ID: 383906
Sample Name: Quotation-4834898943949883.pdf.exe
Cookbook: default.jbs
Time: 12:11:06
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

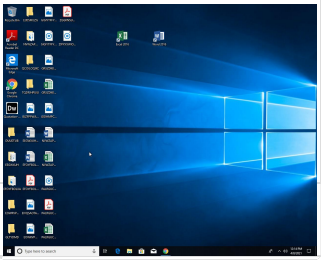
Analysis Report Quotation-4834898943949883.pdf.exe

Overview

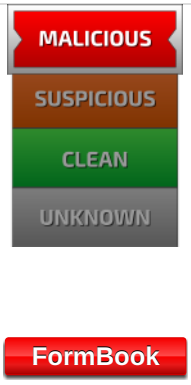
General Information

Sample Name:	Quotation-4834898943949883.pdf.exe
Analysis ID:	383906
MD5:	57055ad7429ef21.
SHA1:	4df1aae070d95c2.
SHA256:	f15085a9037c117.
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection

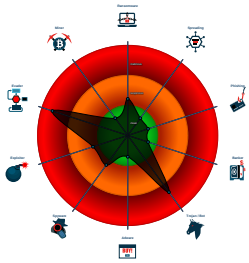


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Yara detected AntiVM3
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Machine Learning detection for samp…
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…

Classification



Startup

- **System is w10x64**
- Quotation-4834898943949883.pdf.exe (PID: 5956 cmdline: 'C:\Users\user\Desktop\Quotation-4834898943949883.pdf.exe' MD5: 57055AD7429EF21CACA78A9428E8A332)
  - Quotation-4834898943949883.pdf.exe (PID: 4120 cmdline: C:\Users\user\Desktop\Quotation-4834898943949883.pdf.exe MD5: 57055AD7429EF21CACA78A9428E8A332)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.mcgeefamilychildcare.com/nc6m/"
  ],
  "decoy": [
    "saltypar.com",
    "most.community",
    "johnmucollection.com",
    "houzzthings.net",
    "onemarketips.com",
    "legalmarketingtx.net",
    "criminalmindeddesign.com",
    "dtrinvesting.com",
    "millertaxpreparation.com",
    "wckfwwehmo.net",
    "begoodmeat.com",
    "tradefinance.fyi",
    "taxbizfunnels.com",
    "learnstartupdesign.com",
    "hxmdelights.com",
    "christiandantrust.faith",
    "dimensionshypnosis.com",
    "261391.com",
    "cancellednot.com",
    "paodanmeng.com",
    "thewayoutbooks.com",
    "halsdraincleaning.com",
    "jumlasx.xyz",
    "sutransformacion.com",
    "abisagne.com",
    "yingjiebj.com",
    "prodgra.com",
    "phone-review24.club",
    "weandvirus.com",
    "thelibertyhomeinspector.com",
    "fuckblarkie.com",
    "tappesupportservices.com",
    "marianiemorazzani.com",
    "skyybluchildkare.info",
    "diysecurityreview.com",
    "insuranceagentwilliams.com",
    "k-yahagigumi.com",
    "b3ourg.xyz",
    "mawhl.net",
    "billionartoffaith.com",
    "tech4thelolo.com",
    "vlvglobal.com",
    "positive-agenda-advisory.com",
    "sdzcsyy.com",
    "jxdiil.com",
    "craicing.com",
    "opinionesymodelos.com",
    "tulsaprintingcompany.com",
    "papaifotografo.com",
    "kalpavasi.com",
    "century21comingsoon.com",
    "bahiaprincipegrand.com",
    "tinwinsolar.ltd",
    "emprenviendo.com",
    "nineykal.com",
    "tam-rh.cat",
    "onlyfanscash.com",
    "florida-sunny.com",
    "workmone.online",
    "sastaafoods.com",
    "financiallyhealthy.life",
    "unudix.com",
    "wwwsumwater.com",
    "iparametricjobs.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.240710316.0000000002D35000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000001.00000002.241153701.0000000003DA3000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000001.00000002.241153701.0000000003DA3000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x936b0:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9392a:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0xc00d0:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0xc034a:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9f44d:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0xcbe6d:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x9ef39:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0xcb959:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x9f54f:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0xcbf6f:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x9f6c7:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xcc0e7:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x94342:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0xc0d62:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x9e1b4:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xcabd4:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9503b:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0xc1a5b:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0xa52bf:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0xd1cdf:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0xa62c2:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000001.00000002.241153701.0000000003DA3000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0xa21e1:$sqlite3step: 68 34 1C 7B E1 • 0xa22f4:$sqlite3step: 68 34 1C 7B E1 • 0xcec01:$sqlite3step: 68 34 1C 7B E1 • 0xced14:$sqlite3step: 68 34 1C 7B E1 • 0xa2210:$sqlite3text: 68 38 2A 90 C5 • 0xa2335:$sqlite3text: 68 38 2A 90 C5 • 0xcec30:$sqlite3text: 68 38 2A 90 C5 • 0xced55:$sqlite3text: 68 38 2A 90 C5 • 0xa2223:$sqlite3blob: 68 53 D8 7F 8C • 0xa234b:$sqlite3blob: 68 53 D8 7F 8C • 0xcec43:$sqlite3blob: 68 53 D8 7F 8C • 0xced6b:$sqlite3blob: 68 53 D8 7F 8C
00000004.00000002.240662044.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 3 entries				

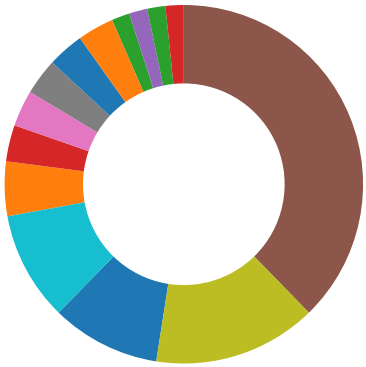
Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.Quotation-4834898943949883.pdf.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
4.2.Quotation-4834898943949883.pdf.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b4f7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c4fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
4.2.Quotation-4834898943949883.pdf.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18419:$sqlite3step: 68 34 1C 7B E1 • 0x1852c:$sqlite3step: 68 34 1C 7B E1 • 0x18448:$sqlite3text: 68 38 2A 90 C5 • 0x1856d:$sqlite3text: 68 38 2A 90 C5 • 0x1845b:$sqlite3blob: 68 53 D8 7F 8C • 0x18583:$sqlite3blob: 68 53 D8 7F 8C
4.2.Quotation-4834898943949883.pdf.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
4.2.Quotation-4834898943949883.pdf.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x977a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa473:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a6f7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b6fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- E-Banking Fraud
- 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 detection for URL or domain

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected AntiVM3

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

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected FormBook

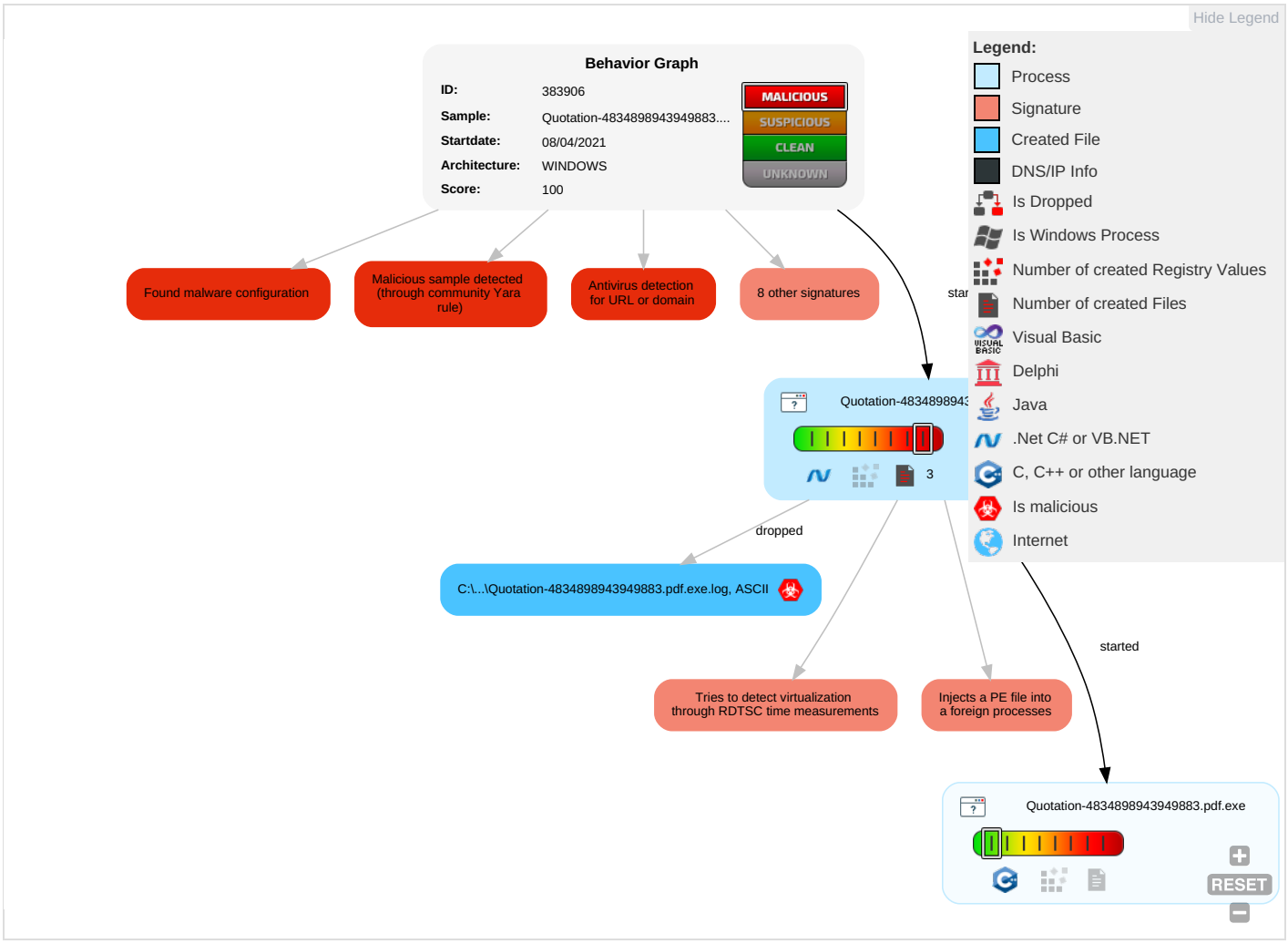
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 1 1	Masquerading 1 1	OS Credential Dumping	Security Software Discovery 2 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communi
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS Redirect F Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS Track Dev Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 1	NTDS	System Information Discovery 1 1 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulat Device Communi
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1 4	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi Access P

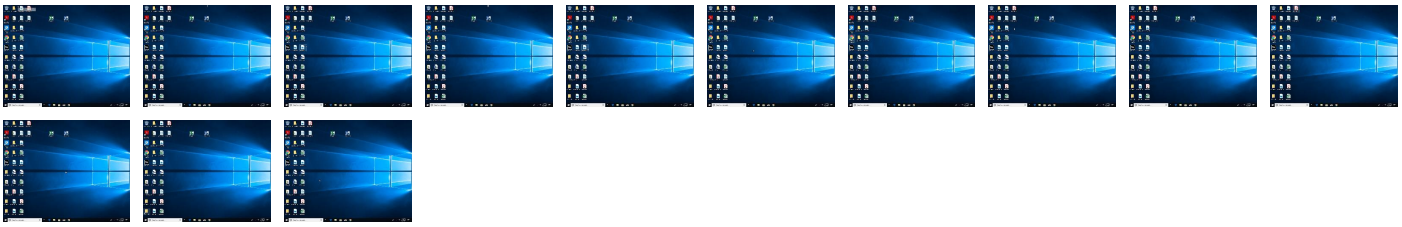
Behavior Graph



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
Quotation-4834898943949883.pdf.exe	27%	Virustotal		Browse
Quotation-4834898943949883.pdf.exe	23%	ReversingLabs	Win32.Trojan.AgentTesla	
Quotation-4834898943949883.pdf.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.Quotation-4834898943949883.pdf.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://tempuri.org/HighScoresDataSet.xsd	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
www.mcgeefamilychildcare.com/nc6m/	100%	Avira URL Cloud	malware	
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://tempuri.org/GridOneHSDataSet.xsd	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	
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://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	
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	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.mcgeefamilychildcare.com/nc6m/	true	• Avira URL Cloud: malware	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://tempuri.org/HighScoresDataSet.xsd	Quotation-4834898943949883.pdf.exe	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	Quotation-4834898943949883.pdf.exe, 00000001.00000002.245213081.000000 0006F12000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com	Quotation-4834898943949883.pdf.exe, 00000001.00000002.245213081.000000 0006F12000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	Quotation-4834898943949883.pdf.exe, 00000001.00000002.245213081.000000 0006F12000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	Quotation-4834898943949883.pdf.exe, 00000001.00000002.245213081.000000 0006F12000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Quotation-4834898943949883.pdf.exe, 00000001.00000002.245213081.000000 0006F12000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	Quotation-4834898943949883.pdf.exe, 00000001.00000002.245213081.000000 0006F12000.00000004.00000001.sdmp	false		high
http://tempuri.org/GridOneHSDataSet.xsd	Quotation-4834898943949883.pdf.exe	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name4	Quotation-4834898943949883.pdf.exe, 00000001.00000002.240759928.000000 0002D72000.00000004.00000001.sdmp	false		high
http://www.tiro.com	Quotation-4834898943949883.pdf.exe, 00000001.00000002.245213081.000000 0006F12000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	Quotation-4834898943949883.pdf.exe, 00000001.00000002.245213081.000000 0006F12000.00000004.00000001.sdmp	false		high
http://www.goodfont.co.kr	Quotation-4834898943949883.pdf.exe, 00000001.00000002.245213081.000000 0006F12000.00000004.00000001.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	Quotation-4834898943949883.pdf.exe, 00000001.00000002.240710316.000000 0002D35000.00000004.00000001.sdmp	false		high
http://www.carterandcone.coml	Quotation-4834898943949883.pdf.exe, 00000001.00000002.245213081.000000 0006F12000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	Quotation-4834898943949883.pdf.exe, 00000001.00000002.245213081.000000 0006F12000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	Quotation-4834898943949883.pdf.exe, 00000001.00000002.245213081.000000 0006F12000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Quotation-4834898943949883.pdf.exe, 00000001.00000002.245213081.000000 0006F12000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	Quotation-4834898943949883.pdf.exe, 00000001.00000002.245213081.000000 0006F12000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Quotation-4834898943949883.pdf.exe, 00000001.00000002.245213081.000000 0006F12000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	Quotation-4834898943949883.pdf.exe, 00000001.00000002.245213081.000000 0006F12000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	Quotation-4834898943949883.pdf.exe, 00000001.00000002.245213081.000000 0006F12000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	Quotation-4834898943949883.pdf.exe, 00000001.00000002.245213081.000000 0006F12000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	Quotation-4834898943949883.pdf.exe, 00000001.00000002.245213081.000000 0006F12000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	Quotation-4834898943949883.pdf.exe, 00000001.00000002.245213081.000000 0006F12000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	Quotation-4834898943949883.pdf.exe, 00000001.00000002.245213081.000000 0006F12000.00000004.00000001.sdmp	false		high
http://www.fonts.com	Quotation-4834898943949883.pdf.exe, 00000001.00000002.245213081.000000 0006F12000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sandoll.co.kr	Quotation-4834898943949883.pdf.exe, 00000001.00000002.245213081.0000000006F12000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	Quotation-4834898943949883.pdf.exe, 00000001.00000002.245213081.0000000006F12000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	Quotation-4834898943949883.pdf.exe, 00000001.00000002.245213081.0000000006F12000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Quotation-4834898943949883.pdf.exe, 00000001.00000002.240759928.0000000002D72000.00000004.00000001.sdmp, Quotation-4834898943949883.pdf.exe, 00000001.00000002.240654193.0000000002CE1000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	Quotation-4834898943949883.pdf.exe, 00000001.00000002.245213081.0000000006F12000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383906
Start date:	08.04.2021
Start time:	12:11:06
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Quotation-4834898943949883.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:	28
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.evad.winEXE@3/1@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 4.8% (good quality ratio 4.7%) • Quality average: 79.7% • Quality standard deviation: 23.6%
HCA Information:	• Successful, ratio: 90% • 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, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
12:12:09	API Interceptor	1x Sleep call for process: Quotation-4834898943949883.pdf.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Quotation-4834898943949883.pdf.exe.log

Process:	C:\Users\user\Desktop\Quotation-4834898943949883.pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Quotation-4834898943949883.pdf.exe.log	
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..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=b77a

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.595750596480351
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:	Quotation-4834898943949883.pdf.exe
File size:	681472
MD5:	57055ad7429ef21caca78a9428e8a332
SHA1:	4df1aae070d95c2fd6c40ba3070a2af53462f3e6
SHA256:	f15085a9037c117355a6b500780d5df0530a6c6724e4506622565b4c13582876
SHA512:	afe126a28e09f69f5c4cb255a9baaa92ae94ca07ae7c93e257a4e7f9b1907d8c651b89bc938b11ba23244a1d32941e47b8ae1268a6ce342148d3653c16c5d7af
SSDEEP:	12288:kRRKtxL91LEPkJP/QHV6OcreeaAvV5vEqfkeH7zEfi/22A/4:kRREP1WkGV6/rxV5vEqfkiAq/e
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...I{n`.....P.. ...D.....N9... ...@....@.. ....@.....

File Icon

	
Icon Hash:	2b014c5a4a450127

Static PE Info

General

Entrypoint:	0x4a394e
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:	0x606E7B49 [Thu Apr 8 03:40:57 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 dword ptr [eax], eax
add byte ptr [eax], al
add al, byte ptr [eax]
add byte ptr [eax], al
or byte ptr [eax], al
add byte ptr [eax], al
or eax, 0C000000h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax+eax], al
add byte ptr [eax], al
pop es
add byte ptr [eax], al
add byte ptr [esi], al
add byte ptr [eax], al
add byte ptr [edx], cl
add byte ptr [eax], al
add byte ptr [esi], cl
add byte ptr [eax], al
add byte ptr [eax], cl
add byte ptr [eax], al
add byte ptr [eax+eax], cl
add byte ptr [eax], al
push cs
add byte ptr [eax], al
add byte ptr [esi], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [esi], cl
add byte ptr [eax], al
add byte ptr [ecx], cl
add byte ptr [eax], al
add byte ptr [eax], cl
add byte ptr [eax], al
add byte ptr [ebx], al
add byte ptr [eax], al
add byte ptr [esi], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax+eax], al
add byte ptr [eax], al
pop es
add byte ptr [eax], al
add byte ptr [eax+eax], cl
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add al, byte ptr [eax]
add byte ptr [eax], al
push es
add byte ptr [eax], al
add byte ptr [edx], cl
add byte ptr [eax], al
add byte ptr [eax+eax], al
add byte ptr [eax], al
or al, byte ptr [eax]
add byte ptr [eax], al
push cs
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 [ecx], cl
add byte ptr [eax], al
add byte ptr [eax+eax], cl
add byte ptr [eax], al
add eax, 00000000h
add byte ptr [eax], al
add byte ptr [ebx], al
add byte ptr [eax], al
add byte ptr [eax+eax], al
add byte ptr [eax], al
or eax, dword ptr [eax]
add byte ptr [eax], al
or eax, dword ptr [eax]
add byte ptr [eax], al
or al, 00h
add byte ptr [eax], al
or eax, 02000000h
add byte ptr [eax], al
add byte ptr [ecx], al
add byte ptr [eax], al
add byte ptr [edx], al
add byte ptr [eax], al
add byte ptr [esi], cl
add byte ptr [eax], al
add byte ptr [00000000h], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xa38fc	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xa4000	0x41a8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xaa000	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	0xa1e84	0xa2000	False	0.781325352045	data	7.61748315782	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xa4000	0x41a8	0x4200	False	0.222478693182	data	4.4812106987	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xaa000	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	0xa4190	0x468	GLS_BINARY_LSB_FIRST		

Name	RVA	Size	Type	Language	Country
RT_ICON	0xa45f8	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 4294967295, next used block 4294967295		
RT_ICON	0xa56a0	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 4294967295, next used block 4294967295		
RT_GROUP_ICON	0xa7c48	0x30	data		
RT_VERSION	0xa7c78	0x344	data		
RT_MANIFEST	0xa7fbc	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 2015
Assembly Version	1.0.0.0
InternalName	ReadBufferAsyncd97.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	Codewords
ProductVersion	1.0.0.0
FileDescription	Codewords
OriginalFilename	ReadBufferAsyncd97.exe

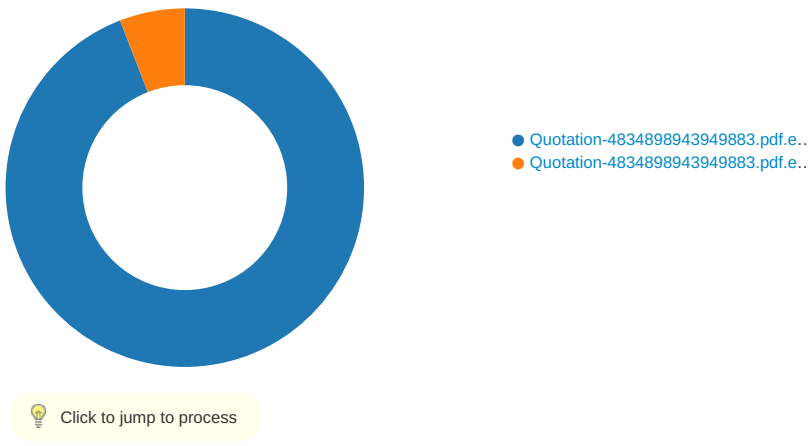
Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Quotation-4834898943949883.pdf.exe PID: 5956 Parent PID: 5488

General

Start time:	12:12:01
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\Quotation-4834898943949883.pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Quotation-4834898943949883.pdf.exe'
Imagebase:	0x940000
File size:	681472 bytes
MD5 hash:	57055AD7429EF21CACA78A9428E8A332
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: 00000001.00000002.240710316.0000000002D35000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.241153701.0000000003DA3000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.241153701.0000000003DA3000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.241153701.0000000003DA3000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
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	6E0FCF06	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	6E0FCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Quotation-4834898943949883.pdf.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E40C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Quotation-4834898943949883.pdf.exe.log	unknown	1314	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 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	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6E40C907	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	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0D5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0DCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF41B4F	ReadFile

Analysis Process: Quotation-4834898943949883.pdf.exe PID: 4120 Parent PID: 5956

General

Start time:	12:12:11
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\Quotation-4834898943949883.pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Quotation-4834898943949883.pdf.exe
Imagebase:	0x970000
File size:	681472 bytes
MD5 hash:	57055AD7429EF21CACA78A9428E8A332
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.240662044.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.240662044.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.240662044.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	41A027	NtReadFile

Disassembly

Code Analysis