4{...W....b.i...j.I.....1:..b\.0.... .Ait.2t.....w.%.&.",tL_...4.8L[G..;.57....AT.k.....V..K.....(....mzS...G....r.".=H.?>.....x&...S%....X.M^.j...A..x.9`.9...A../.s..#.4#.....ld.w..B....s.8..(...dj....=L.)..s.d.]NxQX8 ....stV#.K.'7.tH..9u~.2..!..2./.....!..9C../...mP $..../y.....@p.6.}.`...5. 0r.w...@(.. .Q....)g.....m..z*.8rR..).].T9r<.L....0..`.....c.....;-.g...;.wk.).....i..c5.....{v.u...AS..=.....&.:... .....+..P.N..9..EAQ.V.$s.....B.`.Mfe..8.....$...y-.q9J.....W...2.Q8...O.....i..@\^.=X..dG$.M..#=....m.h..{9.'...-.v..Z...!....z.....N....i..^.,.....d...%Xa~q.@D|0...Y.m..... ...&d.4..A..{t=...../.t.3._.....?-.....uroP?.d.Z..S..{...$.i....X..$.O..4..N.)....U.Z..P....X,.... ...Lg..35..W..s.!c...Ap.].P..8..M..W.....U.,..m.u..|=.m1..~..!..b...._.

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

Process:	C:\Users\user\Desktop\SHIPMENT DOCUMENTS.exe
File Type:	data
Category:	modified
Size (bytes):	290
Entropy (8bit):	2.9611813546708383
Encrypted:	false
SSDEEP:	6:kKAJNzlNiN+SkQlPlEGYRMY9z+4KlDA3RUe/:YDVkPlE99SNxAhUe/
MD5:	37EE5D1705C30E983C3B068D6F6F6004
SHA1:	94570FA7C66A5A4199A49647CBDFA69B85AACFFB
SHA-256:	38E5CB69BAED0165FBE956D68D52E0B226806006A8952DE0D8C602B25D024684
SHA-512:	36023F34ACF3BD9779273502DBCC0535C9F9B6D1AE4F7CD9706CA6B00631C79CFECAB44F276C773DF644045A7B6F18A0D7FE604AC6D5DF8D0ADF2152E84188 B6
Malicious:	false
Preview:	p..... .....q..%Y...(..... .....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\SHIPMENT DOCUMENTS.exe.log

Process:	C:\Users\user\Desktop\SHIPMENT DOCUMENTS.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F F8
Malicious:	**true**
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, Ve rsion=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72 e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Cultur e=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.Con figuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\cnWCiicEpxW.exe.log

Process:	C:\Users\user\AppData\Roaming\cnWCiicEpxW.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859

Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F F8
Malicious:	false
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, Ve rsion=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72 e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Cultur e=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.Con figuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Temp\tmp2A80.tmp

Process:	C:\Users\user\Desktop\SHIPMENT DOCUMENTS.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1656
Entropy (8bit):	5.156182356770437
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7h2ulNMFp2O/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB3sUtn:cbha7JlNQV/rydbz9l3YODOLNdq3T
MD5:	D452BE05EEC71DF72B608581ADB5DCC8
SHA1:	36F9E125299B3DC5751091A6F91B9183E587229F
SHA-256:	5646F4B081F4451AA51F15E1F1803831B170AD7251DB920F06E75269658C0466
SHA-512:	41CE620A09EF983B7C42579864BF781B1543B71F11A184C3D0127AD099EE0EE6B0D523B441C6CB2E5E4A56966836E8730A591D3D830F54B57F0F580B5798D774
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>.. </Pri ncipal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatte ries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvail

C:\Users\user\AppData\Local\Temp\tmpC7C9.tmp

Process:	C:\Users\user\AppData\Roaming\cnWCiicEpxW.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1656
Entropy (8bit):	5.156182356770437
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7h2ulNMFp2O/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB3sUtn:cbha7JlNQV/rydbz9l3YODOLNdq3T
MD5:	D452BE05EEC71DF72B608581ADB5DCC8
SHA1:	36F9E125299B3DC5751091A6F91B9183E587229F
SHA-256:	5646F4B081F4451AA51F15E1F1803831B170AD7251DB920F06E75269658C0466
SHA-512:	41CE620A09EF983B7C42579864BF781B1543B71F11A184C3D0127AD099EE0EE6B0D523B441C6CB2E5E4A56966836E8730A591D3D830F54B57F0F580B5798D774
Malicious:	false
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>.. </Pri ncipal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatte ries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvail

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

Process:	C:\Users\user\Desktop\SHIPMENT DOCUMENTS.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	896000
Entropy (8bit):	7.5003924727258
Encrypted:	false
SSDEEP:	12288:xcn1uQarFr5cE8LHWzVDLIKnnaYz4gIc+zuWl9wzV9av/SEdRMA/LyVu6gt0IPP:xYDvL6+Kn7ZciImV9an9/L1t0In

MD5:	12DC06D3034A17BE7A70A4AA45EDCE8D
SHA1:	9B68AE25498A12F19360DC0DC023AF61CA9BFA9D
SHA-256:	91826EFE412B5C829801D1C52FBB43225CF1F0FC4CBA201453AD877341C64B90
SHA-512:	49E50AFDE47577D004322820A4F37DE2DF21968751D863F312D4653934187C4F42E4AC8EEAA43F67CB73EF10A35F14E3CDEC4F710116ACAF52114007EFD6C4A
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 32%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...Iz.c.....P..... .....@.. ....@.....K.....R..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....X.....Z(....8.....(....8....*.&~.....*...~....*.b(....8.....(....8.....*...&~.....*...~....*..0..~.....8?.....E..... ...8....s.....8I...s.....8....s.....8....(....8....*s..... ....9...& ....8....s.....8.....0..$.....8....8....8.....~....o.....8.....*.0..$.....8.....*8....8.....~....o.....8.....0..$.....8....8... .8.....*.~....o.....8.....0.....~....o.....8....8.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.5003924727258
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:	SHIPMENT DOCUMENTS.exe
File size:	896000
MD5:	12dc06d3034a17be7a70a4aa45edce8d
SHA1:	9b68ae25498a12f19360dc0dc023af61ca9bfa9d
SHA256:	91826efe412b5c829801d1c52fbb43225cf1f0fc4cba201453ad877341c64b90
SHA512:	49e50afde47577d004322820a4f37de2df21968751d863f312d4653934187c4f42e4ac8eeaa43f67cb73ef10a35f14e3cdec4f710116acaf52114007efd6c4a1
SSDEEP:	12288:xcn1uQarFr5cE8LHWzVDLlKnnaYz4gIc+zuWl9wzV9av/SEdRMA/LyVu6gt0IPP:xYDvL6+Kn7ZciImV9an9/L1t0In
TLSH:	CA158D5232728873F5CF0135949535CC6EBCA543A6A6E2076FB7368056027BFFAACE41
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...Iz.c.....P..... .....@.. ....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4dc0ee
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x63857A49 [Tue Nov 29 03:19:37 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
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xdc0a0	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xde000	0x5c8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xe0000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xdc052	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xda0f4	0xda200	False	0.7780544860315186	data	7.505864996836325	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xde000	0x5c8	0x600	False	0.4303385416666667	data	4.156459778607487	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xe0000	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_VERSION	0xde0a0	0x33c	data		
RT_MANIFEST	0xde3dc	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Network Port Distribution

Total Packets: 54

- 53 (DNS)
- 587 undefined
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 16:43:51.102545977 CET	49713	443	192.168.2.6	52.20.78.240
Nov 29, 2022 16:43:51.102605104 CET	443	49713	52.20.78.240	192.168.2.6
Nov 29, 2022 16:43:51.102689981 CET	49713	443	192.168.2.6	52.20.78.240
Nov 29, 2022 16:43:51.206545115 CET	49713	443	192.168.2.6	52.20.78.240
Nov 29, 2022 16:43:51.206588984 CET	443	49713	52.20.78.240	192.168.2.6
Nov 29, 2022 16:43:51.515335083 CET	443	49713	52.20.78.240	192.168.2.6
Nov 29, 2022 16:43:51.515436888 CET	49713	443	192.168.2.6	52.20.78.240
Nov 29, 2022 16:43:51.518362045 CET	49713	443	192.168.2.6	52.20.78.240
Nov 29, 2022 16:43:51.518392086 CET	443	49713	52.20.78.240	192.168.2.6
Nov 29, 2022 16:43:51.518759966 CET	443	49713	52.20.78.240	192.168.2.6
Nov 29, 2022 16:43:51.679316998 CET	49713	443	192.168.2.6	52.20.78.240
Nov 29, 2022 16:43:52.707773924 CET	49713	443	192.168.2.6	52.20.78.240
Nov 29, 2022 16:43:52.707817078 CET	443	49713	52.20.78.240	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 16:44:00.619170904 CET	49713	443	192.168.2.6	52.20.78.240
Nov 29, 2022 16:44:00.619304895 CET	443	49713	52.20.78.240	192.168.2.6
Nov 29, 2022 16:44:00.619389057 CET	49713	443	192.168.2.6	52.20.78.240
Nov 29, 2022 16:44:20.968451977 CET	49721	587	192.168.2.6	199.79.62.12
Nov 29, 2022 16:44:21.135443926 CET	587	49721	199.79.62.12	192.168.2.6
Nov 29, 2022 16:44:21.135611057 CET	49721	587	192.168.2.6	199.79.62.12
Nov 29, 2022 16:44:21.397145033 CET	587	49721	199.79.62.12	192.168.2.6
Nov 29, 2022 16:44:21.397443056 CET	49721	587	192.168.2.6	199.79.62.12
Nov 29, 2022 16:44:21.564626932 CET	587	49721	199.79.62.12	192.168.2.6
Nov 29, 2022 16:44:21.565397024 CET	49721	587	192.168.2.6	199.79.62.12
Nov 29, 2022 16:44:21.735054016 CET	587	49721	199.79.62.12	192.168.2.6
Nov 29, 2022 16:44:21.735600948 CET	49721	587	192.168.2.6	199.79.62.12
Nov 29, 2022 16:44:21.908711910 CET	587	49721	199.79.62.12	192.168.2.6
Nov 29, 2022 16:44:21.908756018 CET	587	49721	199.79.62.12	192.168.2.6
Nov 29, 2022 16:44:21.908780098 CET	587	49721	199.79.62.12	192.168.2.6
Nov 29, 2022 16:44:21.908802986 CET	587	49721	199.79.62.12	192.168.2.6
Nov 29, 2022 16:44:21.908874989 CET	49721	587	192.168.2.6	199.79.62.12
Nov 29, 2022 16:44:21.910600901 CET	587	49721	199.79.62.12	192.168.2.6
Nov 29, 2022 16:44:21.950762033 CET	49721	587	192.168.2.6	199.79.62.12
Nov 29, 2022 16:44:22.117940903 CET	587	49721	199.79.62.12	192.168.2.6
Nov 29, 2022 16:44:22.270884991 CET	49721	587	192.168.2.6	199.79.62.12
Nov 29, 2022 16:44:29.999057055 CET	49721	587	192.168.2.6	199.79.62.12
Nov 29, 2022 16:44:30.165992975 CET	587	49721	199.79.62.12	192.168.2.6
Nov 29, 2022 16:44:30.167831898 CET	49721	587	192.168.2.6	199.79.62.12
Nov 29, 2022 16:44:30.335340977 CET	587	49721	199.79.62.12	192.168.2.6
Nov 29, 2022 16:44:30.361396074 CET	49721	587	192.168.2.6	199.79.62.12
Nov 29, 2022 16:44:30.568722963 CET	587	49721	199.79.62.12	192.168.2.6
Nov 29, 2022 16:44:30.607850075 CET	587	49721	199.79.62.12	192.168.2.6
Nov 29, 2022 16:44:30.616848946 CET	49721	587	192.168.2.6	199.79.62.12
Nov 29, 2022 16:44:30.783982038 CET	587	49721	199.79.62.12	192.168.2.6
Nov 29, 2022 16:44:30.784010887 CET	587	49721	199.79.62.12	192.168.2.6
Nov 29, 2022 16:44:30.784365892 CET	49721	587	192.168.2.6	199.79.62.12
Nov 29, 2022 16:44:30.982860088 CET	587	49721	199.79.62.12	192.168.2.6
Nov 29, 2022 16:44:30.986498117 CET	49721	587	192.168.2.6	199.79.62.12
Nov 29, 2022 16:44:31.154088974 CET	587	49721	199.79.62.12	192.168.2.6
Nov 29, 2022 16:44:31.157778978 CET	49721	587	192.168.2.6	199.79.62.12
Nov 29, 2022 16:44:31.158020020 CET	49721	587	192.168.2.6	199.79.62.12
Nov 29, 2022 16:44:31.159809113 CET	49721	587	192.168.2.6	199.79.62.12
Nov 29, 2022 16:44:31.159926891 CET	49721	587	192.168.2.6	199.79.62.12
Nov 29, 2022 16:44:31.324496031 CET	587	49721	199.79.62.12	192.168.2.6
Nov 29, 2022 16:44:31.324537992 CET	587	49721	199.79.62.12	192.168.2.6
Nov 29, 2022 16:44:31.326929092 CET	587	49721	199.79.62.12	192.168.2.6
Nov 29, 2022 16:44:31.326965094 CET	587	49721	199.79.62.12	192.168.2.6
Nov 29, 2022 16:44:31.327480078 CET	587	49721	199.79.62.12	192.168.2.6
Nov 29, 2022 16:44:31.459182024 CET	49721	587	192.168.2.6	199.79.62.12
Nov 29, 2022 16:44:42.362598896 CET	49738	443	192.168.2.6	3.232.242.170
Nov 29, 2022 16:44:42.362658024 CET	443	49738	3.232.242.170	192.168.2.6
Nov 29, 2022 16:44:42.362791061 CET	49738	443	192.168.2.6	3.232.242.170
Nov 29, 2022 16:44:42.394437075 CET	49738	443	192.168.2.6	3.232.242.170
Nov 29, 2022 16:44:42.394474030 CET	443	49738	3.232.242.170	192.168.2.6
Nov 29, 2022 16:44:42.694560051 CET	443	49738	3.232.242.170	192.168.2.6
Nov 29, 2022 16:44:42.694652081 CET	49738	443	192.168.2.6	3.232.242.170
Nov 29, 2022 16:44:42.708673954 CET	49738	443	192.168.2.6	3.232.242.170
Nov 29, 2022 16:44:42.708719969 CET	443	49738	3.232.242.170	192.168.2.6
Nov 29, 2022 16:44:42.709182978 CET	443	49738	3.232.242.170	192.168.2.6
Nov 29, 2022 16:44:42.788177967 CET	49738	443	192.168.2.6	3.232.242.170
Nov 29, 2022 16:44:43.747045040 CET	49738	443	192.168.2.6	3.232.242.170
Nov 29, 2022 16:44:43.747087955 CET	443	49738	3.232.242.170	192.168.2.6
Nov 29, 2022 16:44:43.893496990 CET	443	49738	3.232.242.170	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 16:44:43.893613100 CET	443	49738	3.232.242.170	192.168.2.6
Nov 29, 2022 16:44:43.895062923 CET	49738	443	192.168.2.6	3.232.242.170
Nov 29, 2022 16:44:43.912725925 CET	49738	443	192.168.2.6	3.232.242.170
Nov 29, 2022 16:45:10.773142099 CET	49743	587	192.168.2.6	199.79.62.12
Nov 29, 2022 16:45:10.940119028 CET	587	49743	199.79.62.12	192.168.2.6
Nov 29, 2022 16:45:10.940232038 CET	49743	587	192.168.2.6	199.79.62.12
Nov 29, 2022 16:45:11.515913010 CET	587	49743	199.79.62.12	192.168.2.6
Nov 29, 2022 16:45:11.549631119 CET	49743	587	192.168.2.6	199.79.62.12
Nov 29, 2022 16:45:11.717298031 CET	587	49743	199.79.62.12	192.168.2.6
Nov 29, 2022 16:45:11.721335888 CET	49743	587	192.168.2.6	199.79.62.12
Nov 29, 2022 16:45:11.889170885 CET	587	49743	199.79.62.12	192.168.2.6
Nov 29, 2022 16:45:11.893830061 CET	49743	587	192.168.2.6	199.79.62.12
Nov 29, 2022 16:45:12.065943956 CET	587	49743	199.79.62.12	192.168.2.6
Nov 29, 2022 16:45:12.066029072 CET	587	49743	199.79.62.12	192.168.2.6
Nov 29, 2022 16:45:12.066091061 CET	587	49743	199.79.62.12	192.168.2.6
Nov 29, 2022 16:45:12.066140890 CET	587	49743	199.79.62.12	192.168.2.6
Nov 29, 2022 16:45:12.066225052 CET	49743	587	192.168.2.6	199.79.62.12
Nov 29, 2022 16:45:12.066225052 CET	49743	587	192.168.2.6	199.79.62.12
Nov 29, 2022 16:45:12.067401886 CET	587	49743	199.79.62.12	192.168.2.6
Nov 29, 2022 16:45:12.089962959 CET	49743	587	192.168.2.6	199.79.62.12
Nov 29, 2022 16:45:12.257469893 CET	587	49743	199.79.62.12	192.168.2.6
Nov 29, 2022 16:45:12.366664886 CET	49743	587	192.168.2.6	199.79.62.12
Nov 29, 2022 16:45:12.534174919 CET	587	49743	199.79.62.12	192.168.2.6
Nov 29, 2022 16:45:12.539052010 CET	49743	587	192.168.2.6	199.79.62.12
Nov 29, 2022 16:45:12.706226110 CET	587	49743	199.79.62.12	192.168.2.6
Nov 29, 2022 16:45:12.706975937 CET	49743	587	192.168.2.6	199.79.62.12
Nov 29, 2022 16:45:12.914741039 CET	587	49743	199.79.62.12	192.168.2.6
Nov 29, 2022 16:45:12.955040932 CET	587	49743	199.79.62.12	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 16:43:50.994033098 CET	58595	53	192.168.2.6	8.8.8.8
Nov 29, 2022 16:43:51.012947083 CET	53	58595	8.8.8.8	192.168.2.6
Nov 29, 2022 16:43:51.037520885 CET	56331	53	192.168.2.6	8.8.8.8
Nov 29, 2022 16:43:51.056447029 CET	53	56331	8.8.8.8	192.168.2.6
Nov 29, 2022 16:44:20.796726942 CET	59504	53	192.168.2.6	8.8.8.8
Nov 29, 2022 16:44:20.967142105 CET	53	59504	8.8.8.8	192.168.2.6
Nov 29, 2022 16:44:42.209783077 CET	63229	53	192.168.2.6	8.8.8.8
Nov 29, 2022 16:44:42.226728916 CET	53	63229	8.8.8.8	192.168.2.6
Nov 29, 2022 16:44:42.301785946 CET	62538	53	192.168.2.6	8.8.8.8
Nov 29, 2022 16:44:42.320725918 CET	53	62538	8.8.8.8	192.168.2.6
Nov 29, 2022 16:45:10.583590984 CET	54903	53	192.168.2.6	8.8.8.8
Nov 29, 2022 16:45:10.742371082 CET	53	54903	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 29, 2022 16:43:50.994033098 CET	192.168.2.6	8.8.8.8	0x4c8d	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:43:51.037520885 CET	192.168.2.6	8.8.8.8	0x6b43	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:44:20.796726942 CET	192.168.2.6	8.8.8.8	0xde78	Standard query (0)	mail.southernboilers.org	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:44:42.209783077 CET	192.168.2.6	8.8.8.8	0x8455	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:44:42.301785946 CET	192.168.2.6	8.8.8.8	0x5a80	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:45:10.583590984 CET	192.168.2.6	8.8.8.8	0x4af5	Standard query (0)	mail.southernboilers.org	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 29, 2022 16:43:51.012947083 CET	8.8.8.8	192.168.2.6	0x4c8d	No error (0)	api.ipify.org	api.ipify.org.herokudns.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 16:43:51.012947083 CET	8.8.8.8	192.168.2.6	0x4c8d	No error (0)	api.ipify.org.herokudns.com		52.20.78.240	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:43:51.012947083 CET	8.8.8.8	192.168.2.6	0x4c8d	No error (0)	api.ipify.org.herokudns.com		3.220.57.224	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:43:51.012947083 CET	8.8.8.8	192.168.2.6	0x4c8d	No error (0)	api.ipify.org.herokudns.com		3.232.242.170	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:43:51.012947083 CET	8.8.8.8	192.168.2.6	0x4c8d	No error (0)	api.ipify.org.herokudns.com		54.91.59.199	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:43:51.056447029 CET	8.8.8.8	192.168.2.6	0x6b43	No error (0)	api.ipify.org	api.ipify.org.herokudns.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 16:43:51.056447029 CET	8.8.8.8	192.168.2.6	0x6b43	No error (0)	api.ipify.org.herokudns.com		3.220.57.224	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:43:51.056447029 CET	8.8.8.8	192.168.2.6	0x6b43	No error (0)	api.ipify.org.herokudns.com		54.91.59.199	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:43:51.056447029 CET	8.8.8.8	192.168.2.6	0x6b43	No error (0)	api.ipify.org.herokudns.com		52.20.78.240	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:43:51.056447029 CET	8.8.8.8	192.168.2.6	0x6b43	No error (0)	api.ipify.org.herokudns.com		3.232.242.170	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:44:01.656429052 CET	8.8.8.8	192.168.2.6	0xb330	No error (0)	windowsupdatebg.s.llnwi.net		178.79.242.0	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:44:01.656429052 CET	8.8.8.8	192.168.2.6	0xb330	No error (0)	windowsupdatebg.s.llnwi.net		95.140.236.0	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:44:20.967142105 CET	8.8.8.8	192.168.2.6	0xde78	No error (0)	mail.southernboilers.org		199.79.62.12	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:44:23.143907070 CET	8.8.8.8	192.168.2.6	0x7b4e	No error (0)	windowsupdatebg.s.llnwi.net		178.79.242.0	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:44:23.143907070 CET	8.8.8.8	192.168.2.6	0x7b4e	No error (0)	windowsupdatebg.s.llnwi.net		178.79.242.128	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:44:42.226728916 CET	8.8.8.8	192.168.2.6	0x8455	No error (0)	api.ipify.org	api.ipify.org.herokudns.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 16:44:42.226728916 CET	8.8.8.8	192.168.2.6	0x8455	No error (0)	api.ipify.org.herokudns.com		3.232.242.170	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:44:42.226728916 CET	8.8.8.8	192.168.2.6	0x8455	No error (0)	api.ipify.org.herokudns.com		54.91.59.199	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:44:42.226728916 CET	8.8.8.8	192.168.2.6	0x8455	No error (0)	api.ipify.org.herokudns.com		52.20.78.240	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:44:42.226728916 CET	8.8.8.8	192.168.2.6	0x8455	No error (0)	api.ipify.org.herokudns.com		3.220.57.224	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:44:42.320725918 CET	8.8.8.8	192.168.2.6	0x5a80	No error (0)	api.ipify.org	api.ipify.org.herokudns.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 16:44:42.320725918 CET	8.8.8.8	192.168.2.6	0x5a80	No error (0)	api.ipify.org.herokudns.com		3.232.242.170	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:44:42.320725918 CET	8.8.8.8	192.168.2.6	0x5a80	No error (0)	api.ipify.org.herokudns.com		54.91.59.199	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:44:42.320725918 CET	8.8.8.8	192.168.2.6	0x5a80	No error (0)	api.ipify.org.herokudns.com		52.20.78.240	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 29, 2022 16:44:42.320725918 CET	8.8.8.8	192.168.2.6	0x5a80	No error (0)	api.ipify.org.herokudns.com		3.220.57.224	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:45:10.742371082 CET	8.8.8.8	192.168.2.6	0x4af5	No error (0)	mail.southernboilers.org		199.79.62.12	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

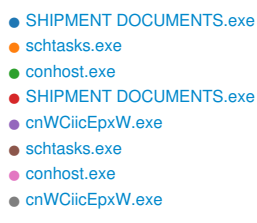
- api.ipify.org

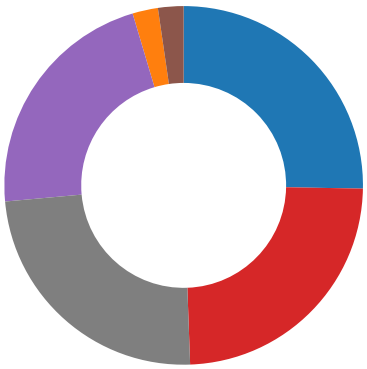
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 29, 2022 16:44:21.397145033 CET	587	49721	199.79.62.12	192.168.2.6	220-md-33.webhostbox.net ESMTP Exim 4.95 #2 Tue, 29 Nov 2022 15:44:21 +0000 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 29, 2022 16:44:21.397443056 CET	49721	587	192.168.2.6	199.79.62.12	EHLO 942247
Nov 29, 2022 16:44:21.564626932 CET	587	49721	199.79.62.12	192.168.2.6	250-md-33.webhostbox.net Hello 942247 [102.129.143.49] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Nov 29, 2022 16:44:21.565397024 CET	49721	587	192.168.2.6	199.79.62.12	STARTTLS
Nov 29, 2022 16:44:21.735054016 CET	587	49721	199.79.62.12	192.168.2.6	220 TLS go ahead
Nov 29, 2022 16:45:11.515913010 CET	587	49743	199.79.62.12	192.168.2.6	220-md-33.webhostbox.net ESMTP Exim 4.95 #2 Tue, 29 Nov 2022 15:45:11 +0000 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 29, 2022 16:45:11.549631119 CET	49743	587	192.168.2.6	199.79.62.12	EHLO 942247
Nov 29, 2022 16:45:11.717298031 CET	587	49743	199.79.62.12	192.168.2.6	250-md-33.webhostbox.net Hello 942247 [102.129.143.49] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Nov 29, 2022 16:45:11.721335888 CET	49743	587	192.168.2.6	199.79.62.12	STARTTLS
Nov 29, 2022 16:45:11.889170885 CET	587	49743	199.79.62.12	192.168.2.6	220 TLS go ahead

Statistics

Behavior





Click to jump to process

System Behavior

Analysis Process: SHIPMENT DOCUMENTS.exe PID: 3192, Parent PID: 3452

General

Target ID:	0
Start time:	16:44:02
Start date:	29/11/2022
Path:	C:\Users\user\Desktop\SHIPMENT DOCUMENTS.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SHIPMENT DOCUMENTS.exe
Imagebase:	0x910000
File size:	896000 bytes
MD5 hash:	12DC06D3034A17BE7A70A4AA45EDCE8D
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: 00000000.00000002.309368123.0000000003DCC000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.309368123.0000000003DCC000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000000.00000002.309368123.0000000003DCC000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.308207563.0000000003CA9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.308207563.0000000003CA9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000000.00000002.308207563.0000000003CA9000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D65CF06	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	6D65CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\cnWCiicEpxW.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C4A1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp2A80.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C4A7038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SHIPMENT DOCUMENTS.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D96C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp2A80.tmp	success or wait	1	6C4A6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\cnWCiicEpxW.exe	0	896000	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 49 7a fd 63 00 00 00 00 00 00 00 00 fd 00 0e 01 0b 01 50 00 00 fd 0d 00 00 08 00 00 00 00 00 00 fd fd 0d 00 00 20 00 00 00 fd 0d 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 20 0e 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELIzcP @ @	success or wait	1	6C4A1B4F	WriteFile
C:\Users\user\AppData\Local\Temp\tmp2A80.tmp	0	1656	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 65 72 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f	<?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> </Registratio	success or wait	1	6C4A1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SHIPMENT DOCUMENTS.exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6D96C907	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	6D635705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D635705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D63CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D5903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D635705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D635705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C4A1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C4A1B4F	ReadFile
C:\Users\user\Desktop\SHIPMENT DOCUMENTS.exe	unknown	896000	success or wait	1	6C4A1B4F	ReadFile

Analysis Process: schtasks.exe PID: **5900**, Parent PID: **3192**

General

Target ID:	16
Start time:	16:44:26
Start date:	29/11/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\cnWCiicEpxW" /XML "C:\Users\user\AppData\Local\Temp\tmp2A80.tmp
Imagebase:	0xac0000
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\tmp2A80.tmp	unknown	2	success or wait	1	ACAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp2A80.tmp	unknown	1657	success or wait	1	ACABD9	ReadFile

Analysis Process: conhost.exe PID: **1632**, Parent PID: **5900**

General

Target ID:	17
Start time:	16:44:26
Start date:	29/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
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: SHIPMENT DOCUMENTS.exe PID: **3244**, Parent PID: **3192**

General

Target ID:	20
Start time:	16:44:28
Start date:	29/11/2022
Path:	C:\Users\user\Desktop\SHIPMENT DOCUMENTS.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xab0000
File size:	896000 bytes
MD5 hash:	12DC06D3034A17BE7A70A4AA45EDCE8D
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: 00000014.00000000.301553016.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000014.00000000.301553016.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000014.00000000.301553016.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000014.00000002.522417697.0000000002EF1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000014.00000002.524431731.0000000002F44000.00000004.00000800.00020000.00000000.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	6D65CF06	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	6D65CF06	unknown
C:\Users\user\AppData\Local\Temp\tmpB8FB.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C4A7038	GetTempFileNameW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

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	6D635705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D635705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D63CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D5903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D635705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D635705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C4A1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C4A1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11072	success or wait	1	6C4A1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\422c3acc-afa2-4d28-854b-0223e53e9fba	unknown	4096	success or wait	1	6C4A1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11072	success or wait	1	6C4A1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C4A1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C4A1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	49152	success or wait	1	6C4A1B4F	ReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: cnWCiicEpxW.exe PID: **4444**, Parent PID: **1064**

General

Target ID:	21
Start time:	16:44:29
Start date:	29/11/2022
Path:	C:\Users\user\AppData\Roaming\cnWCiicEpxW.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\cnWCiicEpxW.exe

Imagebase:	0x6a0000
File size:	896000 bytes
MD5 hash:	12DC06D3034A17BE7A70A4AA45EDCE8D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 32%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D65CF06	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	6D65CF06	unknown
C:\Users\user\AppData\Local\Temp\tmpC7C9.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C4A7038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\cnWCiicEpxW.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D96C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpC7C9.tmp	success or wait	1	6C4A6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpC7C9.tmp	0	1656	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 65 72 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f	<?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> </Registratio	success or wait	1	6C4A1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\cnWCiicEpxW.exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6D96C907	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	6D635705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D635705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D63CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D5903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D635705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D635705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C4A1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C4A1B4F	ReadFile

Analysis Process: schtasks.exe PID: **5740**, Parent PID: **4444**

General

Target ID:	25
Start time:	16:45:10
Start date:	29/11/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\cnWCiicEpxW" /XML "C:\Users\user\AppData\Local\Temp\tmpC7C9.tmp
Imagebase:	0xac0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	false
Has administrator privileges:	false
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\tmpC7C9.tmp	unknown	2	success or wait	1	ACAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpC7C9.tmp	unknown	1657	success or wait	1	ACABD9	ReadFile

Analysis Process: conhost.exe PID: **4512**, Parent PID: **5740**

General

Target ID:	26
Start time:	16:45:10
Start date:	29/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cnWCiicEpxW.exe PID: **3132**, Parent PID: **4444**

General

Target ID:	27
Start time:	16:45:12
Start date:	29/11/2022
Path:	C:\Users\user\AppData\Roaming\cnWCiicEpxW.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xb20000
File size:	896000 bytes
MD5 hash:	12DC06D3034A17BE7A70A4AA45EDCE8D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000001B.00000002.528419495.0000000003164000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000001B.00000002.525674867.0000000003111000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D65CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D65CF06	unknown
C:\Users\user\AppData\Local\Temp\tmp7527.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C4A7038	GetTempFileNameW

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	6D635705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D635705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D63CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D5903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D635705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D635705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C4A1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C4A1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11072	success or wait	1	6C4A1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\422c3acc-afa2-4d28-854b-0223e53e9fba	unknown	4096	success or wait	1	6C4A1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11072	success or wait	1	6C4A1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C4A1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C4A1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	49152	success or wait	1	6C4A1B4F	ReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly