ID: 356562
Sample Name: OC 136584.PDF.exe
Cookbook: default.jbs
Time: 10:13:25
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

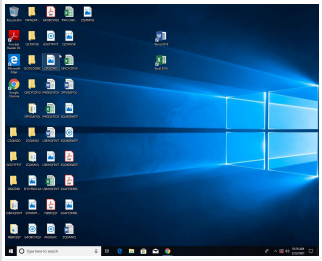
Analysis Report OC 136584.PDF.exe

Overview

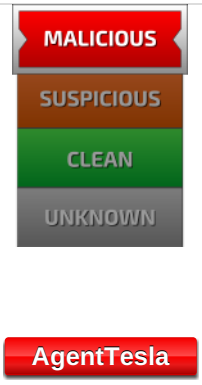
General Information

Sample Name:	OC 136584.PDF.exe
Analysis ID:	356562
MD5:	cd02744201573e..
SHA1:	3d39dd04c23ba5..
SHA256:	559bf7a1059928b.
Tags:	AgentTesla exe

Most interesting Screenshot:



Detection



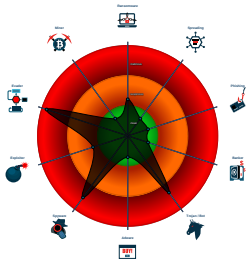
AgentTesla

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

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Sigma detected: Suspicious Double …
- Yara detected AgentTesla
- Yara detected AntiVM_3
- .NET source code contains potentia…
- .NET source code contains very larg…
- .NET source code contains very larg…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Installs a global keyboard hook
- Machine Learning detection for samp…
- Moves itself to temp directory

Classification



Startup

- **System is w10x64**
- OC 136584.PDF.exe (PID: 6736 cmdline: 'C:\Users\user\Desktop\OC 136584.PDF.exe' MD5: CD02744201573E3AC3C7DFDE851005F3)
  - OC 136584.PDF.exe (PID: 6988 cmdline: C:\Users\user\Desktop\OC 136584.PDF.exe MD5: CD02744201573E3AC3C7DFDE851005F3)
  - OC 136584.PDF.exe (PID: 6996 cmdline: C:\Users\user\Desktop\OC 136584.PDF.exe MD5: CD02744201573E3AC3C7DFDE851005F3)
  - OC 136584.PDF.exe (PID: 7124 cmdline: C:\Users\user\Desktop\OC 136584.PDF.exe MD5: CD02744201573E3AC3C7DFDE851005F3)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.262677197.000000000251 1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000006.00000002.498958297.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.266834340.000000000351 9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000006.00000002.505611814.0000000002BF 1000.00000004.00000001.sdmp	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	
00000000.00000002.262887194.000000000254 D000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Click to see the 4 entries

Unpacked PEs

Source	Rule	Description	Author	Strings

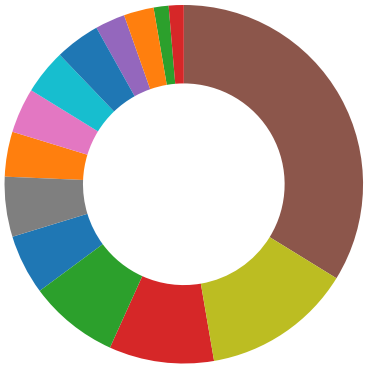
Source	Rule	Description	Author	Strings
0.2.OC 136584.PDF.exe.2539e90.1.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
6.2.OC 136584.PDF.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.OC 136584.PDF.exe.37e4050.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.OC 136584.PDF.exe.36e3da0.4.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.OC 136584.PDF.exe.37e4050.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 1 entries				

Sigma Overview

System Summary:

Sigma detected: Suspicious Double Extension

Signature Overview



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

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

Uses secure TLS version for HTTPS connections

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

Networking:

Uses the Telegram API (likely for C&C communication)

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

System Summary:

.NET source code contains very large array initializations

.NET source code contains very large strings

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

Moves itself to temp directory

Uses an obfuscated file name to hide its real file extension (double extension)

Malware Analysis System Evasion:

Yara detected AntiVM_3

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

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

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

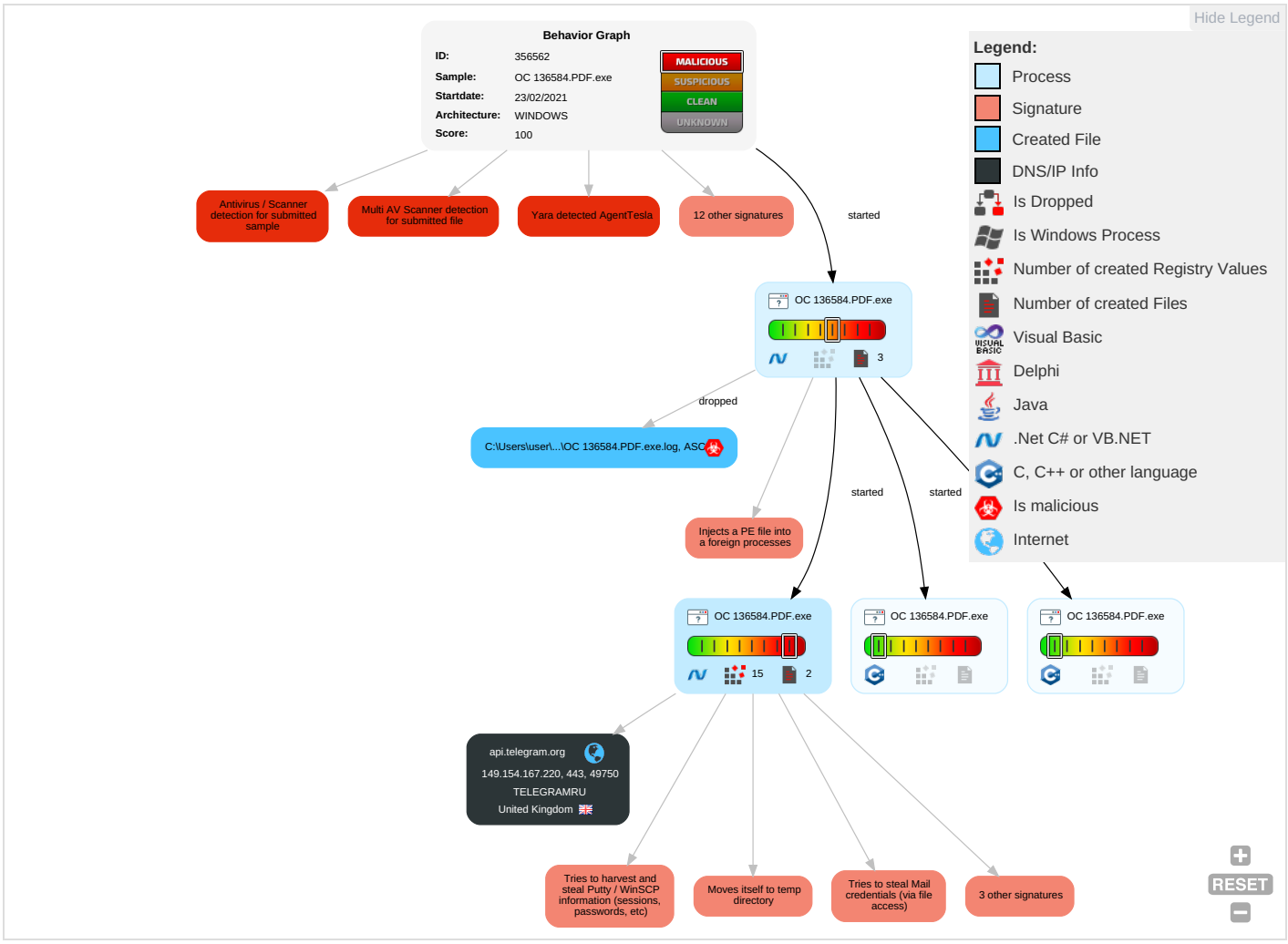
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contro
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1 1 2	Masquerading 2 1	OS Credential Dumping 2	Query Registry 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Web Service 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1 3	Input Capture 1 1	Security Software Discovery 2 1 1	Remote Desktop Protocol	Input Capture 1 1	Exfiltration Over Bluetooth	Encrypted Channel 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Credentials in Registry 1	Virtualization/Sandbox Evasion 1 3	SMB/Windows Admin Shares	Archive Collected Data 1 1	Automated Exfiltration	Non-Application Layer Protocol 1

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contro
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Process Discovery 2	Distributed Component Object Model	Data from Local System 2	Scheduled Transfer	Application Layer Protocol 2
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1 3 1	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communica
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 3	DCSync	System Information Discovery 1 1 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port

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
OC 136584.PDF.exe	14%	Metadefender		Browse
OC 136584.PDF.exe	21%	ReversingLabs	ByteCode-MSIL.Backdoor.Androm	
OC 136584.PDF.exe	100%	Avira	HEUR/AGEN.1138558	
OC 136584.PDF.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.OC 136584.PDF.exe.190000.0.unpack	100%	Avira	HEUR/AGEN.1138558		Download File
4.0.OC 136584.PDF.exe.10000.0.unpack	100%	Avira	HEUR/AGEN.1138558		Download File
3.0.OC 136584.PDF.exe.190000.0.unpack	100%	Avira	HEUR/AGEN.1138558		Download File
6.2.OC 136584.PDF.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
6.0.OC 136584.PDF.exe.5f0000.0.unpack	100%	Avira	HEUR/AGEN.1138558		Download File
0.2.OC 136584.PDF.exe.140000.0.unpack	100%	Avira	HEUR/AGEN.1138558		Download File
6.2.OC 136584.PDF.exe.5f0000.1.unpack	100%	Avira	HEUR/AGEN.1138558		Download File
0.0.OC 136584.PDF.exe.140000.0.unpack	100%	Avira	HEUR/AGEN.1138558		Download File
4.2.OC 136584.PDF.exe.10000.0.unpack	100%	Avira	HEUR/AGEN.1138558		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	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://https://api.telegram.org4Zk	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	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://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	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://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	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://mIjlctNEsyMKGExgO3.org	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	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	

Source	Detection	Scanner	Label	Link
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	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.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
api.telegram.org	149.154.167.220	true	false		high

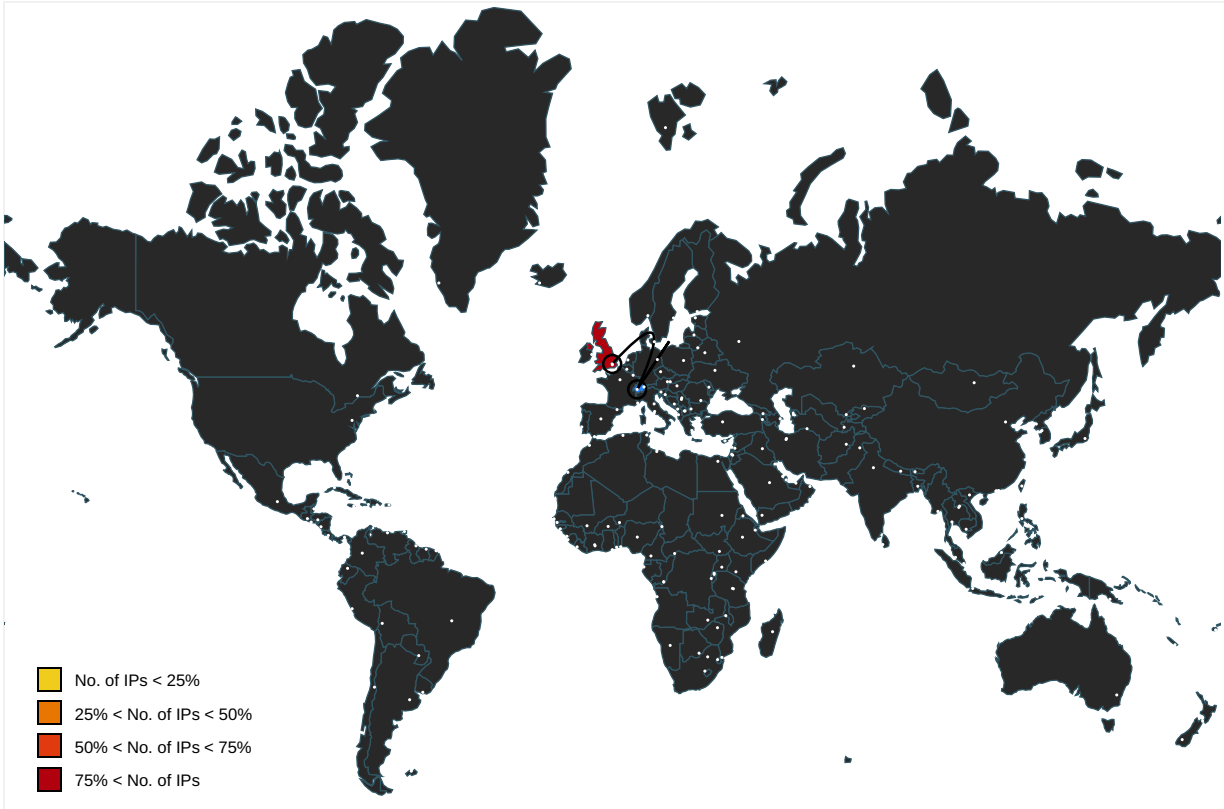
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	OC 136584.PDF.exe, 00000006.00000002.505611814.0000000002BF1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.apache.org/licenses/LICENSE-2.0	OC 136584.PDF.exe, 00000000.00000002.270062469.00000000066A2000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com	OC 136584.PDF.exe, 00000000.00000002.270062469.00000000066A2000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	OC 136584.PDF.exe, 00000000.00000002.270062469.00000000066A2000.00000004.00000001.sdmp	false		high
http://DynDns.comDynDNS	OC 136584.PDF.exe, 00000006.00000002.505611814.0000000002BF1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	OC 136584.PDF.exe, 00000000.00000002.270062469.00000000066A2000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	OC 136584.PDF.exe, 00000000.00000002.270062469.00000000066A2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.telegram.org	OC 136584.PDF.exe, 00000006.00000002.510324365.0000000002EBA000.00000004.00000001.sdmp	false		high
http://https://api.telegram.org4Zk	OC 136584.PDF.exe, 00000006.00000002.510324365.0000000002EBA000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	OC 136584.PDF.exe, 00000006.00000002.505611814.0000000002BF1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://certificates.godaddy.com/repository/0	OC 136584.PDF.exe, 00000006.00000002.510407923.0000000002ECD000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers?	OC 136584.PDF.exe, 00000000.00000002.270062469.00000000066A2000.00000004.00000001.sdmp	false		high
http://certs.godaddy.com/repository/1301	OC 136584.PDF.exe, 00000006.00000002.510407923.0000000002ECD000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://api.telegram.org/bot1683948232:AAHc7uMmgJY5DzV0V0BhJXUizPMr1l1dubE/	OC 136584.PDF.exe, 00000000.00000002.266834340.0000000003519000.00000004.00000001.sdmp, OC 136584.PDF.exe, 00000006.00000002.498958297.0000000000402000.00000040.00000001.sdmp	false		high
http://www.tiro.com	OC 136584.PDF.exe, 00000000.00000002.270062469.00000000066A2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.godaddy.com/gdig2s1-1823.crl0	OC 136584.PDF.exe, 00000006.00000002.510407923.0000000002ECD000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers	OC 136584.PDF.exe, 00000000.00000002.270062469.00000000066A2000.00000004.00000001.sdmp	false		high
http://https://certs.godaddy.com/repository/0	OC 136584.PDF.exe, 00000006.00000002.510407923.0000000002ECD000.00000004.00000001.sdmp	false		high
http://www.goodfont.co.kr	OC 136584.PDF.exe, 00000000.00000002.270062469.00000000066A2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	OC 136584.PDF.exe, 00000000.00000002.262677197.0000000002511000.00000004.00000001.sdmp	false		high
http://www.carterandcone.coml	OC 136584.PDF.exe, 00000000.00000002.270062469.00000000066A2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	OC 136584.PDF.exe, 00000000.00000002.270062469.00000000066A2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	OC 136584.PDF.exe, 00000000.00000002.270062469.00000000066A2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.godaddy.com/gdroot-g2.crl0F	OC 136584.PDF.exe, 00000006.00000002.510407923.0000000002ECD000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/cabarga.htmlN	OC 136584.PDF.exe, 00000000.00000002.270062469.00000000066A2000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	OC 136584.PDF.exe, 00000000.00000002.270062469.00000000066A2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	OC 136584.PDF.exe, 00000000.00000002.270062469.00000000066A2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	OC 136584.PDF.exe, 00000000.00000002.270062469.00000000066A2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	OC 136584.PDF.exe, 00000000.00000002.270062469.00000000066A2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	OC 136584.PDF.exe, 00000000.00000002.270062469.00000000066A2000.00000004.00000001.sdmp	false		high
http://mIjlctNEsyMKGExgO3.org	OC 136584.PDF.exe, 00000006.00000002.505611814.0000000002BF1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	OC 136584.PDF.exe, 00000000.00000002.270062469.00000000066A2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.godaddy.com/gdroot.crl0F	OC 136584.PDF.exe, 00000006.00000002.510407923.0000000002ECD000.00000004.00000001.sdmp	false		high
http://www.galapagosdesign.com/DPlease	OC 136584.PDF.exe, 00000000.00000002.270062469.00000000066A2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	OC 136584.PDF.exe, 00000000.00000002.270062469.00000000066A2000.00000004.00000001.sdmp	false		high
http://www.fonts.com	OC 136584.PDF.exe, 00000000.00000002.270062469.00000000066A2000.00000004.00000001.sdmp	false		high
http://www.sandoll.co.kr	OC 136584.PDF.exe, 00000000.00000002.270062469.00000000066A2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	OC 136584.PDF.exe, 00000000.00000002.270062469.00000000066A2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.zhongyicts.com.cn	OC 136584.PDF.exe, 00000000.00000002.270062469.00000000066A2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://api.telegram.org	OC 136584.PDF.exe, 00000006.00000002.510407923.0000000002ECD000.00000004.00000001.sdmp	false		high
http://certificates.godaddy.com/repository/gdig2.crt0	OC 136584.PDF.exe, 00000006.00000002.510407923.0000000002ECD000.00000004.00000001.sdmp	false		high
http://https://api.telegram.org/bot1683948232:AAHc7uMmgJY5DzV0V0BhJXUizPMr1l1dubE/sendDocument	OC 136584.PDF.exe, 00000006.00000002.510324365.0000000002EBA000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	OC 136584.PDF.exe, 00000006.00000002.510324365.0000000002EBA000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	OC 136584.PDF.exe, 00000000.00000002.270062469.00000000066A2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	OC 136584.PDF.exe, 00000000.00000002.266834340.0000000003519000.00000004.00000001.sdmp, OC 136584.PDF.exe, 00000006.00000002.498958297.000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.telegram.org/bot1683948232:AAHc7uMmgJY5DzV0V0BhJXUizPMr1l1dubE/sendDocumentdocument-----	OC 136584.PDF.exe, 00000006.00000002.505611814.0000000002BF1000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
149.154.167.220	unknown	United Kingdom		62041	TELEGRAMRU	false

General Information

Joe Sandbox Version:	31.0.0 Emerald

Analysis ID:	356562
Start date:	23.02.2021
Start time:	10:13:25
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	OC 136584.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:	26
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@7/1@1/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 2.9% (good quality ratio 0%) • Quality average: 0% • Quality standard deviation: 0%
HCA Information:	• Successful, ratio: 99% • 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): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 104.43.139.144, 52.255.188.83, 104.43.193.48, 168.61.161.212, 40.88.32.150, 184.30.20.56, 51.11.168.160, 8.253.207.120, 67.27.157.254, 8.248.131.254, 8.253.204.121, 67.26.83.254, 51.103.5.186, 52.155.217.156, 20.54.26.129, 92.122.213.194, 92.122.213.247, 51.104.139.180 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, wns.notify.trafficmanager.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, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, vip2-par02p.wns.notify.trafficmanager.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 NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/356562/sample/OC 136584.PDF.exe

Simulations

Behavior and APIs

Time	Type	Description
10:14:25	API Interceptor	643x Sleep call for process: OC 136584.PDF.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
149.154.167.220	Quote_13940007.exe	Get hash	malicious	Browse	
	SKBM 0222.exe	Get hash	malicious	Browse	
	crypted.exe	Get hash	malicious	Browse	
	PO-735643-SALES.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	muOvK6dngg.exe	Get hash	malicious	Browse	
	SKBM 0222..exe	Get hash	malicious	Browse	
	PO 86540.exe	Get hash	malicious	Browse	
	Unterlagen PDF.exe	Get hash	malicious	Browse	
	JFAaEh5hB6.exe	Get hash	malicious	Browse	
	BMfiIGROO2.exe	Get hash	malicious	Browse	
	Inv_874520.exe	Get hash	malicious	Browse	
	Inv_95736.scr.exe	Get hash	malicious	Browse	
	purchase_order.exe	Get hash	malicious	Browse	
	RFQ_2345.exe	Get hash	malicious	Browse	
	Rechnung.exe	Get hash	malicious	Browse	
	Shipping_Doc.exe	Get hash	malicious	Browse	
	Purchase_Order16-122020.exe	Get hash	malicious	Browse	
	DHL_Shipment_74683783_Details_Pdf.exe	Get hash	malicious	Browse	
	Pnzyltwcdn1.exe	Get hash	malicious	Browse	
	PO20-001602-1.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
api.telegram.org	Quote_13940007.exe	Get hash	malicious	Browse	• 149.154.167.220
	SKBM 0222.exe	Get hash	malicious	Browse	• 149.154.167.220
	crypted.exe	Get hash	malicious	Browse	• 149.154.167.220
	PO-735643-SALES.exe	Get hash	malicious	Browse	• 149.154.167.220
	muOvK6dngg.exe	Get hash	malicious	Browse	• 149.154.167.220
	SKBM 0222..exe	Get hash	malicious	Browse	• 149.154.167.220
	PO 86540.exe	Get hash	malicious	Browse	• 149.154.167.220
	Unterlagen PDF.exe	Get hash	malicious	Browse	• 149.154.167.220
	JFAaEh5hB6.exe	Get hash	malicious	Browse	• 149.154.167.220
	BMfiIGROO2.exe	Get hash	malicious	Browse	• 149.154.167.220
	Inv_874520.exe	Get hash	malicious	Browse	• 149.154.167.220
	Inv_95736.scr.exe	Get hash	malicious	Browse	• 149.154.167.220
	REVISED_INVOICE_Company_BankDetails_fle_doc.xlsx.exe	Get hash	malicious	Browse	• 149.154.167.220
	purchase_order.exe	Get hash	malicious	Browse	• 149.154.167.220
	RFQ_2345.exe	Get hash	malicious	Browse	• 149.154.167.220
	Rechnung.exe	Get hash	malicious	Browse	• 149.154.167.220
	Shipping_Doc.exe	Get hash	malicious	Browse	• 149.154.167.220
	Purchase_Order16-122020.exe	Get hash	malicious	Browse	• 149.154.167.220
	DHL_Shipment_74683783_Details_Pdf.exe	Get hash	malicious	Browse	• 149.154.167.220
	Pnzyltwcdn1.exe	Get hash	malicious	Browse	• 149.154.167.220

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
TELEGRAMRU	Quote_13940007.exe	Get hash	malicious	Browse	• 149.154.167.220
	SKBM 0222.exe	Get hash	malicious	Browse	• 149.154.167.220
	crypted.exe	Get hash	malicious	Browse	• 149.154.167.220

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO-735643-SALES.exe	Get hash	malicious	Browse	• 149.154.167.220
	muOvK6dngg.exe	Get hash	malicious	Browse	• 149.154.167.220
	SKBM 0222..exe	Get hash	malicious	Browse	• 149.154.167.220
	PO 86540.exe	Get hash	malicious	Browse	• 149.154.167.220
	Unterlagen PDF.exe	Get hash	malicious	Browse	• 149.154.167.220
	JFAaEh5hB6.exe	Get hash	malicious	Browse	• 149.154.167.220
	BMfilGROO2.exe	Get hash	malicious	Browse	• 149.154.167.220
	Inv_874520.exe	Get hash	malicious	Browse	• 149.154.167.220
	Inv_95736.scr.exe	Get hash	malicious	Browse	• 149.154.167.220
	purchase_order.exe	Get hash	malicious	Browse	• 149.154.167.220
	RFQ_2345.exe	Get hash	malicious	Browse	• 149.154.167.220
	Rechnung.exe	Get hash	malicious	Browse	• 149.154.167.220
	Shipping_Doc.exe	Get hash	malicious	Browse	• 149.154.167.220
	Purchase_Order16-122020.exe	Get hash	malicious	Browse	• 149.154.167.220
	DHL_Shipment_74683783_Details_Pdf.exe	Get hash	malicious	Browse	• 149.154.167.220
	Pnzyltwcdn1.exe	Get hash	malicious	Browse	• 149.154.167.220
	PO20-001602-1.exe	Get hash	malicious	Browse	• 149.154.167.220

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
3b5074b1b5d032e5620f69f9f700ff0e	Quote_13940007.exe	Get hash	malicious	Browse	• 149.154.167.220
	SecuriteInfo.com.Variant.Zusy.368685.25618.exe	Get hash	malicious	Browse	• 149.154.167.220
	SKBM 0222.exe	Get hash	malicious	Browse	• 149.154.167.220
	8WjU4jrBlr.exe	Get hash	malicious	Browse	• 149.154.167.220
	crypted.exe	Get hash	malicious	Browse	• 149.154.167.220
	PO-735643-SALES.exe	Get hash	malicious	Browse	• 149.154.167.220
	SecuriteInfo.com.Mal.Generic-S.15142.exe	Get hash	malicious	Browse	• 149.154.167.220
	LIQUIDACION INTERBANCARIA 02_22_2021.xls	Get hash	malicious	Browse	• 149.154.167.220
	muOvK6dngg.exe	Get hash	malicious	Browse	• 149.154.167.220
	SKBM 0222..exe	Get hash	malicious	Browse	• 149.154.167.220
	Vessel Line Up 7105082938.exe	Get hash	malicious	Browse	• 149.154.167.220
	ProtonVPN.exe	Get hash	malicious	Browse	• 149.154.167.220
	PO 86540.exe	Get hash	malicious	Browse	• 149.154.167.220
	RTM DIAS - CTM.exe	Get hash	malicious	Browse	• 149.154.167.220
	uTorrent.exe	Get hash	malicious	Browse	• 149.154.167.220
	hreheh.exe	Get hash	malicious	Browse	• 149.154.167.220
	JFAaEh5hB6.exe	Get hash	malicious	Browse	• 149.154.167.220
	Dmjsru7tdt.exe	Get hash	malicious	Browse	• 149.154.167.220

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Documents_pdf.exe	Get hash	malicious	Browse	• 149.154.167.220
	BANK SWIFT- USD 98,712.00.pdf.exe	Get hash	malicious	Browse	• 149.154.167.220

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\OC 136584.PDF.exe.log

Process:	C:\Users\user\Desktop\OC 136584.PDF.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:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F8
Malicious:	**true**
Reputation:	moderate, 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..2,"Microsoft.VisualBasic, Version=10.0.0.0, 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=b77a

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.505996390400658
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:	OC 136584.PDF.exe
File size:	534528
MD5:	cd02744201573e3ac3c7dfde851005f3
SHA1:	3d39dd04c23ba52ed6f660e51e7510fef647186b
SHA256:	559bf7a1059928bb51ba72f92ff7c8348b219c0bcc92e59376a4d0f553ae3ee7
SHA512:	ff7f72c4847228a217a38a822217de735641476ab6a9430de49c9de2b71d816b5387abc9b290d79e39c2524686db4542688c5b80db39d19d8467f34b3295d1e5
SSDEEP:	12288:mfWysvBqTZ2MUWv4rzPdwFLhFH1rrQBPyBL9wht:mfWyoqTNSvlYzuRyBL
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....4`.....P.....:.. ...@....@.. .....@.....

File Icon

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x483a16
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:	0x6034067F [Mon Feb 22 19:31:11 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x839c4	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x84000	0x620	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x86000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x81a1c	0x81c00	False	0.784209793473	data	7.52188684985	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x84000	0x620	0x800	False	0.33349609375	data	3.46671523025	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x86000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x84090	0x390	data		
RT_MANIFEST	0x84430	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

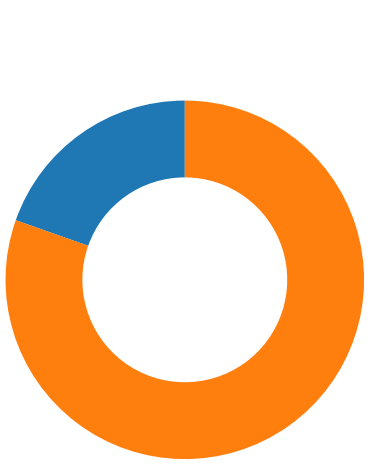
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Microsoft 2014
Assembly Version	1.0.0.0
InternalName	RSAOAEPKeyExchangeDeformatter.exe
FileVersion	1.0.0.0
CompanyName	Microsoft
LegalTrademarks	
Comments	
ProductName	WinClient
ProductVersion	1.0.0.0
FileDescription	WinClient
OriginalFilename	RSAOAEPKeyExchangeDeformatter.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 10:16:14.067445993 CET	49750	443	192.168.2.7	149.154.167.220
Feb 23, 2021 10:16:14.117803097 CET	443	49750	149.154.167.220	192.168.2.7
Feb 23, 2021 10:16:14.119429111 CET	49750	443	192.168.2.7	149.154.167.220
Feb 23, 2021 10:16:14.171078920 CET	49750	443	192.168.2.7	149.154.167.220
Feb 23, 2021 10:16:14.221415043 CET	443	49750	149.154.167.220	192.168.2.7
Feb 23, 2021 10:16:14.221463919 CET	443	49750	149.154.167.220	192.168.2.7
Feb 23, 2021 10:16:14.221487045 CET	443	49750	149.154.167.220	192.168.2.7
Feb 23, 2021 10:16:14.221509933 CET	443	49750	149.154.167.220	192.168.2.7
Feb 23, 2021 10:16:14.221529007 CET	443	49750	149.154.167.220	192.168.2.7
Feb 23, 2021 10:16:14.221612930 CET	49750	443	192.168.2.7	149.154.167.220
Feb 23, 2021 10:16:14.222774982 CET	443	49750	149.154.167.220	192.168.2.7
Feb 23, 2021 10:16:14.222812891 CET	443	49750	149.154.167.220	192.168.2.7
Feb 23, 2021 10:16:14.223772049 CET	49750	443	192.168.2.7	149.154.167.220
Feb 23, 2021 10:16:14.231332064 CET	49750	443	192.168.2.7	149.154.167.220
Feb 23, 2021 10:16:14.281833887 CET	443	49750	149.154.167.220	192.168.2.7
Feb 23, 2021 10:16:14.330393076 CET	49750	443	192.168.2.7	149.154.167.220
Feb 23, 2021 10:16:14.366359949 CET	49750	443	192.168.2.7	149.154.167.220
Feb 23, 2021 10:16:14.417613983 CET	443	49750	149.154.167.220	192.168.2.7
Feb 23, 2021 10:16:14.422624111 CET	49750	443	192.168.2.7	149.154.167.220
Feb 23, 2021 10:16:14.514781952 CET	443	49750	149.154.167.220	192.168.2.7
Feb 23, 2021 10:16:14.548568010 CET	443	49750	149.154.167.220	192.168.2.7
Feb 23, 2021 10:16:14.596049070 CET	49750	443	192.168.2.7	149.154.167.220

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 10:14:08.204071999 CET	56590	53	192.168.2.7	8.8.8.8
Feb 23, 2021 10:14:08.263199091 CET	53	56590	8.8.8.8	192.168.2.7
Feb 23, 2021 10:14:09.277232885 CET	60501	53	192.168.2.7	8.8.8.8
Feb 23, 2021 10:14:09.326216936 CET	53	60501	8.8.8.8	192.168.2.7
Feb 23, 2021 10:14:12.617805004 CET	53775	53	192.168.2.7	8.8.8.8
Feb 23, 2021 10:14:12.669291019 CET	53	53775	8.8.8.8	192.168.2.7
Feb 23, 2021 10:14:14.051386118 CET	51837	53	192.168.2.7	8.8.8.8
Feb 23, 2021 10:14:14.100642920 CET	53	51837	8.8.8.8	192.168.2.7
Feb 23, 2021 10:14:14.987487078 CET	55411	53	192.168.2.7	8.8.8.8
Feb 23, 2021 10:14:15.036165953 CET	53	55411	8.8.8.8	192.168.2.7
Feb 23, 2021 10:14:16.252763033 CET	63668	53	192.168.2.7	8.8.8.8
Feb 23, 2021 10:14:16.310053110 CET	53	63668	8.8.8.8	192.168.2.7
Feb 23, 2021 10:14:17.974282026 CET	54640	53	192.168.2.7	8.8.8.8
Feb 23, 2021 10:14:18.023017883 CET	53	54640	8.8.8.8	192.168.2.7
Feb 23, 2021 10:14:18.775087118 CET	58739	53	192.168.2.7	8.8.8.8
Feb 23, 2021 10:14:18.823709011 CET	53	58739	8.8.8.8	192.168.2.7
Feb 23, 2021 10:14:19.741203070 CET	60338	53	192.168.2.7	8.8.8.8
Feb 23, 2021 10:14:19.790915012 CET	53	60338	8.8.8.8	192.168.2.7
Feb 23, 2021 10:14:20.575700045 CET	58717	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 10:14:20.624413013 CET	53	58717	8.8.8.8	192.168.2.7
Feb 23, 2021 10:14:23.150199890 CET	59762	53	192.168.2.7	8.8.8.8
Feb 23, 2021 10:14:23.208918095 CET	53	59762	8.8.8.8	192.168.2.7
Feb 23, 2021 10:14:24.310127974 CET	54329	53	192.168.2.7	8.8.8.8
Feb 23, 2021 10:14:24.359009981 CET	53	54329	8.8.8.8	192.168.2.7
Feb 23, 2021 10:14:25.192791939 CET	58052	53	192.168.2.7	8.8.8.8
Feb 23, 2021 10:14:25.241801977 CET	53	58052	8.8.8.8	192.168.2.7
Feb 23, 2021 10:14:26.194890022 CET	54008	53	192.168.2.7	8.8.8.8
Feb 23, 2021 10:14:26.243719101 CET	53	54008	8.8.8.8	192.168.2.7
Feb 23, 2021 10:14:30.639187098 CET	59451	53	192.168.2.7	8.8.8.8
Feb 23, 2021 10:14:30.690882921 CET	53	59451	8.8.8.8	192.168.2.7
Feb 23, 2021 10:14:33.303613901 CET	52914	53	192.168.2.7	8.8.8.8
Feb 23, 2021 10:14:33.365236998 CET	53	52914	8.8.8.8	192.168.2.7
Feb 23, 2021 10:14:33.474751949 CET	64569	53	192.168.2.7	8.8.8.8
Feb 23, 2021 10:14:33.523542881 CET	53	64569	8.8.8.8	192.168.2.7
Feb 23, 2021 10:14:34.684807062 CET	52816	53	192.168.2.7	8.8.8.8
Feb 23, 2021 10:14:34.736526966 CET	53	52816	8.8.8.8	192.168.2.7
Feb 23, 2021 10:14:35.984615088 CET	50781	53	192.168.2.7	8.8.8.8
Feb 23, 2021 10:14:36.036494970 CET	53	50781	8.8.8.8	192.168.2.7
Feb 23, 2021 10:14:36.930886030 CET	54230	53	192.168.2.7	8.8.8.8
Feb 23, 2021 10:14:36.982584000 CET	53	54230	8.8.8.8	192.168.2.7
Feb 23, 2021 10:14:37.800461054 CET	54911	53	192.168.2.7	8.8.8.8
Feb 23, 2021 10:14:37.849299908 CET	53	54911	8.8.8.8	192.168.2.7
Feb 23, 2021 10:14:38.692162037 CET	49958	53	192.168.2.7	8.8.8.8
Feb 23, 2021 10:14:38.740888119 CET	53	49958	8.8.8.8	192.168.2.7
Feb 23, 2021 10:14:47.218127966 CET	50860	53	192.168.2.7	8.8.8.8
Feb 23, 2021 10:14:47.269622087 CET	53	50860	8.8.8.8	192.168.2.7
Feb 23, 2021 10:15:03.083425045 CET	50452	53	192.168.2.7	8.8.8.8
Feb 23, 2021 10:15:03.140851974 CET	53	50452	8.8.8.8	192.168.2.7
Feb 23, 2021 10:15:04.790332079 CET	59730	53	192.168.2.7	8.8.8.8
Feb 23, 2021 10:15:04.839184999 CET	53	59730	8.8.8.8	192.168.2.7
Feb 23, 2021 10:15:12.987952948 CET	59310	53	192.168.2.7	8.8.8.8
Feb 23, 2021 10:15:13.051109076 CET	53	59310	8.8.8.8	192.168.2.7
Feb 23, 2021 10:15:13.742677927 CET	51919	53	192.168.2.7	8.8.8.8
Feb 23, 2021 10:15:13.791402102 CET	53	51919	8.8.8.8	192.168.2.7
Feb 23, 2021 10:15:14.403383970 CET	64296	53	192.168.2.7	8.8.8.8
Feb 23, 2021 10:15:14.463449955 CET	53	64296	8.8.8.8	192.168.2.7
Feb 23, 2021 10:15:14.943226099 CET	56680	53	192.168.2.7	8.8.8.8
Feb 23, 2021 10:15:15.000531912 CET	53	56680	8.8.8.8	192.168.2.7
Feb 23, 2021 10:15:15.466594934 CET	58820	53	192.168.2.7	8.8.8.8
Feb 23, 2021 10:15:15.530623913 CET	53	58820	8.8.8.8	192.168.2.7
Feb 23, 2021 10:15:16.061304092 CET	60983	53	192.168.2.7	8.8.8.8
Feb 23, 2021 10:15:16.130430937 CET	53	60983	8.8.8.8	192.168.2.7
Feb 23, 2021 10:15:16.318660975 CET	49247	53	192.168.2.7	8.8.8.8
Feb 23, 2021 10:15:16.375713110 CET	53	49247	8.8.8.8	192.168.2.7
Feb 23, 2021 10:15:17.313102961 CET	52286	53	192.168.2.7	8.8.8.8
Feb 23, 2021 10:15:17.370675087 CET	53	52286	8.8.8.8	192.168.2.7
Feb 23, 2021 10:15:18.210941076 CET	56064	53	192.168.2.7	8.8.8.8
Feb 23, 2021 10:15:18.271023989 CET	53	56064	8.8.8.8	192.168.2.7
Feb 23, 2021 10:15:18.293623924 CET	63744	53	192.168.2.7	8.8.8.8
Feb 23, 2021 10:15:18.357074976 CET	53	63744	8.8.8.8	192.168.2.7
Feb 23, 2021 10:15:19.578265905 CET	61457	53	192.168.2.7	8.8.8.8
Feb 23, 2021 10:15:19.638094902 CET	53	61457	8.8.8.8	192.168.2.7
Feb 23, 2021 10:15:20.239558935 CET	58367	53	192.168.2.7	8.8.8.8
Feb 23, 2021 10:15:20.301743031 CET	53	58367	8.8.8.8	192.168.2.7
Feb 23, 2021 10:15:50.199729919 CET	60599	53	192.168.2.7	8.8.8.8
Feb 23, 2021 10:15:50.264888048 CET	53	60599	8.8.8.8	192.168.2.7
Feb 23, 2021 10:15:53.303788900 CET	59571	53	192.168.2.7	8.8.8.8
Feb 23, 2021 10:15:53.352643967 CET	53	59571	8.8.8.8	192.168.2.7
Feb 23, 2021 10:16:08.229257107 CET	52689	53	192.168.2.7	8.8.8.8
Feb 23, 2021 10:16:08.279499054 CET	53	52689	8.8.8.8	192.168.2.7
Feb 23, 2021 10:16:13.988753080 CET	50290	53	192.168.2.7	8.8.8.8
Feb 23, 2021 10:16:14.040211916 CET	53	50290	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 10:16:13.988753080 CET	192.168.2.7	8.8.8.8	0x5fdc	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 10:16:14.040211916 CET	8.8.8.8	192.168.2.7	0x5fdc	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)

HTTPS Packets

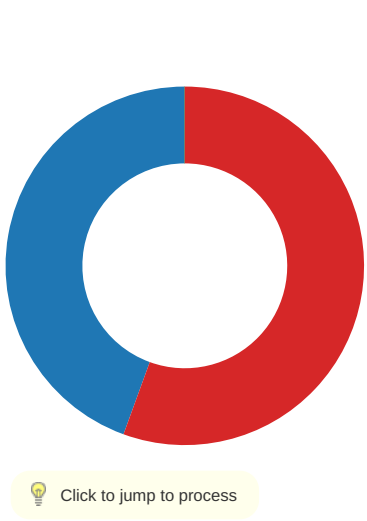
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 23, 2021 10:16:14.222774982 CET	149.154.167.220	443	192.168.2.7	49750	CN=api.telegram.org, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Mar 24 14:48:17 CET 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Mon May 23 18:17:38 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	3b5074b1b5d032e5620f69f9f700ff0e
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		

Code Manipulations

Statistics

Behavior

● OC 136584.PDF.exe
● OC 136584.PDF.exe
● OC 136584.PDF.exe



System Behavior

Analysis Process: OC 136584.PDF.exe PID: 6736 Parent PID: 5784

General

Start time:	10:14:15
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\OC 136584.PDF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\OC 136584.PDF.exe'
Imagebase:	0x140000
File size:	534528 bytes
MD5 hash:	CD02744201573E3AC3C7DFDE851005F3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.262677197.0000000002511000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.266834340.0000000003519000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.262887194.000000000254D000.00000004.00000001.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	6D38CF06	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	6D38CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\OC 136584.PDF.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D69C78D	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\OC 136584.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 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	6D69C907	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	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D365705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D36CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1D1B4F	ReadFile

Analysis Process: OC 136584.PDF.exe PID: 6988 Parent PID: 6736

General

Start time:	10:14:28
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\OC 136584.PDF.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\OC 136584.PDF.exe
Imagebase:	0x190000

File size:	534528 bytes
MD5 hash:	CD02744201573E3AC3C7DFDE851005F3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: OC 136584.PDF.exe PID: 6996 Parent PID: 6736

General

Start time:	10:14:29
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\OC 136584.PDF.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\OC 136584.PDF.exe
Imagebase:	0x10000
File size:	534528 bytes
MD5 hash:	CD02744201573E3AC3C7DFDE851005F3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: OC 136584.PDF.exe PID: 7124 Parent PID: 6736

General

Start time:	10:14:29
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\OC 136584.PDF.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\OC 136584.PDF.exe
Imagebase:	0x5f0000
File size:	534528 bytes
MD5 hash:	CD02744201573E3AC3C7DFDE851005F3
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: 00000006.00000002.498958297.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000006.00000002.505611814.0000000002BF1000.00000004.00000001.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	6D38CF06	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	6D38CF06	unknown

Old File Path	New File Path	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	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D365705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D36CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6C1D1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\d35a2573-25a9-4d93-8ad1-79ec139dd1d8	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C1D1B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis