

JoeSandbox Cloud BASIC



ID: 553186

Sample Name:

20220114080343434.pdf.exe

Cookbook: default.jbs

Time: 12:59:46

Date: 14/01/2022

Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents	2
Windows Analysis Report 20220114080343434.pdf.exe	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Threatname: Telegram RAT	4
Threatname: Agenttesla	4
Yara Overview	4
Memory Dumps	4
Unpacked PEs	5
Sigma Overview	5
System Summary:	5
Jbx Signature Overview	5
AV Detection:	5
Networking:	5
System Summary:	5
Data Obfuscation:	5
Hooking and other Techniques for Hiding and Protection:	5
Malware Analysis System Evasion:	6
HIPS / PFW / Operating System Protection Evasion:	6
Stealing of Sensitive Information:	6
Remote Access Functionality:	6
Mitre Att&ck Matrix	6
Behavior Graph	7
Screenshots	7
Thumbnails	7
Antivirus, Machine Learning and Genetic Malware Detection	8
Initial Sample	8
Dropped Files	8
Unpacked PE Files	8
Domains	8
URLs	8
Domains and IPs	9
Contacted Domains	9
Contacted URLs	10
URLs from Memory and Binaries	10
Contacted IPs	10
Public	10
General Information	10
Simulations	10
Behavior and APIs	10
Joe Sandbox View / Context	11
IPs	11
Domains	11
ASN	11
JA3 Fingerprints	11
Dropped Files	11
Created / dropped Files	11
Static File Info	11
General	11
File Icon	12
Static PE Info	12
General	12
Entrypoint Preview	12
Data Directories	12
Sections	12
Resources	12
Imports	13
Version Infos	13
Network Behavior	13
Network Port Distribution	13
TCP Packets	13
UDP Packets	13
DNS Queries	13
DNS Answers	13
HTTP Request Dependency Graph	13
HTTPS Proxied Packets	13
Code Manipulations	14
Statistics	14
Behavior	14

System Behavior	14
Analysis Process: 20220114080343434.pdf.exe PID: 7036 Parent PID: 5456	14
General	14
File Activities	15
File Created	15
File Written	15
File Read	15
Analysis Process: RegSvc.exe PID: 6540 Parent PID: 7036	15
General	15
File Activities	15
File Created	15
File Read	16
Registry Activities	16
Disassembly	16
Code Analysis	16

Windows Analysis Report 20220114080343434.pdf.exe

Overview

General Information

Sample Name:

20220114080343434.pdf.exe

Analysis ID:

553186

MD5:

cd9290d22bb18c...

SHA1:

83b1ce896dca71...

SHA256:

3876b600bafaaaf..

Infos:

Most interesting Screenshot:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

AgentTesla

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

Signatures

Found malware configuration

Yara detected Telegram RAT

Yara detected AgentTesla

Yara detected AntiVM3

Tries to steal Mail credentials (via fil...

Sigma detected: Bad Opsec Default...

Initial sample is a PE file and has a ...

Writes to foreign memory regions

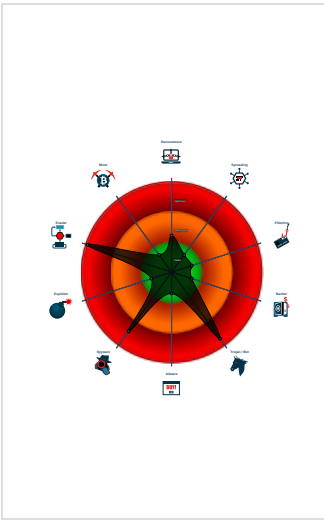
Tries to harvest and steal Putty / Wi...

Tries to harvest and steal ftp login c...

Tries to detect sandboxes and other...

Uses the Telegram API (likely for C&...

Classification



Process Tree

System is w10x64

20220114080343434.pdf.exe (PID: 7036 cmdline: "C:\Users\user\Desktop\20220114080343434.pdf.exe" MD5: CD9290D22BB18CED32A1B81814888382)

RegSvc.exe (PID: 6540 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvc.exe MD5: 2867A3817C9245F7CF518524DFD18F28)

cleanup

Malware Configuration

Threatname: Telegram RAT

```
{  
  "C2 url": "https://api.telegram.org/bot2122434962:AAFqLuKwJfwmfN8BZ9xq0IjLIiJbDmwbKs/sendMessage"  
}
```

Threatname: Agenttesla

```
{  
  "Exfil Mode": "Telegram",  
  "Chat id": "2124798776",  
  "Chat URL": "https://api.telegram.org/bot2122434962:AAFqLuKwJfwmfN8BZ9xq0IjLIiJbDmwbKs/sendDocument"  
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000002.558557812.0000000000344 E000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000009.00000000.304424534.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000009.00000000.304424534.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Copyright Joe Security LLC 2022

Page 4 of 16

Source	Rule	Description	Author	Strings
00000009.00000000.303933701.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000009.00000000.303933701.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 21 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.20220114080343434.pdf.exe.28df808.2.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
9.0.RegSvcs.exe.400000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
9.0.RegSvcs.exe.400000.1.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
9.0.RegSvcs.exe.400000.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
9.0.RegSvcs.exe.400000.4.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 17 entries				

Sigma Overview

System Summary:



Sigma detected: Bad Opsec Defaults Sacrificial Processes With Improper Arguments

Sigma detected: Possible Applocker Bypass

Jbx Signature Overview

 Click to jump to signature section

AV Detection:



Found malware configuration

Machine Learning detection for sample

Networking:



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

System Summary:



Initial sample is a PE file and has a suspicious name

.NET source code contains very large array initializations

Data Obfuscation:



.NET source code contains potential unpacker

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

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)

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

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

HIPS / PFW / Operating System Protection Evasion:



Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Stealing of Sensitive Information:



Yara detected Telegram RAT

Yara detected AgentTesla

Tries to steal Mail credentials (via file / registry access)

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

Tries to harvest and steal ftp login credentials

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

Remote Access Functionality:



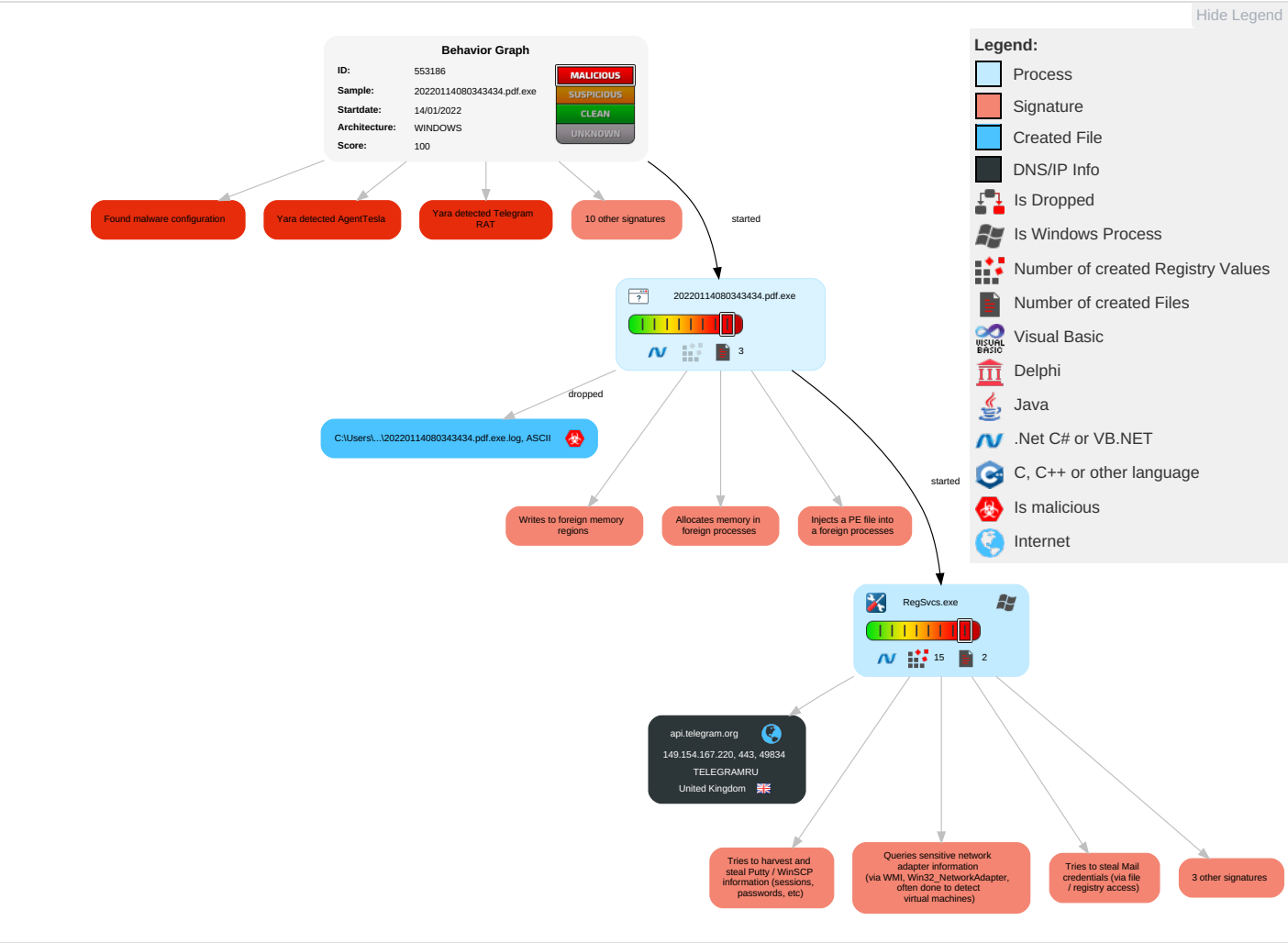
Yara detected Telegram RAT

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 3 1 2	Masquerading 1 1	OS Credential Dumping 2	Security Software Discovery 2 1 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Web Service 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	Credentials in Registry 1	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Encrypted Channel 1 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1 3 1	Security Account Manager	Virtualization/Sandbox Evasion 1 3 1	SMB/Windows Admin Shares	Data from Local System 2	Automated Exfiltration	Non-Application Layer Protocol 2
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 3 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 3
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1 2	Cached Domain Credentials	System Information Discovery 1 1 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 2 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port

Behavior Graph





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
20220114080343434.pdf.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
9.0.RegSvc.exe.400000.3.unpack	100%	Avira	TR/Spy.Gen8		Download File
9.0.RegSvc.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
9.0.RegSvc.exe.400000.2.unpack	100%	Avira	TR/Spy.Gen8		Download File
9.0.RegSvc.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File
9.0.RegSvc.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
9.2.RegSvc.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://en.wE	0%	Avira URL Cloud	safe	
http://www.fontbureau.comd1	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com2	0%	URL Reputation	safe	
http://www.sajatypeworks.comeu	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.fontbureau.comalict	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.fontbureau.comessed	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://UeFrqT.com	0%	Avira URL Cloud	safe	
http://www.fontbureau.comt:	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	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.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fontbureau.comgrita	0%	URL Reputation	safe	
http://www.founder.com.cn/cnl-g	0%	URL Reputation	safe	
http://https://api.telegram.org4	0%	URL Reputation	safe	
http://www.founder.com.cn/cnu	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.fontbureau.comtto	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/ft	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fontbureau.comtoTF	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://www.sakkal.comrmx	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://https://mVBubsTSBV2T9Joj.org	0%	Avira URL Cloud	safe	
http://https://mVBubsTSBV2T9Joj.org(	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%ha	0%	URL Reputation	safe	
http://www.founder.com.cn/cnres	0%	Avira URL Cloud	safe	
http://www.fontbureau.comdf	0%	Avira URL Cloud	safe	
http://www.sakkal.com-iX	0%	Avira URL Cloud	safe	
http://en.wikipedia	0%	URL Reputation	safe	
http://www.fontbureau.comtuet:	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.founder.com.cn/cncr;	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%\$	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/#	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/o	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.founder.com.cn/cnu-h	0%	Avira URL Cloud	safe	
http://www.fontbureau.comrsivo	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/oby	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

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

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http:// https://api.telegram.org/bot2122434962:AAFqluKwJfwmfN8BZ9xq0jlilijJbDmwbKs/sendDocument	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
149.154.167.220	api.telegram.org	United Kingdom		62041	TELEGRAMRU	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553186
Start date:	14.01.2022
Start time:	12:59:46
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	20220114080343434.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:	24
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@1/1
EGA Information:	Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	- Successful, ratio: 100% - Number of executed functions: 0 - Number of non-executed functions: 0
Cookbook Comments:	- Adjust boot time - Enable AMSI - Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
13:00:47	API Interceptor	1x Sleep call for process: 20220114080343434.pdf.exe modified
13:01:00	API Interceptor	731x Sleep call for process: RegSvc.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\20220114080343434.pdf.exe.log		
Process:	C:\Users\user\Desktop\20220114080343434.pdf.exe	
File Type:	ASCII text, with CRLF line terminators	
Category:	dropped	
Size (bytes):	1310	
Entropy (8bit):	5.345651901398759	
Encrypted:	false	
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x847mE4P:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzQ	
MD5:	A9EFF9253CAF99EC8665E41D736DDAED	
SHA1:	D95BB4ABC856D774DA4602A59DE252B4BF560530	
SHA-256:	DBC637B33F1F3CD1AB40AFED23F94C4571CA43621EBB52C5DC267DBDC52D4783	
SHA-512:	96B67A84B750589BDB758224641065919F34BBF02BB286B9F5D566B48965A0E38FB88308B61351A6E11C46B76BFEC370FBC8B978A9F0F07A847567172D5CA5F3	
Malicious:	true	
Reputation:	moderate, very likely benign file	
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21	

Static File Info

General		
File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows	
Entropy (8bit):	7.224593030373487	

General

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:	20220114080343434.pdf.exe
File size:	589824
MD5:	cd9290d22bb18ced32a1b81814888382
SHA1:	83b1ce896dca71d611232fe4197cbe3993cccf64
SHA256:	3876b600bafaaaf0a580e3925b9851c1c82ea16b40fb6b2b127296a523cf86fd
SHA512:	1c2c1b126910aad08d6434ed65c49d10e24c3fa79463ec7829ebc6dc4f3601020edaa0d07e7a60c12faec39c557ae4ecafe5804ac324231ff8cf3f4d8d8e7b23
SSDEEP:	12288:Scck777777777777N7cPGR72wUjuf/R9nkIE9NciKpSj1kv6e:CK777777777777lcudvUjuX7S+8kv
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....\$......PE..L...5 O.a.....>.....@.....`..... ..@.....

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General	
Entrypoint:	0x49143e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61E14F35 [Fri Jan 14 10:23:49 2022 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

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x8f444	0x8f600	False	0.755026700087	data	7.23442041847	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x92000	0x5e4	0x600	False	0.439453125	data	4.1825921697	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x94000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 13:02:29.542478085 CET	192.168.2.3	8.8.8.8	0xb165	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 13:02:29.561613083 CET	8.8.8.8	192.168.2.3	0xb165	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49834	149.154.167.220	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe

[illegible]

Timestamp	kBytes transferred	Direction	Data
2022-01-14 12:02:31 UTC	1	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 Date: Fri, 14 Jan 2022 12:02:31 GMT Content-Type: application/json Content-Length: 632 Connection: close Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET, POST, OPTIONS Access-Control-Expose-Headers: Content-Length,Content-Type,Date,Server,Connection {\"ok\":true,\"result\":{\"message_id\":\"963,\"from\":{\"id\":\"2122434962,\"is_bot\":true,\"first_name\":\"w4kejohn\",\"username\":\"w4kejohnbot\"},\"chat\":{\"id\":\"2124798776,\"first_name\":\"John\",\"last_name\":\"Cena\",\"username\":\"joebest123\",\"type\":\"private\"},\"date\":\"1642161751,\"document\":{\"file_name\":\"user-179605 2022-01-14 04-02-33.html\",\"mime_type\":\"text/html\",\"file_id\":\"BQACAgQAAxkDAIDw2HhZleXb1Ykqx_02hQAAfmaqmgzrwACTAoAAn7QEFM2orzgquUldCME\",\"file_unique_id\":\"AgADTAoAAAn7QEFM\",\"file_size\":436},\"caption\":\"New PW Recovered!\n\nUser Name: user/179605\n\nOSFullName: Microsoft Windows 10 Pro\n\nCPU: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz\n\nRAM: 8191.25 MB\"}}

Code Manipulations

Statistics

Behavior

 Click to jump to process

System Behavior

Analysis Process: 20220114080343434.pdf.exe PID: 7036 Parent PID: 5456

General

Start time:	13:00:39
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\20220114080343434.pdf.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\20220114080343434.pdf.exe"
Imagebase:	0x380000
File size:	589824 bytes
MD5 hash:	CD9290D22BB18CED32A1B81814888382
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: 00000001.00000002.306440139.00000000029B7000.00000004.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.306278830.00000000028B1000.00000004.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.306687989.00000000038B9000.00000004.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.306687989.00000000038B9000.00000004.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.306874211.0000000003A0F000.00000004.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.306874211.0000000003A0F000.00000004.00000001.sdmp, Author: Joe Security

Reputation:	low
-------------	-----

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: RegSvc.exe PID: 6540 Parent PID: 7036

General

Start time:	13:00:48
Start date:	14/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvc.exe
Imagebase:	0xe10000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	- Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000002.558557812.000000000344E000.00000004.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000000.304424534.000000000402000.00000040.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000009.00000000.304424534.000000000402000.00000040.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000000.303933701.000000000402000.00000040.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000009.00000000.303933701.000000000402000.00000040.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000000.303119673.000000000402000.00000040.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000009.00000000.303119673.000000000402000.00000040.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000000.303547707.000000000402000.00000040.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000009.00000000.303547707.000000000402000.00000040.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000002.548274653.000000000402000.00000040.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000009.00000002.548274653.000000000402000.00000040.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000002.558108982.0000000003141000.00000004.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000009.00000002.558108982.0000000003141000.00000004.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000009.00000002.558108982.0000000003141000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

Disassembly

Code Analysis