ID: 356452
Sample Name: (appproved)WJO-TT180,pdf.exe
Cookbook: default.jbs
Time: 08:10:56
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

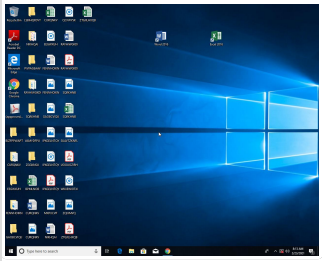
Analysis Report (appproved)WJO-TT180,pdf.exe

Overview

General Information

Sample Name:	(appproved)WJO-TT180,pdf.exe
Analysis ID:	356452
MD5:	e47851c94fdefd9..
SHA1:	7e027a9fadf5f4d…
SHA256:	92244ef8477d782.
Tags:	exe SnakeKeylogger

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

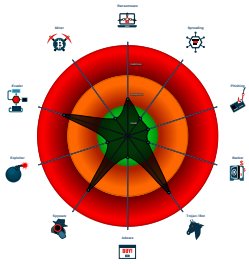
Snake Keylogger

Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected Snake Keylogger
- Injects a PE file into a foreign proce…
- May check the online IP address of …
- Tries to harvest and steal browser in…
- Tries to steal Mail credentials (via fil…
- Yara detected Beds Obfuscator
- Antivirus or Machine Learning detec…
- Contains long sleeps (>= 3 min)
- Creates a process in suspended mo…
- Detected potential crypto function
- Enables debug privileges

Classification



Startup

- **System is w10x64**
- (appproved)WJO-TT180,pdf.exe (PID: 6808 cmdline: 'C:\Users\user\Desktop\(appproved)WJO-TT180,pdf.exe' MD5: E47851C94FDEFD958CFE16AF2AF3661A)
  - (appproved)WJO-TT180,pdf.exe (PID: 5604 cmdline: {path} MD5: E47851C94FDEFD958CFE16AF2AF3661A)
- **cleanup**

Malware Configuration

Threatname: Snake Keylogger


```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": {
    "Port": "587",
    "SMTP Credential": "info@aruscomext.comBhnCP!@g6smtp.aruscomext.com"
  }
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.419975488.000000000350 9000.00000004.00000001.sdmp	JoeSecurity_BedsObfuscat or	Yara detected Beds Obfuscator	Joe Security	
00000000.00000002.419975488.000000000350 9000.00000004.00000001.sdmp	JoeSecurity_SnakeKeylog ger	Yara detected Snake Keylogger	Joe Security	
00000009.00000002.595511779.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_BedsObfuscat or	Yara detected Beds Obfuscator	Joe Security	
00000009.00000002.595511779.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_SnakeKeylog ger	Yara detected Snake Keylogger	Joe Security	
00000000.00000002.420374422.000000000376 9000.00000004.00000001.sdmp	JoeSecurity_BedsObfuscat or	Yara detected Beds Obfuscator	Joe Security	

Source	Rule	Description	Author	Strings
Click to see the 6 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.(appproved)WJO-TT180,pdf.exe.37023d8.1.unpack	JoeSecurity_BedsObfuscator	Yara detected Beds Obfuscator	Joe Security	
0.2.(appproved)WJO-TT180,pdf.exe.37023d8.1.unpack	JoeSecurity_SnakeKeylogger	Yara detected Snake Keylogger	Joe Security	
0.2.(appproved)WJO-TT180,pdf.exe.3549528.2.raw.unpack	JoeSecurity_BedsObfuscator	Yara detected Beds Obfuscator	Joe Security	
0.2.(appproved)WJO-TT180,pdf.exe.3549528.2.raw.unpack	JoeSecurity_SnakeKeylogger	Yara detected Snake Keylogger	Joe Security	
9.2.(appproved)WJO-TT180,pdf.exe.400000.0.unpack	JoeSecurity_BedsObfuscator	Yara detected Beds Obfuscator	Joe Security	
Click to see the 3 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

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

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Compliance:

Uses 32bit PE files

Uses insecure TLS / SSL version for HTTPS connection

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

Networking:

May check the online IP address of the machine

Data Obfuscation:

Yara detected Beds Obfuscator

Malware Analysis System Evasion:

Yara detected Beds Obfuscator

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Snake Keylogger

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

Tries to steal Mail credentials (via file access)

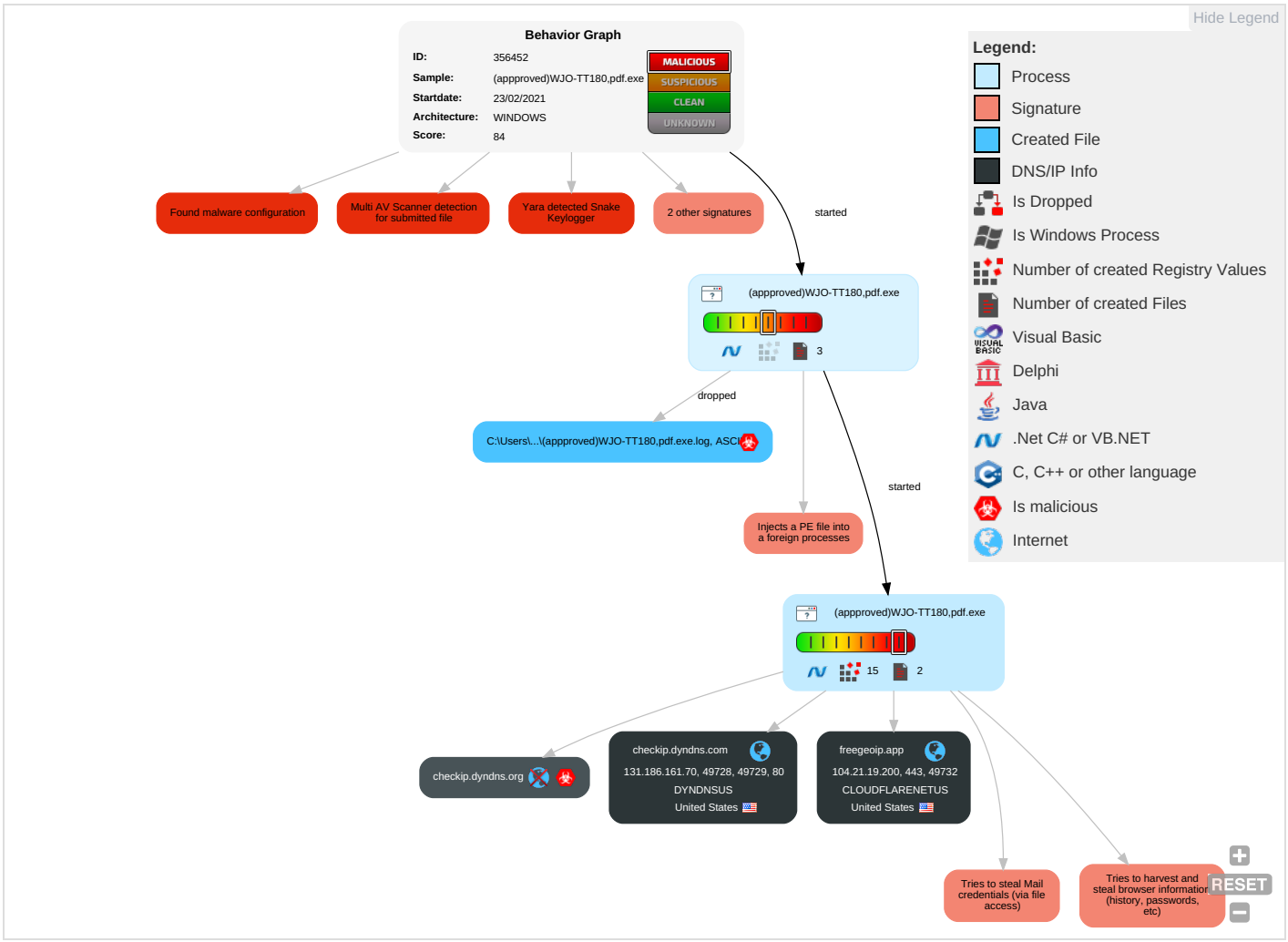
Remote Access Functionality:

Yara detected Snake Keylogger

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 1 2	Masquerading 1	OS Credential Dumping 1	Virtualization/Sandbox Evasion 2	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesd Insecur Networl Commu
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit Redirec Calls/SI
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Remote System Discovery 1	SMB/Windows Admin Shares	Data from Local System 1	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit Track D Locatio
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	System Network Configuration Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1	LSA Secrets	System Information Discovery 1 3	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipul Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammir Denial Service

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
(appproved)WJO-TT180,pdf.exe	18%	Virustotal		Browse
(appproved)WJO-TT180,pdf.exe	13%	ReversingLabs	ByteCode-MSIL.Packed.Generic	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
9.2.(appproved)WJO-TT180,pdf.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
freegeoip.app	0%	Virustotal		Browse
checkip.dyndns.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.ascendercorp.com/typedesigners.htmlU	0%	Avira URL Cloud	safe	
http://www.ascendercorp.com/typedesigners.htmlV	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnicrk	0%	Avira URL Cloud	safe	
http://https://freegeoip.app	0%	URL Reputation	safe	
http://https://freegeoip.app	0%	URL Reputation	safe	
http://https://freegeoip.app	0%	URL Reputation	safe	
http://www.esvstudybible.org/search?q=Whttp://www.blueletterbible.org/Bible.cfm?b=	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://checkip.dyndns.org4	0%	URL Reputation	safe	
http://checkip.dyndns.org4	0%	URL Reputation	safe	
http://checkip.dyndns.org4	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://checkip.dyndns.org/	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnh-c	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htmjsv	0%	Avira URL Cloud	safe	
http://www.urwpp.de2	0%	Avira URL Cloud	safe	
http://checkip.dyndns.org/HB	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.fontbureau.comgrito	0%	URL Reputation	safe	
http://www.fontbureau.comgrito	0%	URL Reputation	safe	
http://www.fontbureau.comgrito	0%	URL Reputation	safe	
http://www.founder.com.cn/cnradq	0%	Avira URL Cloud	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.carterandcone.comypox	0%	Avira URL Cloud	safe	
http://https://freegeoip.app4	0%	URL Reputation	safe	
http://https://freegeoip.app4	0%	URL Reputation	safe	
http://https://freegeoip.app4	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://freegeoip.app	0%	URL Reputation	safe	
http://freegeoip.app	0%	URL Reputation	safe	
http://freegeoip.app	0%	URL Reputation	safe	
http://www.carterandcone.com#vn	0%	Avira URL Cloud	safe	
http://www.sakkal.comM	0%	Avira URL Cloud	safe	
http://www.carterandcone.come	0%	URL Reputation	safe	
http://www.carterandcone.come	0%	URL Reputation	safe	
http://www.carterandcone.come	0%	URL Reputation	safe	
http://www.founder.com.cn/cnade	0%	Avira URL Cloud	safe	
http://www.carterandcone.comn-uU	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cno.U	0%	Avira URL Cloud	safe	
http://www.carterandcone.como.G	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cnicr	0%	Avira URL Cloud	safe	
http://checkip.dyndns.org	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krFe:	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cnh	0%	Avira URL Cloud	safe	
http://https://freegeoip.app/xml/84.17.52.38x	0%	URL Reputation	safe	
http://https://freegeoip.app/xml/84.17.52.38x	0%	URL Reputation	safe	
http://https://freegeoip.app/xml/84.17.52.38x	0%	URL Reputation	safe	
http://https://freegeoip.app/xml/LoadCountryNameClipboard	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://freegeoip.app/xml/LoadCountryNameClipboard	0%	URL Reputation	safe	
http://https://freegeoip.app/xml/LoadCountryNameClipboard	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://www.carterandcone.comm	0%	URL Reputation	safe	
http://www.carterandcone.comm	0%	URL Reputation	safe	
http://www.carterandcone.comm	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://checkip.dyndns.orgD8	0%	URL Reputation	safe	
http://checkip.dyndns.orgD8	0%	URL Reputation	safe	
http://checkip.dyndns.orgD8	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.fontbureau.coma1	0%	Avira URL Cloud	safe	
http://www.monotype.1	0%	Avira URL Cloud	safe	
http://www.carterandcone.como.-	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krim	0%	Avira URL Cloud	safe	
http://www.carterandcone.comradq	0%	Avira URL Cloud	safe	
http://https://freegeoip.app/xml/84.17.52.38	0%	URL Reputation	safe	
http://https://freegeoip.app/xml/84.17.52.38	0%	URL Reputation	safe	
http://https://freegeoip.app/xml/84.17.52.38	0%	URL Reputation	safe	
http://www.carterandcone.comn-u	0%	URL Reputation	safe	
http://www.carterandcone.comn-u	0%	URL Reputation	safe	
http://www.carterandcone.comn-u	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cnV	0%	Avira URL Cloud	safe	
http://www.carterandcone.comams	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
freegeoip.app	104.21.19.200	true	false	• 0%, Virustotal, Browse	unknown
checkip.dyndns.com	131.186.161.70	true	false	• 0%, Virustotal, Browse	unknown
checkip.dyndns.org	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://checkip.dyndns.org/	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.ascendercorp.com/typedesigners.htmlU	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.339262342.00000000005563000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.ascendercorp.com/typedesigners.htmlV	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.339262342.00000000005563000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cnicrk	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.336642030.00000000555B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://freegeoip.app	(appproved)WJO-TT180,pdf.exe, 00000009.00000002.597436548.00000002D32000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.esvstudybible.org/search?q=Whttp://www.blueletterbible.org/Bible.cfm?b=	(appproved)WJO-TT180,pdf.exe	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	(appproved)WJO-TT180,pdf.exe, 00000000.00000002.424947613.00000006752000.00000004.00000001.sdmp, (appproved)WJO-TT180,pdf.exe, 00000000.00000003.349835607.000000000555B000.00000004.00000001.sdmp, (appproved)WJO-TT180,pdf.exe, 00000000.00000003.343079140.000000000555B000.00000004.00000001.sdmp	false		high
http://www.sajatypeworks.com	(appproved)WJO-TT180,pdf.exe, 00000000.00000002.424947613.00000006752000.00000004.00000001.sdmp, (appproved)WJO-TT180,pdf.exe, 00000000.00000003.332645551.0000000005542000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://checkip.dyndns.org4	(appproved)WJO-TT180,pdf.exe, 00000009.00000002.597310595.00000002C81000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	(appproved)WJO-TT180,pdf.exe, 00000000.00000002.424947613.00000006752000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnh-c	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.336828517.0000000555B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htmjsv	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.347435048.0000000555B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.de2	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.342050521.0000000555E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://checkip.dyndns.org/HB	(appproved)WJO-TT180,pdf.exe, 00000009.00000002.597310595.00000002C81000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	(appproved)WJO-TT180,pdf.exe, 00000000.00000002.424947613.00000006752000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comgrito	(appproved)WJO-TT180,pdf.exe, 00000000.00000002.416798330.00000000C07000.00000004.00000040.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnradq	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.336906415.0000000555B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.ascendercorp.com/typedesigners.html	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.338965985.00000005563000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comypox	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.337499341.0000000555B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://freegeoip.app4	(appproved)WJO-TT180,pdf.exe, 00000009.00000002.597436548.00000002D32000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	(appproved)WJO-TT180,pdf.exe, 00000000.00000002.424947613.00000006752000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.zhongyicts.com.cn	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.337329360.00 0000000555B000.00000004.000000 01.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	(appproved)WJO-TT180,pdf.exe, 00000009.00000002.597310595.00 00000002C81000.00000004.000000 01.sdmp	false		high
http://www.carterandcone.como.	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.338241457.00 00000005564000.00000004.000000 01.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://freegeoip.app	(appproved)WJO-TT180,pdf.exe, 00000009.00000002.597436548.00 00000002D32000.00000004.000000 01.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com#vn	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.337929066.00 0000000555B000.00000004.000000 01.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sakkal.comM	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.339003661.00 00000005563000.00000004.000000 01.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.come	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.337929066.00 0000000555B000.00000004.000000 01.sdmp, (appproved)WJO-TT180, pdf.exe, 00000000.00000003.337 602568.000000000555B000.000000 04.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnade	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.336906415.00 0000000555B000.00000004.000000 01.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comn-uU	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.337929066.00 0000000555B000.00000004.000000 01.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cno.U	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.337329360.00 0000000555B000.00000004.000000 01.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.como.G	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.337929066.00 0000000555B000.00000004.000000 01.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cnicr	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.337329360.00 0000000555B000.00000004.000000 01.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.biblegateway.com/passage/?search=	(appproved)WJO-TT180,pdf.exe	false		high
http://www.fontbureau.com/designers/cabarga.htmlsd9#	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.347344265.00 0000000557E000.00000004.000000 01.sdmp	false		high
http://checkip.dyndns.org	(appproved)WJO-TT180,pdf.exe, 00000009.00000002.597436548.00 00000002D32000.00000004.000000 01.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.krFe:	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.336098960.00 0000000555B000.00000004.000000 01.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cnh	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.337329360.00 0000000555B000.00000004.000000 01.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://freegeoip.app/xml/84.17.52.38x	(appproved)WJO-TT180,pdf.exe, 00000009.00000002.597436548.00 00000002D32000.00000004.000000 01.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://freegeoip.app/xml/LoadCountryNameClipboard	(appproved)WJO-TT180,pdf.exe, 00000009.00000002.597310595.00 00000002C81000.00000004.000000 01.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://en.w	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.334003174.00 0000000555B000.00000004.000000 01.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

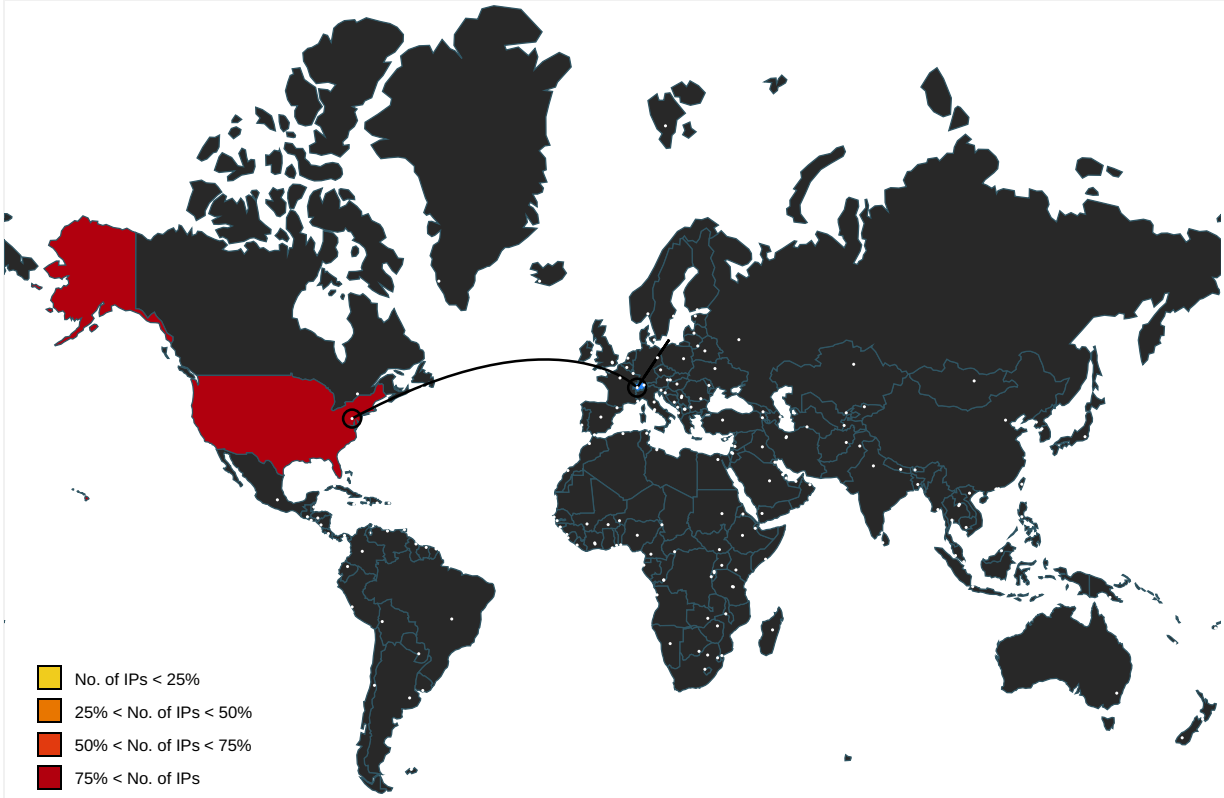
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.comm	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.338549853.00000000555C000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	(appproved)WJO-TT180,pdf.exe, 00000000.00000002.424947613.00000000006752000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://checkip.dyndns.orgD8	(appproved)WJO-TT180,pdf.exe, 00000009.00000002.597436548.00000000002D32000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.336284668.00000000555B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.coma1	(appproved)WJO-TT180,pdf.exe, 00000000.00000002.416798330.00000000C07000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.343474220.0000000557E000.00000004.00000001.sdmp, (appproved)WJO-TT180, pdf.exe, 00000000.00000003.343459978.000000000555B000.00000004.00000001.sdmp, (appproved)WJO-TT180,pdf.exe, 00000000.00000002.424947613.0000000006752000.00000004.00000001.sdmp	false		high
http://www.monotype.1	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.347020395.00000000555B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.carterandcone.como.-	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.337602568.00000000555B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.sandoll.co.krim	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.336284668.00000000555B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comradq	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.337929066.00000000555B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://freegeoip.app/xml/84.17.52.38	(appproved)WJO-TT180,pdf.exe, 00000009.00000002.597436548.00000000002D32000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designersG	(appproved)WJO-TT180,pdf.exe, 00000000.00000002.424947613.0000000006752000.00000004.00000001.sdmp	false		high
http://www.carterandcone.comn-u	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.337929066.00000000555B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designersM	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.344398062.00000000555B000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	(appproved)WJO-TT180,pdf.exe, 00000000.00000002.424947613.0000000006752000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	(appproved)WJO-TT180,pdf.exe, 00000000.00000002.424947613.0000000006752000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnV	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.336561668.00000000555B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	(appproved)WJO-TT180,pdf.exe, 00000000.00000002.424947613.0000000006752000.00000004.00000001.sdmp	false		high
http://www.carterandcone.comams	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.337499341.00000000555B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.tiro.com	(appproved)WJO-TT180,pdf.exe, 00000000.00000002.424947613.00000000006752000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sandoll.co.krom	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.335938249.00000000000555B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	(appproved)WJO-TT180,pdf.exe, 00000000.00000002.424947613.00000000006752000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.337378048.00000000000555B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://topicalmemorysystem.googlecode.com/files/	(appproved)WJO-TT180,pdf.exe	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersP	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.344134436.00000000000555B000.00000004.00000001.sdmp, (appproved)WJO-TT180, pdf.exe, 00000000.00000003.343035874.000000000555B000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cnn-u~	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.336561668.00000000000555B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.krs-c	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.336098960.00000000000555B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.typography.netD	(appproved)WJO-TT180,pdf.exe, 00000000.00000002.424947613.00000000006752000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.347435048.00000000000555B000.00000004.00000001.sdmp, (appproved)WJO-TT180, pdf.exe, 00000000.00000002.424947613.0000000006752000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.333466058.00000000000555B000.00000004.00000001.sdmp, (appproved)WJO-TT180, pdf.exe, 00000000.00000002.424947613.0000000006752000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.comx	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.333585529.00000000000555B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnnie9	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.336642030.00000000000555B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.c	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.336355922.00000000000555B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.agfamonotype.K9	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.349835607.00000000000555B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.telegram.org/bot/sendMessage?chat_id=&text=Createutf-8	(appproved)WJO-TT180,pdf.exe, 00000009.00000002.597310595.00000000002C81000.00000004.00000001.sdmp	false		high
http://www.carterandcone.comV	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.337602568.00000000000555B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	(appproved)WJO-TT180,pdf.exe, 00000000.00000002.424947613.00000000006752000.00000004.00000001.sdmp	false		high
http://www.sandoll.co.kr	(appproved)WJO-TT180,pdf.exe, 00000000.00000002.424947613.00000000006752000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.coma	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.332645551.00000000542000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://checkip.dyndns.com	(appproved)WJO-TT180,pdf.exe, 00000009.00000002.597436548.00000002D32000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.de	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.344532501.00000005567000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designersq	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.343459978.0000000555B000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cnei	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.336906415.0000000555B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sakkal.com	(appproved)WJO-TT180,pdf.exe, 00000000.00000002.424947613.00000006752000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designersr	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.344134436.0000000555B000.00000004.00000001.sdmp	false		high
http://https://freegeoip.app/xml/	(appproved)WJO-TT180,pdf.exe, 00000009.00000002.597436548.00000002D32000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comuct2	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.337929066.0000000555B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	(appproved)WJO-TT180,pdf.exe, 00000000.00000002.424947613.00000006752000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com	(appproved)WJO-TT180,pdf.exe, 00000000.00000002.424947613.00000006752000.00000004.00000001.sdmp	false		high
http://www.sandoll.c8	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.336219913.0000000555B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comF	(appproved)WJO-TT180,pdf.exe, 00000000.00000002.416798330.00000000C07000.00000004.00000040.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tiro.comslnt	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.338069889.0000000555B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/C	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.336906415.0000000555B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comTC	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.337929066.0000000555B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.biblija.net/biblija.cgi?m=	(appproved)WJO-TT180,pdf.exe	false		high
http://www.fontbureau.com/designers/cabarga.htmlN	(appproved)WJO-TT180,pdf.exe, 00000000.00000002.424947613.00000006752000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.336906415.0000000555B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.monotype.	(appproved)WJO-TT180,pdf.exe, 00000000.00000003.347237992.0000000555B000.00000004.00000001.sdmp, (appproved)WJO-TT180,pdf.exe, 00000000.00000003.347777721.000000000555B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/	(appproved)WJO-TT180,pdf.exe, 00000000.00000002.424947613.000000006752000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
131.186.161.70	unknown	United States		33517	DYNDNSUS	false
104.21.19.200	unknown	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356452
Start date:	23.02.2021
Start time:	08:10:56
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	(appproved)WJO-TT180,pdf.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	22
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:	mal84.troj.spyw.evad.winEXE@3/1@3/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 51.132.208.181, 204.79.197.200, 13.107.21.200, 13.64.90.137, 13.88.21.125, 92.122.145.220, 168.61.161.212, 104.42.151.234, 51.11.168.160, 8.248.119.254, 8.248.131.254, 8.253.207.120, 8.248.143.254, 8.253.204.249, 51.103.5.159, 92.122.213.194, 92.122.213.247, 52.155.217.156, 20.54.26.129, 184.30.20.56, 51.104.146.109 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, vip1-par02p.wns.notify.trafficmanager.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, fs.microsoft.com, dual-a-0001.a-msedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
08:11:59	API Interceptor	1x Sleep call for process: (appproved)WJO-TT180,pdf.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
131.186.161.70	SecuriteInfo.com.Trojan.Inject4.6572.13919.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	Scan Document-01.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	Firm Order.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	index_2021-02-18-20_41.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	Quotation and Prices.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	RFQ.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	order170221.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	IMG_144907.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	PAYMENT_SLIP.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	request for quotation.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	zmODG1qz1c.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	0900009000SALES.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	Shipping Documents Original BL, Invoice & Packing List.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	COTIZACI#U00d3N.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	PO00004423.doc	Get hash	malicious	Browse	• checkip.dyndns.org/
	0009876_xls.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	DHL_FORM_00029168873.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	RFQ Q7171.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	Invoice Feb.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	invoice.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
104.21.19.200	SOS URGENT RFQ #2345.exe	Get hash	malicious	Browse	
	GPP.exe	Get hash	malicious	Browse	
	DHL Shipment Notification 6368638172.pdf.exe	Get hash	malicious	Browse	
	#11032019 de investigaci#U00f3n de #U00f3rdenes,pdf.exe	Get hash	malicious	Browse	
	Neue Bestellung_WJO-001, pdf.exe	Get hash	malicious	Browse	
	Halkbank_Ekstre_20210222_082357_541079.exe	Get hash	malicious	Browse	
	swift payment.doc	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Inject4.6572.13919.exe	Get hash	malicious	Browse	
	Order.exe	Get hash	malicious	Browse	
	ORDER PURCHASE ITEMS.exe	Get hash	malicious	Browse	
	SwiftCopyTT.exe	Get hash	malicious	Browse	
	Selected New Order.exe	Get hash	malicious	Browse	
	RFQ file_pdf.exe	Get hash	malicious	Browse	
	Order.exe	Get hash	malicious	Browse	
	telex transfer.exe	Get hash	malicious	Browse	
	cotizaci#U00f3n.exe	Get hash	malicious	Browse	
	ORDEN DE COMPRA.exe	Get hash	malicious	Browse	
	PO 2006-020 MAQQO,zip.exe	Get hash	malicious	Browse	
	Firm Order.exe	Get hash	malicious	Browse	
	purchase order.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
freegeoip.app	purchase order.exe	Get hash	malicious	Browse	• 172.67.188.154
	9073782912,pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	SOS URGENT RFQ #2345.exe	Get hash	malicious	Browse	• 104.21.19.200
	purchase order 1.exe	Get hash	malicious	Browse	• 172.67.188.154
	telex transfer.exe	Get hash	malicious	Browse	• 172.67.188.154
	GPP.exe	Get hash	malicious	Browse	• 172.67.188.154
	DHL Shipment Notification 6368638172.pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	#11032019 de investigaci#U00f3n de #U00f3rdenes,pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	Neue Bestellung_WJO-001, pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	Halkbank_Ekstre_20210222_082357_541079.exe	Get hash	malicious	Browse	• 104.21.19.200
	swift payment.doc	Get hash	malicious	Browse	• 104.21.19.200
	Order_C3350191107102300.exe	Get hash	malicious	Browse	• 172.67.188.154
	SecuriteInfo.com.Trojan.Inject4.6572.13919.exe	Get hash	malicious	Browse	• 104.21.19.200
	Order.exe	Get hash	malicious	Browse	• 104.21.19.200
	ORDER PURCHASE ITEMS.exe	Get hash	malicious	Browse	• 104.21.19.200
	Payment information 366531890544-2222021,pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	SwiftCopyTT.exe	Get hash	malicious	Browse	• 104.21.19.200
	Selected New Order.exe	Get hash	malicious	Browse	• 104.21.19.200
	RFQ file_pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	Order.exe	Get hash	malicious	Browse	• 104.21.19.200
checkip.dyndns.com	purchase order.exe	Get hash	malicious	Browse	• 131.186.113.70
	9073782912,pdf.exe	Get hash	malicious	Browse	• 131.186.113.70
	SOS URGENT RFQ #2345.exe	Get hash	malicious	Browse	• 131.186.113.70
	purchase order 1.exe	Get hash	malicious	Browse	• 162.88.193.70
	telex transfer.exe	Get hash	malicious	Browse	• 162.88.193.70
	iAxkn PDF.exe	Get hash	malicious	Browse	• 216.146.43.71
	GPP.exe	Get hash	malicious	Browse	• 162.88.193.70
	DHL Shipment Notification 6368638172.pdf.exe	Get hash	malicious	Browse	• 216.146.43.70
	#11032019 de investigaci#U00f3n de #U00f3rdenes,pdf.exe	Get hash	malicious	Browse	• 162.88.193.70
	Neue Bestellung_WJO-001, pdf.exe	Get hash	malicious	Browse	• 162.88.193.70
	Halkbank_Ekstre_20210222_082357_541079.exe	Get hash	malicious	Browse	• 131.186.113.70
	swift payment.doc	Get hash	malicious	Browse	• 162.88.193.70
	Order_C3350191107102300.exe	Get hash	malicious	Browse	• 131.186.113.70
	SecuriteInfo.com.Trojan.Inject4.6572.13919.exe	Get hash	malicious	Browse	• 131.186.161.70
	Order.exe	Get hash	malicious	Browse	• 162.88.193.70
	ORDER PURCHASE ITEMS.exe	Get hash	malicious	Browse	• 216.146.43.70
	Payment information 366531890544-2222021,pdf.exe	Get hash	malicious	Browse	• 131.186.113.70
	SwiftCopyTT.exe	Get hash	malicious	Browse	• 216.146.43.70
	Selected New Order.exe	Get hash	malicious	Browse	• 216.146.43.71
	RFQ file_pdf.exe	Get hash	malicious	Browse	• 131.186.113.70

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	purchase order.exe	Get hash	malicious	Browse	• 172.67.188.154
	9073782912,pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	SOS URGENT RFQ #2345.exe	Get hash	malicious	Browse	• 104.21.19.200
	INV_PR2201.docm	Get hash	malicious	Browse	• 162.159.13 4.233
	XP 6.xlsx	Get hash	malicious	Browse	• 172.67.172.17
	b0PmDaDeNh.dll	Get hash	malicious	Browse	• 104.20.184.68
	PO_210222.exe	Get hash	malicious	Browse	• 23.227.38.74
	Sw5kF7zkty.exe	Get hash	malicious	Browse	• 162.159.13 4.233
	PAYRECEIPT.exe	Get hash	malicious	Browse	• 172.67.172.17
	unmapped_executable_of_polyglot_duke.dll	Get hash	malicious	Browse	• 172.67.204.156
	6v3gJQytBL.exe	Get hash	malicious	Browse	• 104.18.87.101
	YqgA9W2m1D.exe	Get hash	malicious	Browse	• 104.18.87.101
	Document1094680387_02012021.xls	Get hash	malicious	Browse	• 104.21.29.200
	Document1094680387_02012021.xls	Get hash	malicious	Browse	• 172.67.149.197
	New Order.exe	Get hash	malicious	Browse	• 104.21.71.230
	PO#87498746510.exe	Get hash	malicious	Browse	• 172.67.172.17

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	muOvK6dngg.exe	Get hash	malicious	Browse	• 172.67.141.244
	rieuro.dll	Get hash	malicious	Browse	• 104.20.185.68
	TT.exe	Get hash	malicious	Browse	• 172.67.172.17
	Payment_pdf.exe	Get hash	malicious	Browse	• 172.67.172.17
DYNDNSUS	purchase order.exe	Get hash	malicious	Browse	• 131.186.113.70
	9073782912,pdf.exe	Get hash	malicious	Browse	• 131.186.113.70
	SOS URGENT RFQ #2345.exe	Get hash	malicious	Browse	• 131.186.113.70
	purchase order 1.exe	Get hash	malicious	Browse	• 162.88.193.70
	telex transfer.exe	Get hash	malicious	Browse	• 162.88.193.70
	iAxkn PDF.exe	Get hash	malicious	Browse	• 216.146.43.71
	GPP.exe	Get hash	malicious	Browse	• 162.88.193.70
	DHL Shipment Notification 6368638172.pdf.exe	Get hash	malicious	Browse	• 216.146.43.70
	#11032019 de investigaci#U00f3n de #U00f3rdenes,pdf.exe	Get hash	malicious	Browse	• 162.88.193.70
	Neue Bestellung_WJO-001, pdf.exe	Get hash	malicious	Browse	• 162.88.193.70
	Halkbank_Ekstre_20210222_082357_541079.exe	Get hash	malicious	Browse	• 131.186.113.70
	swift payment.doc	Get hash	malicious	Browse	• 162.88.193.70
	Order_C3350191107102300.exe	Get hash	malicious	Browse	• 131.186.113.70
	SecuriteInfo.com.Trojan.Inject4.6572.13919.exe	Get hash	malicious	Browse	• 216.146.43.70
	Order.exe	Get hash	malicious	Browse	• 162.88.193.70
	ORDER PURCHASE ITEMS.exe	Get hash	malicious	Browse	• 216.146.43.70
	Payment information 366531890544-2222021,pdf.exe	Get hash	malicious	Browse	• 131.186.113.70
	SwiftCopyTT.exe	Get hash	malicious	Browse	• 216.146.43.70
	Selected New Order.exe	Get hash	malicious	Browse	• 216.146.43.71
	RFQ file_pdf.exe	Get hash	malicious	Browse	• 131.186.113.70

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
54328bd36c14bd82ddaa0c04b25ed9ad	purchase order.exe	Get hash	malicious	Browse	• 104.21.19.200
	9073782912,pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	SOS URGENT RFQ #2345.exe	Get hash	malicious	Browse	• 104.21.19.200
	purchase order 1.exe	Get hash	malicious	Browse	• 104.21.19.200
	telex transfer.exe	Get hash	malicious	Browse	• 104.21.19.200
	GPP.exe	Get hash	malicious	Browse	• 104.21.19.200
	DHL Shipment Notification 6368638172.pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	#11032019 de investigaci#U00f3n de #U00f3rdenes,pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	Neue Bestellung_WJO-001, pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	Halkbank_Ekstre_20210222_082357_541079.exe	Get hash	malicious	Browse	• 104.21.19.200
	Order_C3350191107102300.exe	Get hash	malicious	Browse	• 104.21.19.200
	SecuriteInfo.com.Trojan.Inject4.6572.13919.exe	Get hash	malicious	Browse	• 104.21.19.200
	Order.exe	Get hash	malicious	Browse	• 104.21.19.200
	ORDER PURCHASE ITEMS.exe	Get hash	malicious	Browse	• 104.21.19.200
	Payment information 366531890544-2222021,pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	MR52.vbs	Get hash	malicious	Browse	• 104.21.19.200
	SwiftCopyTT.exe	Get hash	malicious	Browse	• 104.21.19.200
	Selected New Order.exe	Get hash	malicious	Browse	• 104.21.19.200
	RFQ file_pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	Order.exe	Get hash	malicious	Browse	• 104.21.19.200

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\(appproved)WJO-TT180,pdf.exe.log

Process:	C:\Users\user\Desktop\(appproved)WJO-TT180,pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\(appproved)WJO-TT180,pdf.exe.log	
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.56161688167418
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	(appproved)WJO-TT180,pdf.exe
File size:	831488
MD5:	e47851c94fdefd958cfe16af2af3661a
SHA1:	7e027a9fadf5f4d9c1bb65c68db34cc5318353b0
SHA256:	92244ef8477d782361d87f7571458bccf8de2af4cccfd738bde234d91216fbe3
SHA512:	69d1a380c186752263b5a64828551f5f2dda0ed327145bcdd537fbce1d07795b5dc52a7e0a07f8a64fda7b5dab33a64096c60c6b5ad7191186c25f33c08cb10d
SSDEEP:	12288:MzPTExm6YzF0k8Ljz3WZcuZ+JLbvs2zlyAKp:M+gR0k8L/WiouzzlWp
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....H4`.....0..... .....@.. .....@.....

File Icon

Icon Hash:	8604a4acbcace4f8

Static PE Info

General

Entrypoint:	0x49b3aa
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x603448AD [Tue Feb 23 00:13:33 2021 UTC]
TLS Callbacks:	

General

CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x9b358	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x9c000	0x316c4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xce000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
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	0x993b0	0x99400	False	0.594328290681	PGP symmetric key encrypted data - Plaintext or unencrypted data	6.63777304305	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x9c000	0x316c4	0x31800	False	0.430841619318	data	5.94532835965	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xce000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x9c2b0	0x96b5	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0xa5968	0x10828	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0xb6190	0x94a8	data		
RT_ICON	0xbf638	0x5488	data		
RT_ICON	0xc4ac0	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 4294967295, next used block 4294967295		
RT_ICON	0xc8ce8	0x25a8	data		
RT_ICON	0xcb290	0x10a8	data		
RT_ICON	0xcc338	0x988	data		
RT_ICON	0xcccc0	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xcd128	0x84	data		
RT_VERSION	0xcd1ac	0x32c	data		
RT_MANIFEST	0xcd4d8	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

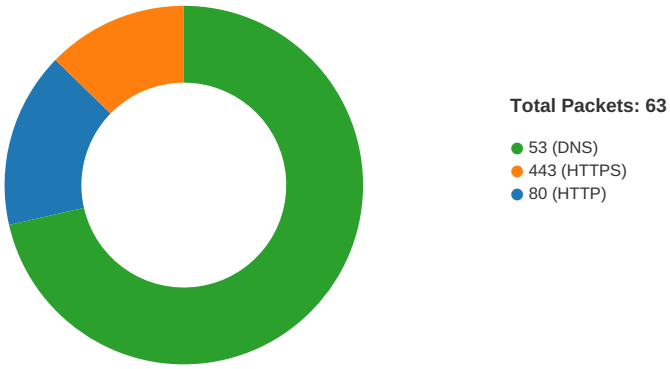
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2016
Assembly Version	1.0.0.0
InternalName	eM.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	Core.Numero
ProductVersion	1.0.0.0
FileDescription	Core.Numero
OriginalFilename	eM.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/23/21-08:12:53.823719	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.6	8.8.8.8

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 08:12:33.058799982 CET	49728	80	192.168.2.6	131.186.161.70
Feb 23, 2021 08:12:33.206585884 CET	80	49728	131.186.161.70	192.168.2.6
Feb 23, 2021 08:12:33.206684113 CET	49728	80	192.168.2.6	131.186.161.70
Feb 23, 2021 08:12:33.207370043 CET	49728	80	192.168.2.6	131.186.161.70
Feb 23, 2021 08:12:33.354996920 CET	80	49728	131.186.161.70	192.168.2.6
Feb 23, 2021 08:12:33.355112076 CET	80	49728	131.186.161.70	192.168.2.6
Feb 23, 2021 08:12:33.355133057 CET	80	49728	131.186.161.70	192.168.2.6
Feb 23, 2021 08:12:33.355236053 CET	49728	80	192.168.2.6	131.186.161.70
Feb 23, 2021 08:12:33.356626034 CET	49728	80	192.168.2.6	131.186.161.70
Feb 23, 2021 08:12:33.504230022 CET	80	49728	131.186.161.70	192.168.2.6
Feb 23, 2021 08:12:33.671633005 CET	49729	80	192.168.2.6	131.186.161.70
Feb 23, 2021 08:12:33.814733982 CET	80	49729	131.186.161.70	192.168.2.6
Feb 23, 2021 08:12:33.818516016 CET	49729	80	192.168.2.6	131.186.161.70
Feb 23, 2021 08:12:33.818556070 CET	49729	80	192.168.2.6	131.186.161.70
Feb 23, 2021 08:12:33.961563110 CET	80	49729	131.186.161.70	192.168.2.6
Feb 23, 2021 08:12:33.961786032 CET	80	49729	131.186.161.70	192.168.2.6
Feb 23, 2021 08:12:33.961798906 CET	80	49729	131.186.161.70	192.168.2.6
Feb 23, 2021 08:12:33.966720104 CET	49729	80	192.168.2.6	131.186.161.70
Feb 23, 2021 08:12:33.966780901 CET	49729	80	192.168.2.6	131.186.161.70
Feb 23, 2021 08:12:34.109927893 CET	80	49729	131.186.161.70	192.168.2.6
Feb 23, 2021 08:12:36.613445044 CET	49732	443	192.168.2.6	104.21.19.200
Feb 23, 2021 08:12:36.654305935 CET	443	49732	104.21.19.200	192.168.2.6
Feb 23, 2021 08:12:36.654407978 CET	49732	443	192.168.2.6	104.21.19.200
Feb 23, 2021 08:12:36.738008976 CET	49732	443	192.168.2.6	104.21.19.200
Feb 23, 2021 08:12:36.778861046 CET	443	49732	104.21.19.200	192.168.2.6
Feb 23, 2021 08:12:36.779741049 CET	443	49732	104.21.19.200	192.168.2.6
Feb 23, 2021 08:12:36.779773951 CET	443	49732	104.21.19.200	192.168.2.6
Feb 23, 2021 08:12:36.779897928 CET	49732	443	192.168.2.6	104.21.19.200
Feb 23, 2021 08:12:36.793313026 CET	49732	443	192.168.2.6	104.21.19.200
Feb 23, 2021 08:12:36.834214926 CET	443	49732	104.21.19.200	192.168.2.6
Feb 23, 2021 08:12:36.834311962 CET	443	49732	104.21.19.200	192.168.2.6
Feb 23, 2021 08:12:36.885832071 CET	49732	443	192.168.2.6	104.21.19.200
Feb 23, 2021 08:12:37.164211035 CET	49732	443	192.168.2.6	104.21.19.200
Feb 23, 2021 08:12:37.206320047 CET	443	49732	104.21.19.200	192.168.2.6
Feb 23, 2021 08:12:37.217717886 CET	443	49732	104.21.19.200	192.168.2.6
Feb 23, 2021 08:12:37.260858059 CET	49732	443	192.168.2.6	104.21.19.200

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 08:11:41.042898893 CET	55074	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 08:11:41.042948008 CET	53	58377	8.8.8.8	192.168.2.6
Feb 23, 2021 08:11:41.089716911 CET	54513	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:11:41.091392040 CET	53	55074	8.8.8.8	192.168.2.6
Feb 23, 2021 08:11:41.138909101 CET	53	54513	8.8.8.8	192.168.2.6
Feb 23, 2021 08:11:42.337898016 CET	62044	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:11:42.386966944 CET	53	62044	8.8.8.8	192.168.2.6
Feb 23, 2021 08:11:43.391204119 CET	63791	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:11:43.452882051 CET	53	63791	8.8.8.8	192.168.2.6
Feb 23, 2021 08:11:43.477947950 CET	64267	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:11:43.526493073 CET	53	64267	8.8.8.8	192.168.2.6
Feb 23, 2021 08:11:44.601594925 CET	49448	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:11:44.652949095 CET	53	49448	8.8.8.8	192.168.2.6
Feb 23, 2021 08:11:45.635008097 CET	60342	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:11:45.686772108 CET	53	60342	8.8.8.8	192.168.2.6
Feb 23, 2021 08:11:46.657526970 CET	61346	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:11:46.709508896 CET	53	61346	8.8.8.8	192.168.2.6
Feb 23, 2021 08:11:47.843038082 CET	51774	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:11:47.891979933 CET	53	51774	8.8.8.8	192.168.2.6
Feb 23, 2021 08:11:48.797451973 CET	56023	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:11:48.846288919 CET	53	56023	8.8.8.8	192.168.2.6
Feb 23, 2021 08:11:50.702054024 CET	58384	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:11:50.754117012 CET	53	58384	8.8.8.8	192.168.2.6
Feb 23, 2021 08:11:51.963953018 CET	60261	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:11:52.026504993 CET	53	60261	8.8.8.8	192.168.2.6
Feb 23, 2021 08:11:53.025890112 CET	56061	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:11:53.074692965 CET	53	56061	8.8.8.8	192.168.2.6
Feb 23, 2021 08:11:54.050085068 CET	58336	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:11:54.101665974 CET	53	58336	8.8.8.8	192.168.2.6
Feb 23, 2021 08:11:55.089487076 CET	53781	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:11:55.138724089 CET	53	53781	8.8.8.8	192.168.2.6
Feb 23, 2021 08:11:56.291686058 CET	54064	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:11:56.342952967 CET	53	54064	8.8.8.8	192.168.2.6
Feb 23, 2021 08:11:57.410840988 CET	52811	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:11:57.461061001 CET	53	52811	8.8.8.8	192.168.2.6
Feb 23, 2021 08:11:58.486507893 CET	55299	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:11:58.537982941 CET	53	55299	8.8.8.8	192.168.2.6
Feb 23, 2021 08:11:59.708019018 CET	63745	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:11:59.756812096 CET	53	63745	8.8.8.8	192.168.2.6
Feb 23, 2021 08:12:01.287244081 CET	50055	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:12:01.338896036 CET	53	50055	8.8.8.8	192.168.2.6
Feb 23, 2021 08:12:18.198642015 CET	61374	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:12:18.250145912 CET	53	61374	8.8.8.8	192.168.2.6
Feb 23, 2021 08:12:32.790579081 CET	50339	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:12:32.843307018 CET	53	50339	8.8.8.8	192.168.2.6
Feb 23, 2021 08:12:32.867288113 CET	63307	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:12:32.916050911 CET	53	63307	8.8.8.8	192.168.2.6
Feb 23, 2021 08:12:36.314872980 CET	49694	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:12:36.368035078 CET	53	49694	8.8.8.8	192.168.2.6
Feb 23, 2021 08:12:36.486615896 CET	54982	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:12:36.535461903 CET	53	54982	8.8.8.8	192.168.2.6
Feb 23, 2021 08:12:36.557137012 CET	50010	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:12:36.608587027 CET	53	50010	8.8.8.8	192.168.2.6
Feb 23, 2021 08:12:37.864195108 CET	63718	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:12:37.914048910 CET	53	63718	8.8.8.8	192.168.2.6
Feb 23, 2021 08:12:47.175699949 CET	62116	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:12:47.234227896 CET	53	62116	8.8.8.8	192.168.2.6
Feb 23, 2021 08:12:52.746474981 CET	63816	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:12:53.763248920 CET	63816	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:12:53.811232090 CET	53	63816	8.8.8.8	192.168.2.6
Feb 23, 2021 08:12:53.823539972 CET	53	63816	8.8.8.8	192.168.2.6
Feb 23, 2021 08:12:54.368508101 CET	55014	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:12:54.427413940 CET	53	55014	8.8.8.8	192.168.2.6
Feb 23, 2021 08:12:55.193805933 CET	62208	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:12:55.262610912 CET	53	62208	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 08:12:56.466254950 CET	57574	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:12:56.519515991 CET	53	57574	8.8.8.8	192.168.2.6
Feb 23, 2021 08:12:57.086797953 CET	51818	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:12:57.151424885 CET	53	51818	8.8.8.8	192.168.2.6
Feb 23, 2021 08:12:57.196923018 CET	56628	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:12:57.256899118 CET	53	56628	8.8.8.8	192.168.2.6
Feb 23, 2021 08:12:57.910900116 CET	60778	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:12:57.972583055 CET	53	60778	8.8.8.8	192.168.2.6
Feb 23, 2021 08:12:58.804559946 CET	53799	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:12:58.861448050 CET	53	53799	8.8.8.8	192.168.2.6
Feb 23, 2021 08:12:59.853691101 CET	54683	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:12:59.914845943 CET	53	54683	8.8.8.8	192.168.2.6
Feb 23, 2021 08:13:00.928369999 CET	59329	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:13:00.987082005 CET	53	59329	8.8.8.8	192.168.2.6
Feb 23, 2021 08:13:01.674340963 CET	64021	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:13:01.731384039 CET	53	64021	8.8.8.8	192.168.2.6
Feb 23, 2021 08:13:03.083286047 CET	56129	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:13:03.140147924 CET	53	56129	8.8.8.8	192.168.2.6
Feb 23, 2021 08:13:19.370528936 CET	58177	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:13:19.433676958 CET	53	58177	8.8.8.8	192.168.2.6
Feb 23, 2021 08:13:19.981214046 CET	50700	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:13:20.048712969 CET	53	50700	8.8.8.8	192.168.2.6
Feb 23, 2021 08:13:23.135993958 CET	54069	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:13:23.187477112 CET	53	54069	8.8.8.8	192.168.2.6
Feb 23, 2021 08:13:45.100763083 CET	61178	53	192.168.2.6	8.8.8.8
Feb 23, 2021 08:13:45.149605989 CET	53	61178	8.8.8.8	192.168.2.6

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Feb 23, 2021 08:12:53.823719025 CET	192.168.2.6	8.8.8.8	d0d3	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 08:12:32.790579081 CET	192.168.2.6	8.8.8.8	0xfaf8	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)
Feb 23, 2021 08:12:32.867288113 CET	192.168.2.6	8.8.8.8	0x7d54	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)
Feb 23, 2021 08:12:36.557137012 CET	192.168.2.6	8.8.8.8	0x9deb	Standard query (0)	freegeoip.app	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 08:12:32.843307018 CET	8.8.8.8	192.168.2.6	0xfaf8	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 08:12:32.843307018 CET	8.8.8.8	192.168.2.6	0xfaf8	No error (0)	checkip.dyndns.com		131.186.161.70	A (IP address)	IN (0x0001)
Feb 23, 2021 08:12:32.843307018 CET	8.8.8.8	192.168.2.6	0xfaf8	No error (0)	checkip.dyndns.com		216.146.43.70	A (IP address)	IN (0x0001)
Feb 23, 2021 08:12:32.843307018 CET	8.8.8.8	192.168.2.6	0xfaf8	No error (0)	checkip.dyndns.com		131.186.113.70	A (IP address)	IN (0x0001)
Feb 23, 2021 08:12:32.843307018 CET	8.8.8.8	192.168.2.6	0xfaf8	No error (0)	checkip.dyndns.com		162.88.193.70	A (IP address)	IN (0x0001)
Feb 23, 2021 08:12:32.843307018 CET	8.8.8.8	192.168.2.6	0xfaf8	No error (0)	checkip.dyndns.com		216.146.43.71	A (IP address)	IN (0x0001)
Feb 23, 2021 08:12:32.916050911 CET	8.8.8.8	192.168.2.6	0x7d54	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 08:12:32.916050911 CET	8.8.8.8	192.168.2.6	0x7d54	No error (0)	checkip.dyndns.com		131.186.161.70	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 08:12:32.916050911 CET	8.8.8.8	192.168.2.6	0x7d54	No error (0)	checkip.dyndns.com		216.146.43.71	A (IP address)	IN (0x0001)
Feb 23, 2021 08:12:32.916050911 CET	8.8.8.8	192.168.2.6	0x7d54	No error (0)	checkip.dyndns.com		216.146.43.70	A (IP address)	IN (0x0001)
Feb 23, 2021 08:12:32.916050911 CET	8.8.8.8	192.168.2.6	0x7d54	No error (0)	checkip.dyndns.com		162.88.193.70	A (IP address)	IN (0x0001)
Feb 23, 2021 08:12:32.916050911 CET	8.8.8.8	192.168.2.6	0x7d54	No error (0)	checkip.dyndns.com		131.186.113.70	A (IP address)	IN (0x0001)
Feb 23, 2021 08:12:36.608587027 CET	8.8.8.8	192.168.2.6	0x9deb	No error (0)	freegeoip.app		104.21.19.200	A (IP address)	IN (0x0001)
Feb 23, 2021 08:12:36.608587027 CET	8.8.8.8	192.168.2.6	0x9deb	No error (0)	freegeoip.app		172.67.188.154	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- checkip.dyndns.org

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49728	131.186.161.70	80	C:\Users\user\Desktop\(appproved)WJO-TT180,pdf.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 08:12:33.207370043 CET	1241	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org Connection: Keep-Alive
Feb 23, 2021 08:12:33.355112076 CET	1242	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 103 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 38 34 2e 31 37 2e 35 32 2e 33 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 84.17.52.38</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49729	131.186.161.70	80	C:\Users\user\Desktop\(appproved)WJO-TT180,pdf.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 08:12:33.818556070 CET	1242	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org
Feb 23, 2021 08:12:33.961786032 CET	1242	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 103 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 38 34 2e 31 37 2e 35 32 2e 33 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 84.17.52.38</body></html>

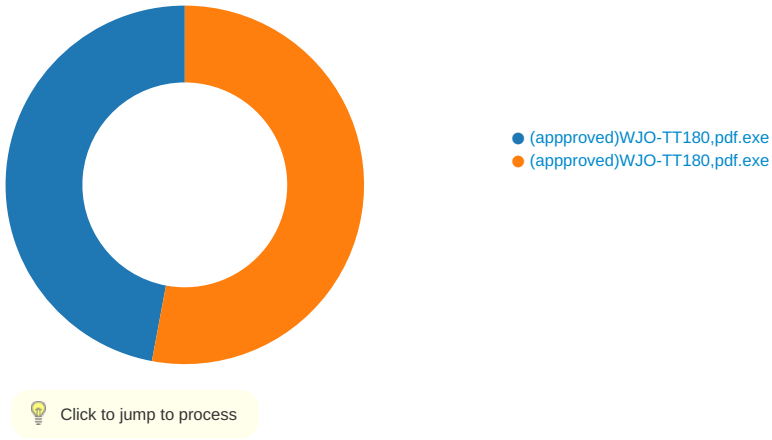
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 23, 2021 08:12:36.779773951 CET	104.21.19.200	443	192.168.2.6	49732	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Aug 10 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Tue Aug 10 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	769,49162-49161-49172-49171-53-47-10,0-10-11-35-23-65281,29-23-24,0	54328bd36c14bd82ddaa0c04b25ed9ad
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: (appproved)WJO-TT180,pdf.exe PID: 6808 Parent PID: 5916

General

Start time:	08:11:47
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\(appproved)WJO-TT180,pdf.exe
Wow64 process (32bit):	true
Commandline:	'(appproved)WJO-TT180,pdf.exe'
Imagebase:	0x7ffd88dc0000
File size:	831488 bytes
MD5 hash:	E47851C94FDEFD958CFE16AF2AF3661A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_BedsObfuscator, Description: Yara detected Beds Obfuscator, Source: 00000000.00000002.419975488.0000000003509000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000000.00000002.419975488.0000000003509000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_BedsObfuscator, Description: Yara detected Beds Obfuscator, Source: 00000000.00000002.420374422.0000000003769000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000000.00000002.420374422.0000000003769000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E11CF06	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	6E11CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\(appproved)WJO-TT180,pdf.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E42C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\(appproved)WJO-TT180,pdf.exe.log	unknown	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 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",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6E42C907	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	6E0F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0F5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0FCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF61B4F	ReadFile

Analysis Process: (appproved)WJO-TT180,pdf.exe PID: 5604 Parent PID: 6808

General

Start time:	08:12:27
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\(appproved)WJO-TT180,pdf.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x7ffd88dc0000
File size:	831488 bytes
MD5 hash:	E47851C94FDEFD958CFE16AF2AF3661A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_BedsObfuscator, Description: Yara detected Beds Obfuscator, Source: 00000009.00000002.595511779.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000009.00000002.595511779.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E11CF06	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	6E11CF06	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies\container.dat	success or wait	1	6CF66A95	DeleteFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies\deprecated.cookie	success or wait	1	6CF66A95	DeleteFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	success or wait	1	6CF66A95	DeleteFileW

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	6E0F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0F5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0FCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF61B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CF61B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis