ID: 356476
Sample Name: FOB offer_1164087223_I0133P2100363812.PDF.exe
Cookbook: default.jbs
Time: 08:35:51
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

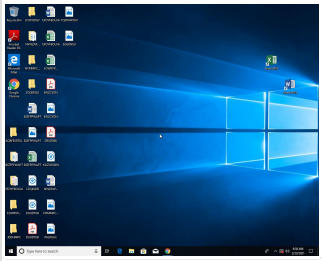
Analysis Report FOB offer_1164087223_I0133P2100363…

Overview

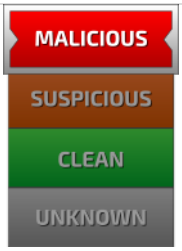
General Information

Sample Name:	FOB offer_1164087223_I0133P2100363812.PDF.exe
Analysis ID:	356476
MD5:	b10eafcd59bf5d8..
SHA1:	ba5b3ade8e66f73.
SHA256:	e2a36e86351414..
Tags:	exe SnakeKeylogger

Most interesting Screenshot:



Detection



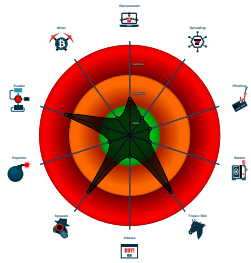
Snake Keylogger

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

Signatures

- Found malware configuration
- Sigma detected: Suspicious Double …
- Yara detected Snake Keylogger
- Binary contains a suspicious time st…
- Initial sample is a PE file and has a …
- Machine Learning detection for samp…
- May check the online IP address of …
- Moves itself to temp directory
- Tries to harvest and steal browser in…
- Tries to harvest and steal ftp login c…
- Tries to steal Mail credentials (via fil…
- Uses an obfuscated file name to hid…
- Yara detected Beds Obfuscator

Classification



Startup

- **System is w10x64**
- FOB offer_1164087223_I0133P2100363812.PDF.exe (PID: 6436 cmdline: 'C:\Users\user\Desktop\FOB offer_1164087223_I0133P2100363812.PDF.exe' MD5: B10EAFCD59BF5D8B5FCAEA7175343DA7)
  - FOB offer_1164087223_I0133P2100363812.PDF.exe (PID: 6484 cmdline: C:\Users\user\Desktop\FOB offer_1164087223_I0133P2100363812.PDF.exe MD5: B10EAFCD59BF5D8B5FCAEA7175343DA7)
- **cleanup**

Malware Configuration

Threatname: Snake Keylogger

```
{
  "Exfil Mode": "Telegram",
  "Telegram Info": {
    "Telegram ID": "1269002131",
    "Telegram Token": "1647674293:AAGNVWUWKyHBC371hZtzAT17lVk_md2UWO8"
  }
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.240971373.000000000543 9000.00000004.00000001.sdmp	JoeSecurity_BedsObfuscat or	Yara detected Beds Obfuscator	Joe Security	
00000000.00000002.240971373.000000000543 9000.00000004.00000001.sdmp	JoeSecurity_SnakeKeylog ger	Yara detected Snake Keylogger	Joe Security	
00000001.00000002.495602752.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_BedsObfuscat or	Yara detected Beds Obfuscator	Joe Security	
00000001.00000002.495602752.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_SnakeKeylog ger	Yara detected Snake Keylogger	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.235333402.00000000044A9000.00000004.00000001.sdmp	JoeSecurity_BedsObfuscator	Yara detected Beds Obfuscator	Joe Security	
Click to see the 9 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.FOB offer_1164087223_I0133P2100363812.PDF.exe.5138fb8.5.raw.unpack	JoeSecurity_BedsObfuscator	Yara detected Beds Obfuscator	Joe Security	
0.2.FOB offer_1164087223_I0133P2100363812.PDF.exe.5138fb8.5.raw.unpack	JoeSecurity_SnakeKeylogger	Yara detected Snake Keylogger	Joe Security	
0.2.FOB offer_1164087223_I0133P2100363812.PDF.exe.47d9340.4.unpack	JoeSecurity_BedsObfuscator	Yara detected Beds Obfuscator	Joe Security	
0.2.FOB offer_1164087223_I0133P2100363812.PDF.exe.4b09170.3.unpack	JoeSecurity_BedsObfuscator	Yara detected Beds Obfuscator	Joe Security	
0.2.FOB offer_1164087223_I0133P2100363812.PDF.exe.63b0000.8.raw.unpack	JoeSecurity_BedsObfuscator	Yara detected Beds Obfuscator	Joe Security	
Click to see the 7 entries				

Sigma Overview

System Summary:

Sigma detected: Suspicious Double Extension

Signature Overview

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

Click to jump to signature section

AV Detection:

Found malware configuration

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

Uses insecure TLS / SSL version for HTTPS connection

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

Binary contains paths to debug symbols

Networking:

May check the online IP address of the machine

System Summary:

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

Binary contains a suspicious time stamp

Yara detected Beds Obfuscator

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 Beds Obfuscator

Stealing of Sensitive Information:

Yara detected Snake Keylogger

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:

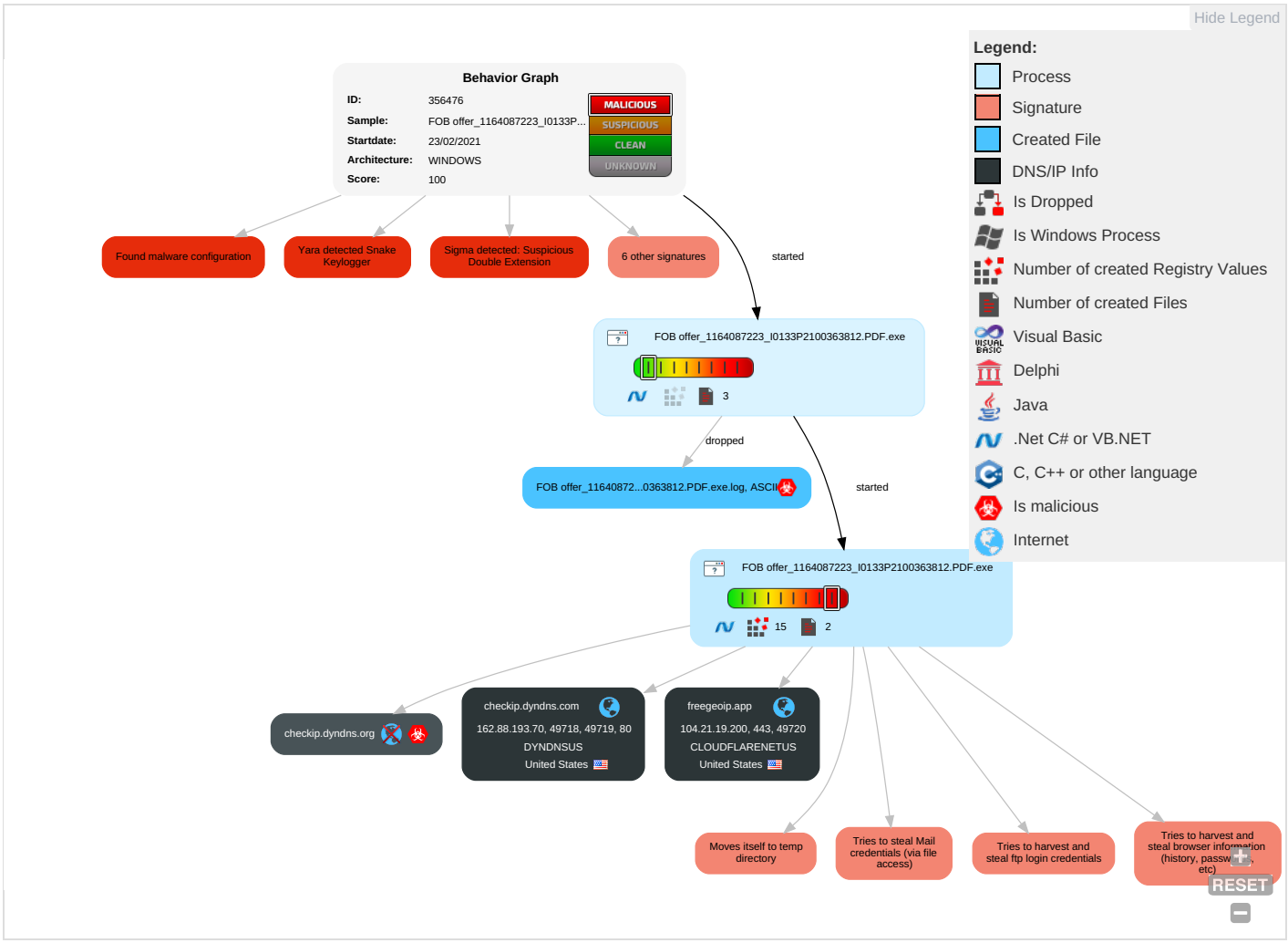
Yara detected Snake Keylogger

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 2	Masquerading 2 1	OS Credential Dumping 2	Security Software Discovery 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdro Insecure Network Commun
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2	LSASS Memory	Virtualization/Sandbox Evasion 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit S Redirect Calls/SM
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Local System 2	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit S Track De Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	System Network Configuration Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipula Device Commun
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1 1	Cached Domain Credentials	System Information Discovery 1 3	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 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue W Access P

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Timestomp 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgra Insecure Protocols

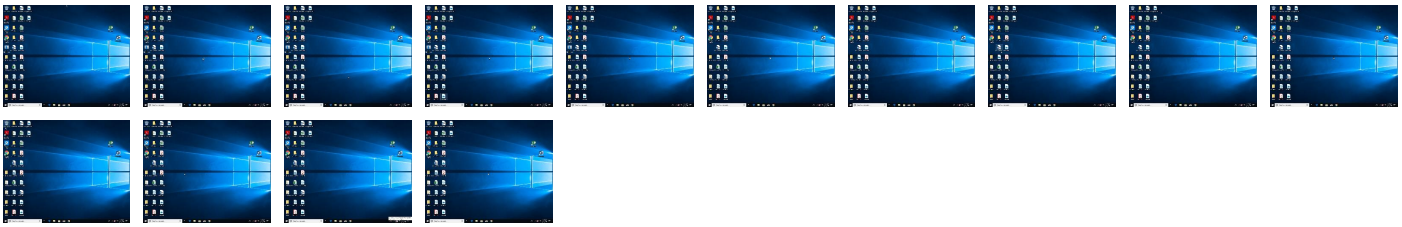
Behavior Graph



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
FOB offer_1164087223_I0133P2100363812.PDF.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.FOB offer_1164087223_I0133P2100363812.PDF.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen		Download File

Domains

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

URLs

Source	Detection	Scanner	Label	Link
http://checkip.dyndns.org/HB	0%	Avira URL Cloud	safe	
http://https://freegeoip.app	0%	URL Reputation	safe	
http://https://freegeoip.app	0%	URL Reputation	safe	
http://https://freegeoip.app	0%	URL Reputation	safe	
http://https://freegeoip.app/xml/	0%	URL Reputation	safe	
http://https://freegeoip.app/xml/	0%	URL Reputation	safe	
http://https://freegeoip.app/xml/	0%	URL Reputation	safe	
http://https://freegeoip.app/xml/84.17.52.38	0%	URL Reputation	safe	
http://https://freegeoip.app/xml/84.17.52.38	0%	URL Reputation	safe	
http://https://freegeoip.app/xml/84.17.52.38	0%	URL Reputation	safe	
http://checkip.dyndns.org	0%	Avira URL Cloud	safe	
http://checkip.dyndns.org/	0%	Avira URL Cloud	safe	
http://https://freegeoip.app/xml/LoadCountryNameClipboard	0%	URL Reputation	safe	
http://https://freegeoip.app/xml/LoadCountryNameClipboard	0%	URL Reputation	safe	
http://https://freegeoip.app/xml/LoadCountryNameClipboard	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
freegeoip.app	104.21.19.200	true	false	• 0%, Virustotal, Browse	unknown
checkip.dyndns.com	162.88.193.70	true	false	• 0%, Virustotal, Browse	unknown
checkip.dyndns.org	unknown	unknown	true	• 0%, Virustotal, Browse	unknown

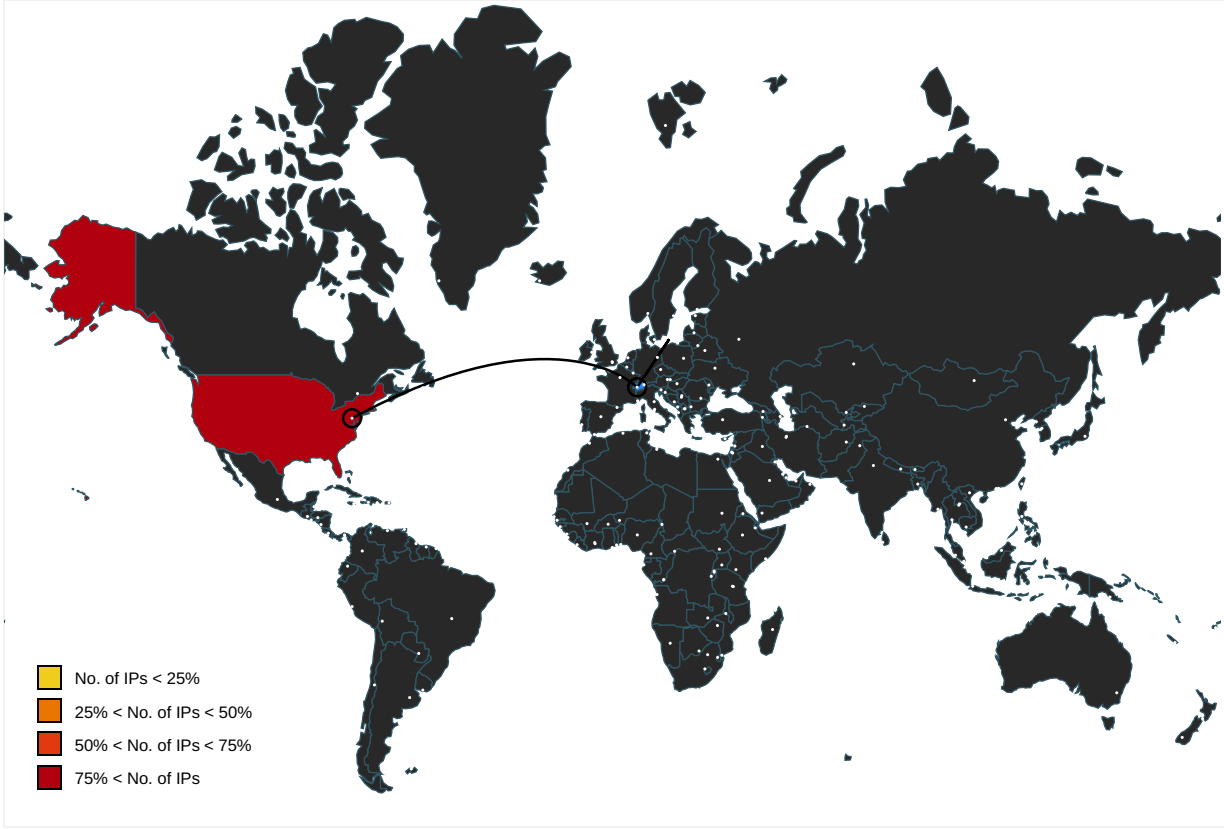
Contacted URLs

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

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://checkip.dyndns.org/HB	FOB offer_1164087223_I0133P210 0363812.PDF.exe, 00000001.0000 0002.499934986.0000000002D6100 0.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://freegeoip.app	FOB offer_1164087223_I0133P210 0363812.PDF.exe, 00000001.0000 0002.500063688.0000000002DAB00 0.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://freegeoip.app/xml/	FOB offer_1164087223_I0133P210 0363812.PDF.exe, 00000001.0000 0002.500063688.0000000002DAB00 0.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.telegram.org/bot/sendMessage?chat_id=&text=Createutf-8	FOB offer_1164087223_I0133P210 0363812.PDF.exe, 00000001.0000 0002.499934986.0000000002D6100 0.00000004.00000001.sdmp	false		high
http://https://freegeoip.app/xml/84.17.52.38	FOB offer_1164087223_I0133P210 0363812.PDF.exe, 00000001.0000 0002.500063688.0000000002DAB00 0.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://checkip.dyndns.org	FOB offer_1164087223_I0133P210 0363812.PDF.exe, 00000001.0000 0002.499934986.0000000002D6100 0.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://blog.naver.com/cubemit314Ghttp://projectofsonagi.tistory.com/	FOB offer_1164087223_I0133P210 0363812.PDF.exe, 00000000.0000 0002.235333402.00000000044A900 0.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	FOB offer_1164087223_I0133P210 0363812.PDF.exe, 00000001.0000 0002.499934986.0000000002D6100 0.00000004.00000001.sdmp	false		high
http://https://freegeoip.app/xml/LoadCountryNameClipboard	FOB offer_1164087223_I0133P210 0363812.PDF.exe, 00000001.0000 0002.499934986.0000000002D6100 0.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

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

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356476
Start date:	23.02.2021
Start time:	08:35:51
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	FOB offer_1164087223_I0133P2100363812.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:	21
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@3/1@3/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 3% (good quality ratio 1.7%) • Quality average: 29.9% • Quality standard deviation: 33.2%
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, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 131.253.33.200, 13.107.22.200, 104.43.139.144, 92.122.145.220, 52.147.198.201, 13.88.21.125, 52.255.188.83, 184.30.20.56, 51.104.144.132, 51.103.5.186, 92.122.213.194, 92.122.213.247, 20.54.26.129 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, www-bing-com.dual-a-0001.a-msedge.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, www.bing.com, client.wns.windows.com, fs.microsoft.com, db3p-ris-pf-prod-atm.trafficmanager.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, dual-a-0001.dc-msedge.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
162.88.193.70	purchase order 1.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	telex transfer.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	GPP.exe	Get hash	malicious	Browse	• checkip.dyndns.org/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	#11032019 de investigaci#U00f3n de #U00f3rdenes,pdf.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	Neue Bestellung_WJO-001, pdf.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	swift payment.doc	Get hash	malicious	Browse	• checkip.dyndns.org/
	Order.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	Order.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	PURCHASE ORDER.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	telex transfer.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	ORDEN DE COMPRA.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	banka bilgisi.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	purchase order.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	XXXXXXXXXXXXXX.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	170221.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	SecuriteInfo.com.Generic.mg.7ce1863c6187f2ad.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	SHIPPING DOCUMENTS.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	SONIVET SARL NOUVEL ORDER.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	Payment_copy.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	SHIPPING DOCUMENTS.exe	Get hash	malicious	Browse	• checkip.dyndns.org/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
freegeoip.app	PURCHASE ORDER CONFIRMATION.exe	Get hash	malicious	Browse	• 172.67.188.154
	Yao Han Industries 61007-51333893QR001U,pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	(appproved)WJO-TT180,pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	purchase order.exe	Get hash	malicious	Browse	• 172.67.188.154
	9073782912,pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	SOS URGENT RFQ #2345.exe	Get hash	malicious	Browse	• 104.21.19.200
	purchase order 1.exe	Get hash	malicious	Browse	• 172.67.188.154
	telex transfer.exe	Get hash	malicious	Browse	• 172.67.188.154
	GPP.exe	Get hash	malicious	Browse	• 172.67.188.154
	DHL Shipment Notification 6368638172.pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	#11032019 de investigaci#U00f3n de #U00f3rdenes,pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	Neue Bestellung_WJO-001, pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	Halkbank_Ekstre_20210222_082357_541079.exe	Get hash	malicious	Browse	• 104.21.19.200
	swift payment.doc	Get hash	malicious	Browse	• 104.21.19.200
	Order_C3350191107102300.exe	Get hash	malicious	Browse	• 172.67.188.154
	SecuriteInfo.com.Trojan.Inject4.6572.13919.exe	Get hash	malicious	Browse	• 104.21.19.200
	Order.exe	Get hash	malicious	Browse	• 104.21.19.200
	ORDER PURCHASE ITEMS.exe	Get hash	malicious	Browse	• 104.21.19.200
	Payment information 366531890544-2222021,pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	SwiftCopyTT.exe	Get hash	malicious	Browse	• 104.21.19.200
checkip.dyndns.com	PURCHASE ORDER CONFIRMATION.exe	Get hash	malicious	Browse	• 131.186.113.70
	Yao Han Industries 61007-51333893QR001U,pdf.exe	Get hash	malicious	Browse	• 131.186.113.70
	(appproved)WJO-TT180,pdf.exe	Get hash	malicious	Browse	• 131.186.161.70
	purchase order.exe	Get hash	malicious	Browse	• 131.186.113.70
	9073782912,pdf.exe	Get hash	malicious	Browse	• 131.186.113.70
	SOS URGENT RFQ #2345.exe	Get hash	malicious	Browse	• 131.186.113.70
	purchase order 1.exe	Get hash	malicious	Browse	• 162.88.193.70
	telex transfer.exe	Get hash	malicious	Browse	• 162.88.193.70
	iAxkn PDF.exe	Get hash	malicious	Browse	• 216.146.43.71
	GPP.exe	Get hash	malicious	Browse	• 162.88.193.70
	DHL Shipment Notification 6368638172.pdf.exe	Get hash	malicious	Browse	• 216.146.43.70

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	#11032019 de investigaci#U00f3n de #U00f3rdenes,pdf.exe	Get hash	malicious	Browse	• 162.88.193.70
	Neue Bestellung_WJO-001, pdf.exe	Get hash	malicious	Browse	• 162.88.193.70
	Halkbank_Ekstre_20210222_082357_541079.exe	Get hash	malicious	Browse	• 131.186.113.70
	swift payment.doc	Get hash	malicious	Browse	• 162.88.193.70
	Order_C3350191107102300.exe	Get hash	malicious	Browse	• 131.186.113.70
	SecuriteInfo.com.Trojan.Inject4.6572.13919.exe	Get hash	malicious	Browse	• 131.186.161.70
	Order.exe	Get hash	malicious	Browse	• 162.88.193.70
	ORDER PURCHASE ITEMS.exe	Get hash	malicious	Browse	• 216.146.43.70
	Payment information 366531890544-2222021,pdf.exe	Get hash	malicious	Browse	• 131.186.113.70

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	PURCHASE ORDER CONFIRMATION.exe	Get hash	malicious	Browse	• 172.67.188.154
	22 FEB -PROCESSING.xlsx	Get hash	malicious	Browse	• 172.67.160.246
	Yao Han Industries 61007-51333893QR001U,pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	PAYMENTADVICENOTE103_SWIFTCOPY0909208.exe	Get hash	malicious	Browse	• 172.67.172.17
	ORDER LIST.xlsx	Get hash	malicious	Browse	• 23.227.38.74
	(appproved)WJO-TT180,pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	purchase order.exe	Get hash	malicious	Browse	• 172.67.188.154
	9073782912,pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	SOS URGENT RFQ #2345.exe	Get hash	malicious	Browse	• 104.21.19.200
	INV_PR2201.docm	Get hash	malicious	Browse	• 162.159.134.233
	XP 6.xlsx	Get hash	malicious	Browse	• 172.67.172.17
	b0PmDaDeNh.dll	Get hash	malicious	Browse	• 104.20.184.68
	PO_210222.exe	Get hash	malicious	Browse	• 23.227.38.74
	Sw5kF7zkty.exe	Get hash	malicious	Browse	• 162.159.134.233
	PAYRECEIPT.exe	Get hash	malicious	Browse	• 172.67.172.17
	unmapped_executable_of_polyglot_duke.dll	Get hash	malicious	Browse	• 172.67.204.156
	6v3gJQytBL.exe	Get hash	malicious	Browse	• 104.18.87.101
	YqgA9W2m1D.exe	Get hash	malicious	Browse	• 104.18.87.101
	Document1094680387_02012021.xls	Get hash	malicious	Browse	• 104.21.29.200
	Document1094680387_02012021.xls	Get hash	malicious	Browse	• 172.67.149.197
DYNDNSUS	PURCHASE ORDER CONFIRMATION.exe	Get hash	malicious	Browse	• 131.186.113.70
	Yao Han Industries 61007-51333893QR001U,pdf.exe	Get hash	malicious	Browse	• 131.186.113.70
	(appproved)WJO-TT180,pdf.exe	Get hash	malicious	Browse	• 131.186.161.70
	purchase order.exe	Get hash	malicious	Browse	• 131.186.113.70
	9073782912,pdf.exe	Get hash	malicious	Browse	• 131.186.113.70
	SOS URGENT RFQ #2345.exe	Get hash	malicious	Browse	• 131.186.113.70
	purchase order 1.exe	Get hash	malicious	Browse	• 162.88.193.70
	telex transfer.exe	Get hash	malicious	Browse	• 162.88.193.70
	iAxkn PDF.exe	Get hash	malicious	Browse	• 216.146.43.71
	GPP.exe	Get hash	malicious	Browse	• 162.88.193.70
	DHL Shipment Notification 6368638172.pdf.exe	Get hash	malicious	Browse	• 216.146.43.70
	#11032019 de investigaci#U00f3n de #U00f3rdenes,pdf.exe	Get hash	malicious	Browse	• 162.88.193.70
	Neue Bestellung_WJO-001, pdf.exe	Get hash	malicious	Browse	• 162.88.193.70
	Halkbank_Ekstre_20210222_082357_541079.exe	Get hash	malicious	Browse	• 131.186.113.70
	swift payment.doc	Get hash	malicious	Browse	• 162.88.193.70
	Order_C3350191107102300.exe	Get hash	malicious	Browse	• 131.186.113.70
	SecuriteInfo.com.Trojan.Inject4.6572.13919.exe	Get hash	malicious	Browse	• 216.146.43.70
	Order.exe	Get hash	malicious	Browse	• 162.88.193.70
	ORDER PURCHASE ITEMS.exe	Get hash	malicious	Browse	• 216.146.43.70
	Payment information 366531890544-2222021,pdf.exe	Get hash	malicious	Browse	• 131.186.113.70

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
54328bd36c14bd82ddaa0c04b25ed9ad	PURCHASE ORDER CONFIRMATION.exe	Get hash	malicious	Browse	• 104.21.19.200
	Yao Han Industries 61007-51333893QR001U,pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	(appproved)WJO-TT180,pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	purchase order.exe	Get hash	malicious	Browse	• 104.21.19.200
	9073782912,pdf.exe	Get hash	malicious	Browse	• 104.21.19.200

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

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\FOB offer_1164087223_I0133P2100363812.PDF.exe.log

Process:	C:\Users\user\Desktop\FOB offer_1164087223_I0133P2100363812.PDF.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	706
Entropy (8bit):	5.342604339328228
Encrypted:	false
SSDEEP:	12:Q3La/hhkvoDLI4MWuCq1KDLI4M9tDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9I0ZKm:MLUE4Kx1qE4qpE4Ks2wKDE4KhK3VZ9px
MD5:	34580C7C598E15B8A008C82FE6A07CDF
SHA1:	2C90E9B7F4AFFE8FC7F9C313B4B867DF5B96CAC1
SHA-256:	08246B9BE1C37F8977CE083319A9D34BE09C65B926CBA30A5E062D79D5A4F1D6
SHA-512:	D836A862804608C3A127BF0CD30ECFB428E682D5E73D90C4C2837F93F02F12307F242F47F3CBBD71249AA6E608AFE230527F2F7D306A35A681346F9DDFE9D820
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..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",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..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..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.330838112428835
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	FOB offer_1164087223_I0133P2100363812.PDF.exe
File size:	3356672
MD5:	b10eafcd59bf5d8b5fcaea7175343da7
SHA1:	ba5b3ade8e66f73650eb50ec3ca78695e215e4e9

General

SHA256:	e2a36e86351414834625d38ab44ba38de9195a28ab9b4 45696c98f80fef9e09
SHA512:	a2f30966dcd4e5f0ba8bd6f8bde00b3b0b5904a24ecd60a 2e15c69bb73ddbc9b74c3a906400558958f41cc85bb695 6f029261551ed3806828e27fd0aace8b556
SSDEEP:	12288:TCbYQjoiuJ3JMCfSprEeGn/gFqJnNnZyTMFF6+BAZnret/:TCbYQjoBJ3JMBrvGn/gFqJnOTU6+Gtr
File Content Preview:	MZ......................@...!..L.!Th is program cannot be run in DOS mode....$.......PE..L...!(b...............0...3..........L3.. ...`3...@.. ....3...... .....@................................

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x734cde
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:	0xA4622821 [Thu May 24 02:17:05 2057 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

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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x334c8c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x336000	0x5d6	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x338000	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	0x332ce4	0x332e00	unknown	unknown	unknown	unknown	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x336000	0x5d6	0x600	False	0.417317708333	data	4.12380412335	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x338000	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	0x3360a0	0x34c	data		
RT_MANIFEST	0x3363ec	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

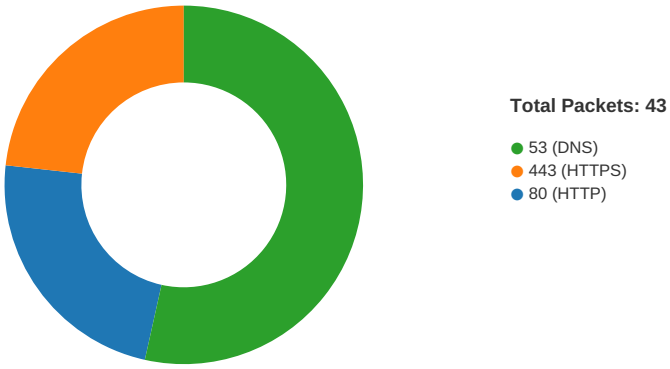
Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2020
Assembly Version	1.0.0.0
InternalName	ScreenCapturer.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	

Description	Data
ProductName	ScreenCapturer
ProductVersion	1.0.0.0
FileDescription	ScreenCapturer
OriginalFilename	ScreenCapturer.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 08:36:47.653973103 CET	49718	80	192.168.2.5	162.88.193.70
Feb 23, 2021 08:36:47.785650015 CET	80	49718	162.88.193.70	192.168.2.5
Feb 23, 2021 08:36:47.785963058 CET	49718	80	192.168.2.5	162.88.193.70
Feb 23, 2021 08:36:47.786459923 CET	49718	80	192.168.2.5	162.88.193.70
Feb 23, 2021 08:36:47.917717934 CET	80	49718	162.88.193.70	192.168.2.5
Feb 23, 2021 08:36:47.917745113 CET	80	49718	162.88.193.70	192.168.2.5
Feb 23, 2021 08:36:47.917757988 CET	80	49718	162.88.193.70	192.168.2.5
Feb 23, 2021 08:36:47.917845964 CET	49718	80	192.168.2.5	162.88.193.70
Feb 23, 2021 08:36:47.918896914 CET	49718	80	192.168.2.5	162.88.193.70
Feb 23, 2021 08:36:48.050234079 CET	80	49718	162.88.193.70	192.168.2.5
Feb 23, 2021 08:36:48.473274946 CET	49719	80	192.168.2.5	162.88.193.70
Feb 23, 2021 08:36:48.603620052 CET	80	49719	162.88.193.70	192.168.2.5
Feb 23, 2021 08:36:48.604887962 CET	49719	80	192.168.2.5	162.88.193.70
Feb 23, 2021 08:36:48.604917049 CET	49719	80	192.168.2.5	162.88.193.70
Feb 23, 2021 08:36:48.734757900 CET	80	49719	162.88.193.70	192.168.2.5
Feb 23, 2021 08:36:48.735183954 CET	80	49719	162.88.193.70	192.168.2.5
Feb 23, 2021 08:36:48.735203981 CET	80	49719	162.88.193.70	192.168.2.5
Feb 23, 2021 08:36:48.737428904 CET	49719	80	192.168.2.5	162.88.193.70
Feb 23, 2021 08:36:48.737974882 CET	49719	80	192.168.2.5	162.88.193.70
Feb 23, 2021 08:36:48.867687941 CET	80	49719	162.88.193.70	192.168.2.5
Feb 23, 2021 08:36:51.445343971 CET	49720	443	192.168.2.5	104.21.19.200
Feb 23, 2021 08:36:51.486318111 CET	443	49720	104.21.19.200	192.168.2.5
Feb 23, 2021 08:36:51.486443996 CET	49720	443	192.168.2.5	104.21.19.200
Feb 23, 2021 08:36:51.575974941 CET	49720	443	192.168.2.5	104.21.19.200
Feb 23, 2021 08:36:51.617038965 CET	443	49720	104.21.19.200	192.168.2.5
Feb 23, 2021 08:36:51.619297981 CET	443	49720	104.21.19.200	192.168.2.5
Feb 23, 2021 08:36:51.619322062 CET	443	49720	104.21.19.200	192.168.2.5
Feb 23, 2021 08:36:51.619399071 CET	49720	443	192.168.2.5	104.21.19.200
Feb 23, 2021 08:36:51.636622906 CET	49720	443	192.168.2.5	104.21.19.200
Feb 23, 2021 08:36:51.677665949 CET	443	49720	104.21.19.200	192.168.2.5
Feb 23, 2021 08:36:51.677731037 CET	443	49720	104.21.19.200	192.168.2.5
Feb 23, 2021 08:36:51.787316084 CET	49720	443	192.168.2.5	104.21.19.200

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 08:36:52.004380941 CET	49720	443	192.168.2.5	104.21.19.200
Feb 23, 2021 08:36:52.045336962 CET	443	49720	104.21.19.200	192.168.2.5
Feb 23, 2021 08:36:52.055479050 CET	443	49720	104.21.19.200	192.168.2.5
Feb 23, 2021 08:36:52.271676064 CET	49720	443	192.168.2.5	104.21.19.200
Feb 23, 2021 08:38:32.211450100 CET	49720	443	192.168.2.5	104.21.19.200
Feb 23, 2021 08:38:32.252652884 CET	443	49720	104.21.19.200	192.168.2.5
Feb 23, 2021 08:38:32.252806902 CET	49720	443	192.168.2.5	104.21.19.200

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 08:36:34.352915049 CET	61805	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:36:34.401505947 CET	53	61805	8.8.8.8	192.168.2.5
Feb 23, 2021 08:36:34.482239962 CET	54795	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:36:34.530970097 CET	53	54795	8.8.8.8	192.168.2.5
Feb 23, 2021 08:36:35.092433929 CET	49557	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:36:35.150553942 CET	53	49557	8.8.8.8	192.168.2.5
Feb 23, 2021 08:36:35.545433044 CET	61733	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:36:35.593908072 CET	53	61733	8.8.8.8	192.168.2.5
Feb 23, 2021 08:36:36.409924030 CET	65447	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:36:36.461545944 CET	53	65447	8.8.8.8	192.168.2.5
Feb 23, 2021 08:36:38.602375984 CET	52441	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:36:38.650939941 CET	53	52441	8.8.8.8	192.168.2.5
Feb 23, 2021 08:36:40.226308107 CET	62176	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:36:40.277834892 CET	53	62176	8.8.8.8	192.168.2.5
Feb 23, 2021 08:36:41.100189924 CET	59596	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:36:41.153681040 CET	53	59596	8.8.8.8	192.168.2.5
Feb 23, 2021 08:36:42.110230923 CET	65296	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:36:42.170021057 CET	53	65296	8.8.8.8	192.168.2.5
Feb 23, 2021 08:36:44.370172024 CET	63183	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:36:44.418952942 CET	53	63183	8.8.8.8	192.168.2.5
Feb 23, 2021 08:36:45.398272991 CET	60151	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:36:45.451570034 CET	53	60151	8.8.8.8	192.168.2.5
Feb 23, 2021 08:36:47.440604925 CET	56969	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:36:47.492157936 CET	53	56969	8.8.8.8	192.168.2.5
Feb 23, 2021 08:36:47.515018940 CET	55161	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:36:47.566571951 CET	53	55161	8.8.8.8	192.168.2.5
Feb 23, 2021 08:36:51.387927055 CET	54757	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:36:51.439770937 CET	53	54757	8.8.8.8	192.168.2.5
Feb 23, 2021 08:36:59.817301989 CET	49992	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:36:59.876332045 CET	53	49992	8.8.8.8	192.168.2.5
Feb 23, 2021 08:37:06.453500032 CET	60075	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:37:06.502176046 CET	53	60075	8.8.8.8	192.168.2.5
Feb 23, 2021 08:37:29.440562963 CET	55016	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:37:29.497395992 CET	53	55016	8.8.8.8	192.168.2.5
Feb 23, 2021 08:37:32.283868074 CET	64345	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:37:32.332545042 CET	53	64345	8.8.8.8	192.168.2.5
Feb 23, 2021 08:37:35.998430014 CET	57128	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:37:36.057640076 CET	53	57128	8.8.8.8	192.168.2.5
Feb 23, 2021 08:37:40.375140905 CET	54791	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:37:40.438473940 CET	53	54791	8.8.8.8	192.168.2.5
Feb 23, 2021 08:37:58.772171021 CET	50463	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:37:58.823683023 CET	53	50463	8.8.8.8	192.168.2.5
Feb 23, 2021 08:38:07.095153093 CET	50394	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:38:07.143791914 CET	53	50394	8.8.8.8	192.168.2.5
Feb 23, 2021 08:38:07.513964891 CET	58530	53	192.168.2.5	8.8.8.8
Feb 23, 2021 08:38:07.580950975 CET	53	58530	8.8.8.8	192.168.2.5

DNS Queries

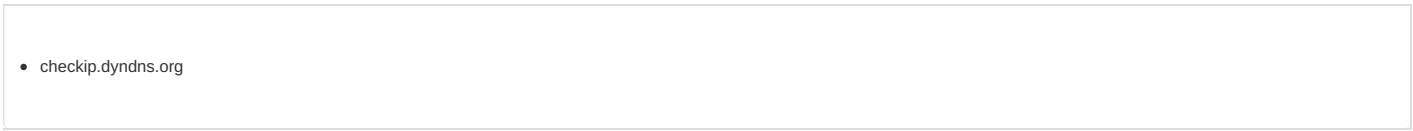
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 08:36:47.440604925 CET	192.168.2.5	8.8.8.8	0xf348	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 08:36:47.515018940 CET	192.168.2.5	8.8.8.8	0xbf6e	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)
Feb 23, 2021 08:36:51.387927055 CET	192.168.2.5	8.8.8.8	0x34d8	Standard query (0)	freegeoip.app	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 08:36:47.492157936 CET	8.8.8.8	192.168.2.5	0xf348	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 08:36:47.492157936 CET	8.8.8.8	192.168.2.5	0xf348	No error (0)	checkip.dyndns.com		162.88.193.70	A (IP address)	IN (0x0001)
Feb 23, 2021 08:36:47.492157936 CET	8.8.8.8	192.168.2.5	0xf348	No error (0)	checkip.dyndns.com		216.146.43.71	A (IP address)	IN (0x0001)
Feb 23, 2021 08:36:47.492157936 CET	8.8.8.8	192.168.2.5	0xf348	No error (0)	checkip.dyndns.com		131.186.161.70	A (IP address)	IN (0x0001)
Feb 23, 2021 08:36:47.492157936 CET	8.8.8.8	192.168.2.5	0xf348	No error (0)	checkip.dyndns.com		216.146.43.70	A (IP address)	IN (0x0001)
Feb 23, 2021 08:36:47.492157936 CET	8.8.8.8	192.168.2.5	0xf348	No error (0)	checkip.dyndns.com		131.186.113.70	A (IP address)	IN (0x0001)
Feb 23, 2021 08:36:47.566571951 CET	8.8.8.8	192.168.2.5	0xbf6e	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 08:36:47.566571951 CET	8.8.8.8	192.168.2.5	0xbf6e	No error (0)	checkip.dyndns.com		162.88.193.70	A (IP address)	IN (0x0001)
Feb 23, 2021 08:36:47.566571951 CET	8.8.8.8	192.168.2.5	0xbf6e	No error (0)	checkip.dyndns.com		216.146.43.70	A (IP address)	IN (0x0001)
Feb 23, 2021 08:36:47.566571951 CET	8.8.8.8	192.168.2.5	0xbf6e	No error (0)	checkip.dyndns.com		131.186.161.70	A (IP address)	IN (0x0001)
Feb 23, 2021 08:36:47.566571951 CET	8.8.8.8	192.168.2.5	0xbf6e	No error (0)	checkip.dyndns.com		131.186.113.70	A (IP address)	IN (0x0001)
Feb 23, 2021 08:36:47.566571951 CET	8.8.8.8	192.168.2.5	0xbf6e	No error (0)	checkip.dyndns.com		216.146.43.71	A (IP address)	IN (0x0001)
Feb 23, 2021 08:36:51.439770937 CET	8.8.8.8	192.168.2.5	0x34d8	No error (0)	freegeoip.app		104.21.19.200	A (IP address)	IN (0x0001)
Feb 23, 2021 08:36:51.439770937 CET	8.8.8.8	192.168.2.5	0x34d8	No error (0)	freegeoip.app		172.67.188.154	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph



HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49718	162.88.193.70	80	C:\Users\user\Desktop\FOB offer_1164087223_I0133P2100363812.PDF.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 08:36:47.786459923 CET	1215	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 08:36:47.917745113 CET	1216	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 103 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 38 34 2e 31 37 2e 35 32 2e 33 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 84.17.52.38</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49719	162.88.193.70	80	C:\Users\user\Desktop\FOB offer_1164087223_I0133P2100363812.PDF.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 08:36:48.604917049 CET	1216	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org
Feb 23, 2021 08:36:48.735183954 CET	1217	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 103 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 38 34 2e 31 37 2e 35 32 2e 33 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 84.17.52.38</body></html>

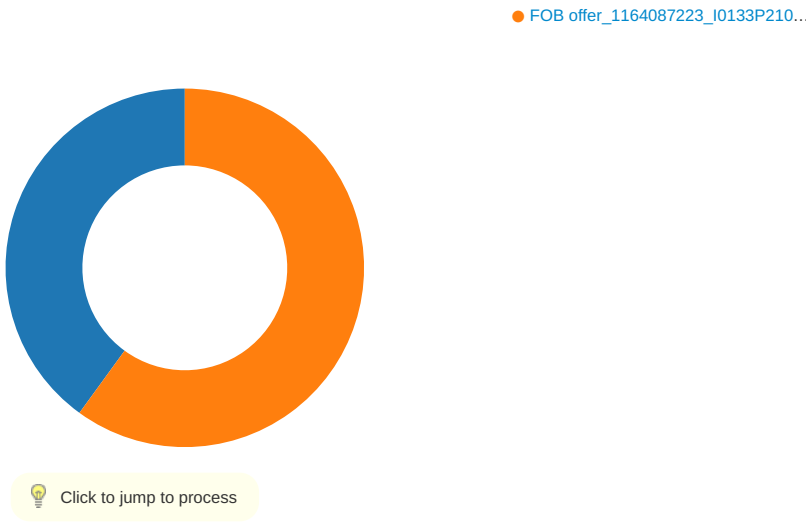
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 23, 2021 08:36:51.619322062 CET	104.21.19.200	443	192.168.2.5	49720	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Aug 10 02:00:00 CEST 2020	Tue Aug 10 14:00:00 CEST 2021	769,49162-49161-49172-49171-53-47-10,0-10-11-35-23-65281,29-23-24,0	54328bd36c14bd82ddaa0c04b25ed9ad
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: FOB offer_1164087223_I0133P2100363812.PDF.exe PID: 6436
Parent PID: 5752

General

Start time:	08:36:41
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\FOB offer_1164087223_I0133P2100363812.PDF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\FOB offer_1164087223_I0133P2100363812.PDF.exe'
Imagebase:	0xd10000
File size:	3356672 bytes
MD5 hash:	B10EAFCD59BF5D8B5FCAEA7175343DA7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_BedsObfuscator, Description: Yara detected Beds Obfuscator, Source: 00000000.00000002.240971373.0000000005439000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000000.00000002.240971373.0000000005439000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_BedsObfuscator, Description: Yara detected Beds Obfuscator, Source: 00000000.00000002.235333402.00000000044A9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_BedsObfuscator, Description: Yara detected Beds Obfuscator, Source: 00000000.00000002.243473367.00000000063B0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_BedsObfuscator, Description: Yara detected Beds Obfuscator, Source: 00000000.00000002.239618557.0000000004EA9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000000.00000002.239618557.0000000004EA9000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DA5CF06	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	6DA5CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\FOB offer_1164087223_I0133P2100363812.PDF.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DD6C78D	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\FOB offer_1164087223_I0133P2100363812.PDF.exe.log	unknown	706	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 32 2c 22 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 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 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System, Version=4.0.0.0, C	success or wait	1	6DD6C907	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	6DA35705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DA35705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA3CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA35705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DA35705	unknown

Analysis Process: FOB offer_1164087223_I0133P2100363812.PDF.exe PID: 6484
Parent PID: 6436

General

Start time:	08:36:43
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\FOB offer_1164087223_I0133P2100363812.PDF.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\FOB offer_1164087223_I0133P2100363812.PDF.exe
Imagebase:	0x700000
File size:	3356672 bytes
MD5 hash:	B10EAFCD59BF5D8B5FCAEA7175343DA7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_BedsObfuscator, Description: Yara detected Beds Obfuscator, Source: 00000001.00000002.495602752.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000001.00000002.495602752.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.500175759.0000000002DCA000.00000004.00000001.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	6DA5CF06	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	6DA5CF06	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies\container.dat	success or wait	1	6C8A6A95	DeleteFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies\deprecated.cookie	success or wait	1	6C8A6A95	DeleteFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	success or wait	1	6C8A6A95	DeleteFileW

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	6DA35705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DA35705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA3CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9903DE	ReadFile

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	6DA35705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DA35705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C8A1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C8A1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C8A1B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis