ID: 479213
Sample Name: RFQ-Order_Sheet#43254363-Sept-21_signed-copy.exe
Cookbook: default.jbs
Time: 18:15:44
Date: 07/09/2021
Version: 33.0.0 White Diamond

Table of Contents

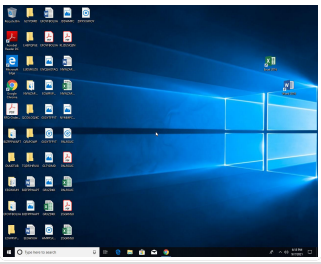
Windows Analysis Report RFQ-Order_Sheet#43254363-…

Overview

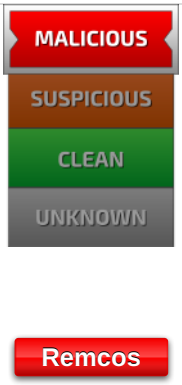
General Information

Sample Name:	RFQ-Order_Sheet#43254363-Sept-21_signed-copy.exe
Analysis ID:	479213
MD5:	06534c059b1117..
SHA1:	7ebda7124a60de..
SHA256:	933a4d2abfdf0f9…
Infos:	

Most interesting Screenshot:



Detection

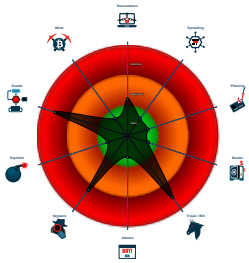


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Malicious sample detected (through …
- Yara detected Remcos RAT
- Detected Remcos RAT
- Initial sample is a PE file and has a …
- Writes to foreign memory regions
- Contains functionality to steal Firefo…
- Delayed program exit found
- Allocates memory in foreign process…
- Injects a PE file into a foreign proce…
- Contains functionality to steal Chrom…
- Contains functionality to inject code …
- C2 URLs / IPs found in malware con…

Classification



Process Tree

- **System is w10x64**
- RFQ-Order_Sheet#43254363-Sept-21_signed-copy.exe (PID: 5256 cmdline: 'C:\Users\user\Desktop\RFQ-Order_Sheet#43254363-Sept-21_signed-copy.exe' MD5: 06534C059B111776B838F793C6444622)
  - mobsync.exe (PID: 4692 cmdline: C:\Windows\System32\mobsync.exe MD5: 44C19378FA529DD88674BAF647EBDC3C)
- Cshgvzx.exe (PID: 5384 cmdline: 'C:\Users\Public\Libraries\Cshgvzx\Cshgvzx.exe' MD5: 06534C059B111776B838F793C6444622)
  - dialer.exe (PID: 6544 cmdline: C:\Windows\System32\dialer.exe MD5: F176211F7372248224D02AC023573870)
- Cshgvzx.exe (PID: 5296 cmdline: 'C:\Users\Public\Libraries\Cshgvzx\Cshgvzx.exe' MD5: 06534C059B111776B838F793C6444622)
  - secinit.exe (PID: 6672 cmdline: C:\Windows\System32\secinit.exe MD5: 174A363BB5A2D88B224546C15DD10906)
- **cleanup**

Malware Configuration

Threatname: Remcos

```
{
  "Host:Port:Password": "204.44.86.179:49151:0123qwegus.duckdns.org:49151:0",
  "Assigned name": "septttt",
  "Connect interval": "1",
  "Install flag": "Disable",
  "Setup HKCU\\Run": "Enable",
  "Setup HKLM\\Run": "Disable",
  "Install path": "AppData",
  "Copy file": "remcos.exe",
  "Startup value": "Remcos",
  "Hide file": "Disable",
  "Mutex": "Remcos-ZXIQGD",
  "Keylog flag": "0",
  "Keylog path": "AppData",
  "Keylog file": "logs.dat",
  "Keylog crypt": "Disable",
  "Hide keylog file": "Disable",
  "Screenshot flag": "Disable",
  "Screenshot time": "10",
  "Take Screenshot option": "Disable",
  "Take screenshot title": "notepad;solitaire;",
  "Take screenshot time": "5",
  "Screenshot path": "AppData",
  "Screenshot file": "Screenshots",
  "Screenshot crypt": "Disable",
  "Mouse option": "Disable",
  "Delete file": "Disable",
  "Audio record time": "5",
  "Audio path": "AppData",
  "Audio folder": "MicRecords",
  "Connect delay": "",
  "Copy folder": "Remcos",
  "Keylog folder": "remcos",
  "Keylog file max size": "20000"
}
```


Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\Public\Libraries\xzvghsC.url	Methodology_Contains_Shortcut_OtherURIhandlers	Detects possible shortcut usage for .URL persistence	@itsreallynick (Nick Carr)	• 0x14:$file: URL= • 0x0:$url_explicit: [InternetShortcut]

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000002.492585881.00000000030E7000.00000004.00000020.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
00000012.00000002.331608026.0000000002F98000.00000004.00000020.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
00000013.00000002.356743910.0000000000500000.00000040.00000001.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000013.00000002.356743910.000000000050 0000.00000040.00000001.sdmp	REMCOS_RAT_variants	unknown	unknown	• 0x606bc:$str_a1: C:\Windows\System32\cmd.exe • 0x60638:$str_a3: /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\ Policies\System /v EnableLUA /t REG_DWOR • 0x60638:$str_a4: /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\ Policies\System /v EnableLUA /t REG_DWOR • 0x5fc38:$str_a5: \AppData\Local\Google\Chrome\User Data\Default\Login Data • 0x60290:$str_b1: CreateObject("Scripting.FileSystemO bject").DeleteFile(Wscript.ScriptFullName) • 0x5f86c:$str_b2: Executing file: • 0x60800:$str_b3: GetDirectListeningPort • 0x60050:$str_b4: Set fso = CreateObject("Scripting.File SystemObject") • 0x603d4:$str_b5: licence_code.txt • 0x60278:$str_b7: \update.vbs • 0x5f8dc:$str_b9: Downloaded file: • 0x5f8a8:$str_b10: Downloading file: • 0x5f890:$str_b12: Failed to upload file: • 0x607c8:$str_b13: StartForward • 0x607e8:$str_b14: StopForward • 0x60220:$str_b15: fso.DeleteFile " • 0x601b4:$str_b16: On Error Resume Next • 0x60250:$str_b17: fso.DeleteFolder " • 0x5f880:$str_b18: Uploaded file: • 0x5f91c:$str_b19: Unable to delete: • 0x601e8:$str_b20: while fso.FileExists("
00000013.00000002.356991304.000000001059 0000.00000040.00000001.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
Click to see the 13 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
8.2.mobsync.exe.10590000.2.raw.unpack	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
8.2.mobsync.exe.10590000.2.raw.unpack	REMCOS_RAT_variants	unknown	unknown	• 0x60553:$str_a1: C:\Windows\System32\cmd.exe • 0x604cf:$str_a3: /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\ Policies\System /v EnableLUA /t REG_DWOR • 0x604cf:$str_a4: /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\ Policies\System /v EnableLUA /t REG_DWOR • 0x5facf:$str_a5: \AppData\Local\Google\Chrome\User Data\Default\Login Data • 0x60127:$str_b1: CreateObject("Scripting.FileSystemO bject").DeleteFile(Wscript.ScriptFullName) • 0x5f703:$str_b2: Executing file: • 0x60697:$str_b3: GetDirectListeningPort • 0x5fee7:$str_b4: Set fso = CreateObject("Scripting.File SystemObject") • 0x6026b:$str_b5: licence_code.txt • 0x6010f:$str_b7: \update.vbs • 0x5f773:$str_b9: Downloaded file: • 0x5f73f:$str_b10: Downloading file: • 0x5f727:$str_b12: Failed to upload file: • 0x6065f:$str_b13: StartForward • 0x6067f:$str_b14: StopForward • 0x600b7:$str_b15: fso.DeleteFile " • 0x6004b:$str_b16: On Error Resume Next • 0x600e7:$str_b17: fso.DeleteFolder " • 0x5f717:$str_b18: Uploaded file: • 0x5f7b3:$str_b19: Unable to delete: • 0x6007f:$str_b20: while fso.FileExists("
18.2.dialer.exe.10590000.2.unpack	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	

Source	Rule	Description	Author	Strings
18.2.dialer.exe.10590000.2.unpack	REMCOS_RAT_variants	unknown	unknown	• 0x5f953:$str_a1: C:\Windows\System32\cmd.exe • 0x5f8cf:$str_a3: /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWOR • 0x5f8cf:$str_a4: /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWOR • 0x5eecf:$str_a5: \AppData\Local\Google\Chrome\User Data\Default\Login Data • 0x5f527:$str_b1: CreateObject("Scripting.FileSystemObject").DeleteFile(Wscript.ScriptFullName) • 0x5eb03:$str_b2: Executing file: • 0x5fa97:$str_b3: GetDirectListeningPort • 0x5f2e7:$str_b4: Set fso = CreateObject("Scripting.FileSystemObject") • 0x5f66b:$str_b5: licence_code.txt • 0x5f50f:$str_b7: \update.vbs • 0x5eb73:$str_b9: Downloaded file: • 0x5eb3f:$str_b10: Downloading file: • 0x5eb27:$str_b12: Failed to upload file: • 0x5fa5f:$str_b13: StartForward • 0x5fa7f:$str_b14: StopForward • 0x5f4b7:$str_b15: fso.DeleteFile " • 0x5f44b:$str_b16: On Error Resume Next • 0x5f4e7:$str_b17: fso.DeleteFolder " • 0x5eb17:$str_b18: Uploaded file: • 0x5ebb3:$str_b19: Unable to delete: • 0x5f47f:$str_b20: while fso.FileExists("
8.2.mobsync.exe.10590000.2.unpack	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
Click to see the 31 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Yara detected Remcos RAT

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Remcos RAT

System Summary:

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Malware Analysis System Evasion:

Delayed program exit found

HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Contains functionality to inject code into remote processes

Creates a thread in another existing process (thread injection)

Stealing of Sensitive Information:

Yara detected Remcos RAT

Contains functionality to steal Firefox passwords or cookies

Contains functionality to steal Chrome passwords or cookies

Remote Access Functionality:

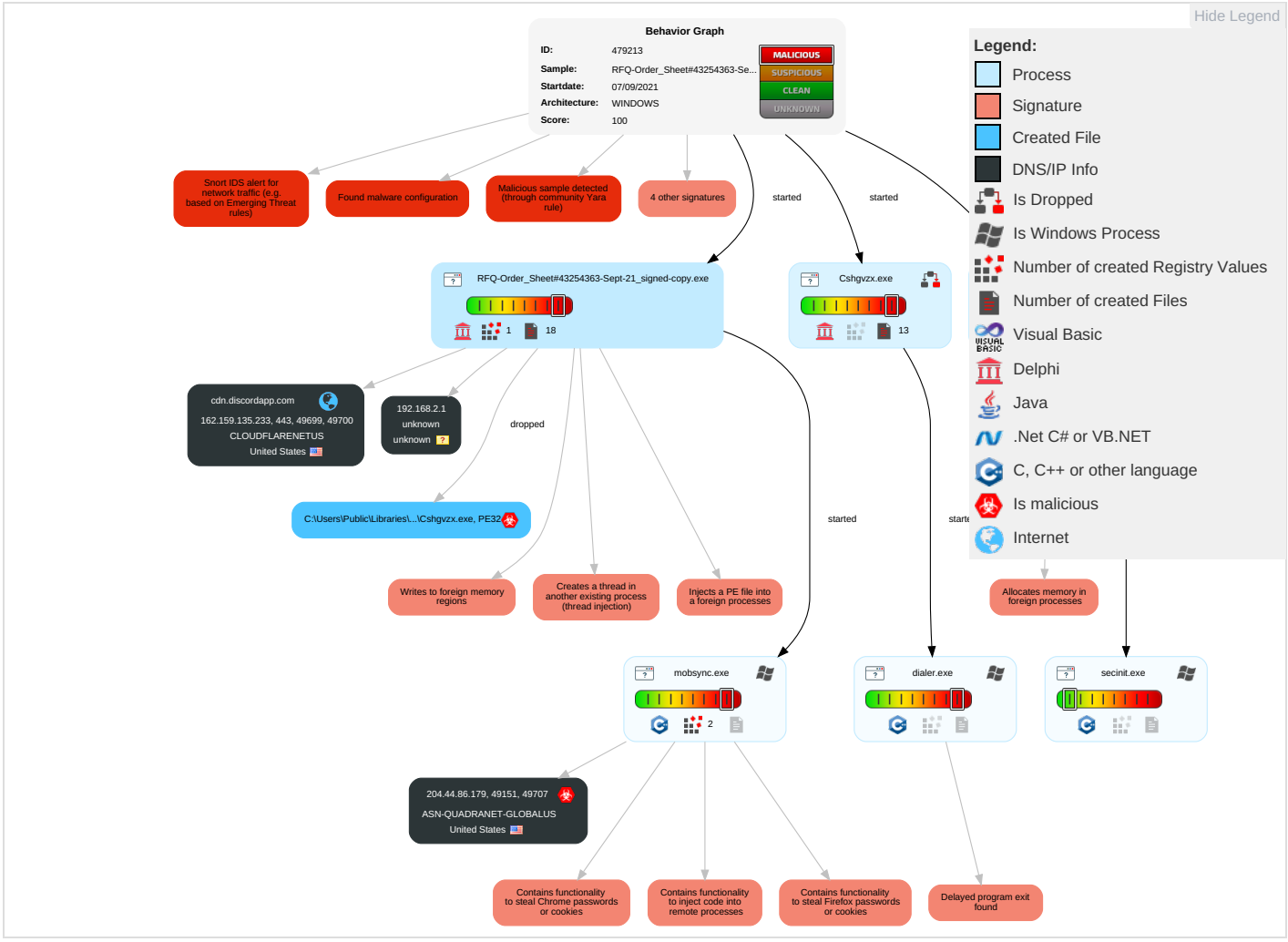
Yara detected Remcos RAT

Detected Remcos RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Co
Valid Accounts	Native API 1	Application Shimming 1	Application Shimming 1	Deobfuscate/Decode Files or Information 1	OS Credential Dumping 1	System Time Discovery 2	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Transfe
Default Accounts	Command and Scripting Interpreter 1	Windows Service 1	Access Token Manipulation 1	Obfuscated Files or Information 2	Input Capture 1 1	Account Discovery 1	Remote Desktop Protocol	Input Capture 1 1	Exfiltration Over Bluetooth	Encrypte Channe
Domain Accounts	Service Execution 2	Registry Run Keys / Startup Folder 1	Windows Service 1	Software Packing 1	Credentials In Files 2	System Service Discovery 1	SMB/Windows Admin Shares	Clipboard Data 2	Automated Exfiltration	Non-Sta Port 1
Local Accounts	At (Windows)	Logon Script (Mac)	Process Injection 5 2 1	Masquerading 1	NTDS	File and Directory Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Remote Access Softwar
Cloud Accounts	Cron	Network Logon Script	Registry Run Keys / Startup Folder 1	Virtualization/Sandbox Evasion 1	LSA Secrets	System Information Discovery 2 3	SSH	Keylogging	Data Transfer Size Limits	Non-Applicat Layer Protocol
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Access Token Manipulation 1	Cached Domain Credentials	Security Software Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Applicat Layer Protocol
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 5 2 1	DCSync	Virtualization/Sandbox Evasion 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commo Used Po
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Process Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applicat Layer Pr
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	Remote System Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tra Protocol

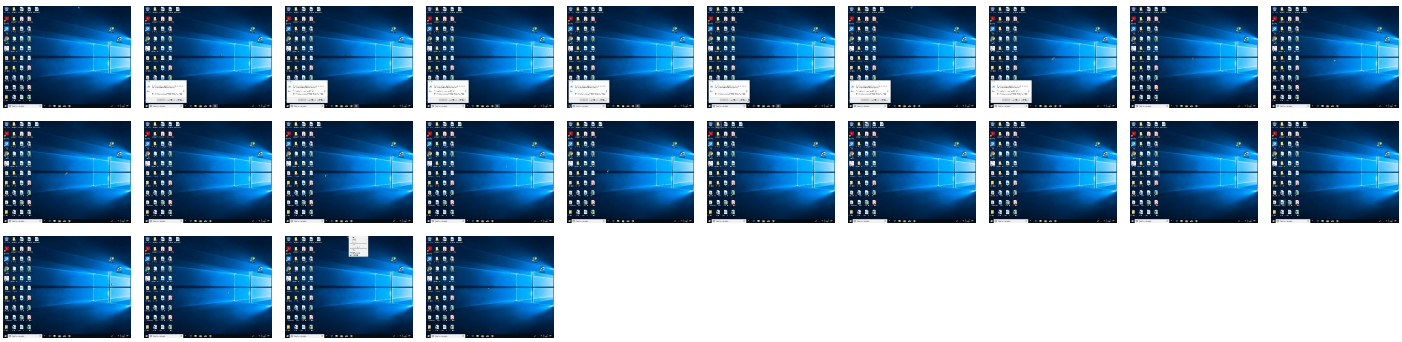
Behavior Graph



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
19.2.secinit.exe.500000.0.unpack	100%	Avira	HEUR/AGEN.1141389		Download File
8.0.mobsync.exe.10590000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
18.2.dialer.exe.10590000.2.unpack	100%	Avira	TR/Dropper.Gen		Download File
8.0.mobsync.exe.10590000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
8.2.mobsync.exe.10590000.2.unpack	100%	Avira	TR/Dropper.Gen		Download File
18.0.dialer.exe.10590000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
8.2.mobsync.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1141389		Download File
19.0.secinit.exe.10590000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
19.0.secinit.exe.10590000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
19.0.secinit.exe.10590000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
18.0.dialer.exe.10590000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
8.0.mobsync.exe.10590000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
18.0.dialer.exe.10590000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
8.0.mobsync.exe.10590000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
18.0.dialer.exe.10590000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
18.2.dialer.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1141389		Download File
19.2.secinit.exe.10590000.1.unpack	100%	Avira	TR/Dropper.Gen		Download File
19.0.secinit.exe.10590000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
204.44.86.179	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cdn.discordapp.com	162.159.135.233	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
204.44.86.179	true	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
204.44.86.179	unknown	United States		8100	ASN-QUADRANET-GLOBALUS	true
162.159.135.233	cdn.discordapp.com	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	479213
Start date:	07.09.2021
Start time:	18:15:44
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 12s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	RFQ-Order_Sheet#43254363-Sept-21_signed-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:	28
Number of new started drivers analysed:	0

Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@9/5@3/3
EGA Information:	• Successful, ratio: 40%
HDC Information:	• Successful, ratio: 80.4% (good quality ratio 76.6%) • Quality average: 82.3% • Quality standard deviation: 26.3%
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

Simulations

Behavior and APIs

Time	Type	Description
18:16:40	API Interceptor	1x Sleep call for process: RFQ-Order_Sheet#43254363-Sept-21_signed-copy.exe modified
18:16:44	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Cshgvzx C:\Users\Public\Libraries\xzvghsC.url
18:16:52	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Cshgvzx C:\Users\Public\Libraries\xzvghsC.url
18:17:00	API Interceptor	2x Sleep call for process: Cshgvzx.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
204.44.86.179	Invoice-packing list BL NO. 212142500 MRKU7550471 ML-IN4104393.tar	Get hash	malicious	Browse	
	New_Order_for_September#442625272-doc-signed copy.exe	Get hash	malicious	Browse	
	New_Order_for_September#442625272-doc-signed copy.exe	Get hash	malicious	Browse	
162.159.135.233	mosoxxxHack.exe	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/710557342755848243/876828681815871488/clp.exe
	Sales-contract-deaho-180521-poweruae.doc	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/843685789120331799/844316591284944986/poiu.exe

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PURCHASE ORDER E3007921.EXE	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/809311531652087809/839820005927550996/Youngest_Snake.exe
	Waybill Document 22700456.exe	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/809311531652087809/839856358152208434/May_Blessing.exe
	COMPANY REQUIREMENT.doc	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/819674896988242004/819677189900861500/harcout.exe
	Email data form.doc	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/789279517516365865/789279697203757066/angelx.scr
	Down Payment.doc	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/788946375533789214/788947376849027092/atlasx.scr
	Vessel details.doc	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/780175015496777751/781048233136226304/mocux.exe
	Teklif Rusya 24 09 2020.doc	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/733818080668680222/758418625429372978/p2.jpg

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cdn.discordapp.com	2101222_OrdineFornitore del.ppam	Get hash	malicious	Browse	• 162.159.133.233
	ORDER 33212762.ppam	Get hash	malicious	Browse	• 162.159.135.233
	38fd2cb3083f33b50606b7821453769103bde24335734.exe	Get hash	malicious	Browse	• 162.159.133.233
	JSYInjvdnM.exe	Get hash	malicious	Browse	• 162.159.129.233
	SecuriteInfo.com.W32.AIDetect.malware2.7985.exe	Get hash	malicious	Browse	• 162.159.134.233
	WAYBILL.EXE	Get hash	malicious	Browse	• 162.159.133.233
	Eklenen yeni siparis.exe	Get hash	malicious	Browse	• 162.159.135.233
	KlErfuBsH2.exe	Get hash	malicious	Browse	• 162.159.135.233
	H32ChHNoNW.exe	Get hash	malicious	Browse	• 162.159.133.233

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Wdq9HRCTrG.exe	Get hash	malicious	Browse	• 162.159.134.233
	bk0Yz4tRBL.exe	Get hash	malicious	Browse	• 162.159.133.233
	Ouiojcejoyugnzyrllxqhjgpjgtmcpzvnp.exe	Get hash	malicious	Browse	• 162.159.133.233
	hhnkZPwzxi.exe	Get hash	malicious	Browse	• 162.159.133.233
	X117Xdqctj.exe	Get hash	malicious	Browse	• 162.159.135.233
	ffe39579163c2315210984353480192 27cca339b735ef.exe	Get hash	malicious	Browse	• 162.159.135.233
	Ko6lDa3LMx.exe	Get hash	malicious	Browse	• 162.159.135.233
	Invoice-packing list BL NO. 212142500 MRKU7550471 ML-IN4104393.tar	Get hash	malicious	Browse	• 162.159.129.233
	UwQkw83lMK.exe	Get hash	malicious	Browse	• 162.159.135.233
	qqlbBIsqPQ.exe	Get hash	malicious	Browse	• 162.159.135.233
	Bxs1wBHcNS.exe	Get hash	malicious	Browse	• 162.159.133.233

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ASN-QUADRANET-GLOBALUS	BahcfFNy25bmV1c.exe	Get hash	malicious	Browse	• 154.81.38.79
	Invoice-packing list BL NO. 212142500 MRKU7550471 ML-IN4104393.tar	Get hash	malicious	Browse	• 204.44.86.179
	PO23456.doc	Get hash	malicious	Browse	• 104.223.93.90
	Swift Copy.doc	Get hash	malicious	Browse	• 104.223.93.90
	mips	Get hash	malicious	Browse	• 104.223.82.208
	DHL-Express-Document.doc	Get hash	malicious	Browse	• 104.223.93.90
	DHL-Express-Description.doc	Get hash	malicious	Browse	• 104.223.93.90
	iq12CZCZjT	Get hash	malicious	Browse	• 198.96.89.47
	ORDER ACKNOWLEDGEMENT & PROFORMA INVOICE .PDF.EXE	Get hash	malicious	Browse	• 154.81.38.104
	udp	Get hash	malicious	Browse	• 204.44.93.54
	lgTwTtkeIR	Get hash	malicious	Browse	• 155.94.178.138
	try.exe	Get hash	malicious	Browse	• 69.174.100.168
	RmjhrUdTri.exe	Get hash	malicious	Browse	• 172.93.187.66
	syna	Get hash	malicious	Browse	• 155.94.178.138
	New_Order_for_September#442625272-doc-signed copy.exe	Get hash	malicious	Browse	• 204.44.86.179
	New_Order_for_September#442625272-doc-signed copy.exe	Get hash	malicious	Browse	• 204.44.86.179
	mirai.x86	Get hash	malicious	Browse	• 107.150.24.141
	BALLANCE PAYMENT.doc	Get hash	malicious	Browse	• 104.223.93.90
	5sNHIrfRwn.exe	Get hash	malicious	Browse	• 107.150.23.149
	1073645267891287347.jar	Get hash	malicious	Browse	• 172.93.187.66
CLOUDFLARENETUS	z5WnxHv7bg.exe	Get hash	malicious	Browse	• 104.18.6.156
	0HsDg7f3eG.exe	Get hash	malicious	Browse	• 104.18.6.156
	3RQvR8bIfa.exe	Get hash	malicious	Browse	• 104.18.7.156
	Swift 07.09.21.exe	Get hash	malicious	Browse	• 66.235.200.146
	IMG_80350001.exe	Get hash	malicious	Browse	• 104.18.6.156
	IMG_8035002078801.doc	Get hash	malicious	Browse	• 104.18.7.156
	DLT_85620000107.exe	Get hash	malicious	Browse	• 23.227.38.74
	SvgoEJMLe7.dll	Get hash	malicious	Browse	• 172.67.70.134
	a1gc77eplx.dll	Get hash	malicious	Browse	• 104.26.6.139
	OKS.exe	Get hash	malicious	Browse	• 172.67.188.154
	eDpXMjvZO0.exe	Get hash	malicious	Browse	• 172.67.173.58
	9c2NwBeaMN.exe	Get hash	malicious	Browse	• 104.21.34.192
	famz6.doc	Get hash	malicious	Browse	• 23.227.38.74
	2101222_OrdineFornitore del.ppam	Get hash	malicious	Browse	• 162.159.133.233
	SYuBVzCs5U.exe	Get hash	malicious	Browse	• 172.67.221.88
	cs.exe	Get hash	malicious	Browse	• 172.67.164.78
	ORDER 33212762.ppam	Get hash	malicious	Browse	• 162.159.134.233

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	vbc(1).exe	Get hash	malicious	Browse	• 104.21.89.140
	ENQUIRYSMRT119862021-ERW PIPES.pdf.exe	Get hash	malicious	Browse	• 172.67.196.70
	COAU7229898130.xlsx	Get hash	malicious	Browse	• 104.21.8.222

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	uYZQ72bfTF.exe	Get hash	malicious	Browse	• 162.159.135.233
	yGY3UQymu4.exe	Get hash	malicious	Browse	• 162.159.135.233
	cGJ916maFX.exe	Get hash	malicious	Browse	• 162.159.135.233
	OffboardDiagLauncher.exe	Get hash	malicious	Browse	• 162.159.135.233
	scan_doc001091121.exe	Get hash	malicious	Browse	• 162.159.135.233
	FedEx AWB# 8611746580734 ,PDF.exe	Get hash	malicious	Browse	• 162.159.135.233
	RFQ_PARTS PRICELIST 110-10007046,pdf.exe	Get hash	malicious	Browse	• 162.159.135.233
	RFQ 2021-09.exe	Get hash	malicious	Browse	• 162.159.135.233
	Quote.exe	Get hash	malicious	Browse	• 162.159.135.233
	purchase order.exe	Get hash	malicious	Browse	• 162.159.135.233
	bt2091.exe	Get hash	malicious	Browse	• 162.159.135.233
	b3qnpvoALc.exe	Get hash	malicious	Browse	• 162.159.135.233
	8X0Zj8zIDN.exe	Get hash	malicious	Browse	• 162.159.135.233
	OKS.exe	Get hash	malicious	Browse	• 162.159.135.233
	eDpXMjvZO0.exe	Get hash	malicious	Browse	• 162.159.135.233
	Ted_Yeung.html	Get hash	malicious	Browse	• 162.159.135.233
	Ted_Yeung.html	Get hash	malicious	Browse	• 162.159.135.233
	Qly2dKZwCy.exe	Get hash	malicious	Browse	• 162.159.135.233
	2101222_OrdineFornitore del.ppam	Get hash	malicious	Browse	• 162.159.135.233
	aJkjc0EPD2.exe	Get hash	malicious	Browse	• 162.159.135.233

Dropped Files

No context

Created / dropped Files

C:\Users\Public\Libraries\Cshgvzx\Cshgvzx.exe

Process:	C:\Users\user\Desktop\RFQ-Order_Sheet#43254363-Sept-21_signed-copy.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	792576
Entropy (8bit):	6.622449628761002
Encrypted:	false
SSDEEP:	6144:5CZ5dEs7ZrwziKYDZ2/avaYvqfbUacyHeP/hz0Xkb5fjUOCMXjqfZPFVb/4rr7ZW:QZ5l7ZrwzLCMHHi5rUll64rimoAzyZV
MD5:	06534C059B111776B838F793C6444622
SHA1:	7EBDA7124A60DE107A00960D9FE0563FD3CD2760
SHA-256:	933A4D2ABFDF0F91550A102808D00ADACE6EB9DF89EA9E254E2DF7601B02DD8F
SHA-512:	9E1498B78D6682F1CDE8717A85570DF742D4FA2D7C59D554AFB938AF4DB1EEFFB13522682068D81EFC676DDD4DD80741ABCF1B1AE94560B01AD2C4FDF69D9(DD

C:\Users\Public\Libraries\Cshgvzx\Cshgvzx.exe	
Malicious:	**true**
Reputation:	low
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....4.....4.....@.....@.....L#...p...&.....j..... .....CODE....|..... ..`DATA.....z.....|.....@...BSS.....A4...p.....`.....idata..L#.....$...`.....@....tls.....rdata .....@..P.reloc...j.....l.....@..P.rsrc....&...p...&.....@..P.....@..P..... .....

C:\Users\Public\Libraries\xzvghsC.url	
Process:	C:\Users\user\Desktop\RFQ-Order_Sheet#43254363-Sept-21_signed-copy.exe
File Type:	MS Windows 95 Internet shortcut text (URL=<file:"C:\\Users\\Public\\Libraries\\Cshgvzx\\Cshgvzx.exe">), ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	96
Entropy (8bit):	4.866547012067739
Encrypted:	false
SSDEEP:	3:HRAbABGQYmTWAX+rSF55i0XMKf6ABvsGKd7ovn:HRYFVmTWDyz/vsb7yn
MD5:	2DDF040A20140597A72FE56E21E798F0
SHA1:	5DCAFBE1835C1A8AC7A97586B6BEF970A6FFC60B
SHA-256:	01ED6321AF738C2093089DD77FDE2C2B54A70655499BC8490B835FDEB4A66FDE
SHA-512:	1369F56AEF6B4FFBB5EBE1AC161FB52693B535259CEF4D0F0842A7C7789F65A9FAFE825C2FFB1D5CCE5563930C0A2DDECBF0CEC6E63E559B6344856E3857C054
Malicious:	false
Yara Hits:	• Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: C:\Users\Public\Libraries\xzvghsC.url, Author: @itsreallynick (Nick Carr)
Reputation:	low
Preview:	[InternetShortcut]..URL=file:"C:\\Users\\Public\\Libraries\\Cshgvzx\\Cshgvzx.exe"..IconIndex=3..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\Cshgvzxpdvyucjurgvmywubhtofxefb[1]	
Process:	C:\Users\Public\Libraries\Cshgvzx\Cshgvzx.exe
File Type:	data
Category:	dropped
Size (bytes):	579072
Entropy (8bit):	**7.997266864646308**
Encrypted:	**true**
SSDEEP:	12288:VIjmqCh/9ePXG9kqy8Yc73pGyho53rgTgbPJ+H7it/rEj/sOf3rr:HqCh8vM3FYZy65cTgbE76z9Of/
MD5:	B5DC22D709B4D41A4B7160A90C203274
SHA1:	48663BAE9BB24E3EBB48F72A81B4CA2AE875D864
SHA-256:	89AFE9CCEFAC3D8481859648551A0F4E7C279F453137E2E6881AFA28EB9262C3
SHA-512:	8AC8EDC4FDC5C682250C7C76E595E40D905A1D5E771D356979209CAA8969F7B3808D7038033A1DFC05A86BA8CB56297BDE124D11B80BF940709EE57F5B3A43A
Malicious:	false
Reputation:	low
Preview:	.....O$.l.....VI)_.W.....G0.2.m.>.t./dt.....z".`a.9.z'l5dw.VI)_.W.....G0.2.m.>.t./dt.....z".`a.9.z'l5dw.VI)_.W.....G0.2.m.>.t./dt.....z".`a.9.z'l5dw.VI)_.W.....G0.2.m.>.t./dt.....z".`a.9.z'l5dw.VI)_.W.....G0.2.m.>.t./dt.....z".`a.9.z'l5dw.VI)_.W.....G0.2.m.>.t./dt.....z".`a.9.z'l5dw.VI)_.W.....G0.2.m.>.t./dt.....z".`a.9.z'l5dw.VI)_.W.....G0.2.m.>.t./dt.....z".`a.9.z'l5dw.VI)_.W.....G0.2.m.>.t...:....":.. .vl.)G=....?p}.....i.-..0.3dVi.....i..Ap)q.'N.+L..m.....h.....D.$.|N.....a ._.B.I.n.*..A.....s..D....*.i..Ap)q.'N.+L..m.....h.....D.$.|N.....a._.B.I.n.*..A.....s..D....*.i..Ap)q.'N..O...`$.....CJ..Z.i..8.....++?N.b7D..\..~q....g.|o..&.a.\.R&vA...c..|qS..W... ....N%...?."\.$UD..C...8...?..&5..Es.I_.....)...b>.W.f&..Oh%..j&....-3?IvL...X...CA[...u.....]........I_.D....=Kb3+&..4..6..a...16..#...Z..B....u...w.....%.....lF..xzs....x.....5-D..... .'.%..@.$.4.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\Cshgvzxpdvyucjurgvmywubhtofxefb[2]	
Process:	C:\Users\Public\Libraries\Cshgvzx\Cshgvzx.exe
File Type:	data
Category:	dropped
Size (bytes):	579072
Entropy (8bit):	**7.997266864646308**
Encrypted:	**true**
SSDEEP:	12288:VIjmqCh/9ePXG9kqy8Yc73pGyho53rgTgbPJ+H7it/rEj/sOf3rr:HqCh8vM3FYZy65cTgbE76z9Of/
MD5:	B5DC22D709B4D41A4B7160A90C203274
SHA1:	48663BAE9BB24E3EBB48F72A81B4CA2AE875D864
SHA-256:	89AFE9CCEFAC3D8481859648551A0F4E7C279F453137E2E6881AFA28EB9262C3
SHA-512:	8AC8EDC4FDC5C682250C7C76E595E40D905A1D5E771D356979209CAA8969F7B3808D7038033A1DFC05A86BA8CB56297BDE124D11B80BF940709EE57F5B3A43A
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\Cshgvzxpdvyucjurgvmywubhtofxefb[2]	
Preview:	.....O$.l.....VI)_.W.....G0.2.m.>.t./dt.....z".`a.9.z'l5dw.VI)_.W.....G0.2.m.>.t./dt.....z".`a.9.z'l5dw.VI)_.W.....G0.2.m.>.t./dt.....z".`a.9.z'l5dw.VI)_.W.....G0.2.m.>.t./dt.....z".`a.9.z'l5dw.VI)_.W.....G0.2.m.>.t./dt.....z".`a.9.z'l5dw.VI)_.W.....G0.2.m.>.t./dt.....z".`a.9.z'l5dw.VI)_.W.....G0.2.m.>.t./dt.....z".`a.9.z'l5dw.VI)_.W.....G0.2.m.>.t...:....":.. .vl.)G=....?p}.....i.-..0.3dVi.....i..Ap)q.'N.+L..m.....h.....D.$.|N.....a ._.B.I.n.*..A.....s..D....*.i..Ap)q.'N.+L..m.....h.....D.$.|N.....a._.B.I.n.*..A.....s..D....*.i..Ap)q.'N..O...`$....CJ..Z.i..8.....++?N.b7D..\..~q....g.|o..&.a.\.R&vA...c..|qS..W... ....N%...?."\.$UD..C...8...?..&5..Es.l_.....)...b>.W.f&..Oh%..j&....-3?IvL...X...CA[...u.....]........l_.D....=Kb3+&..4..6..a...16..#...Z..B....u...w.....%.....lF..xzs....x.....5-D..... .'.%..@.$.4.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.622449628761002
TrID:	• Win32 Executable (generic) a (10002005/4) 99.66% • Win32 Executable Delphi generic (14689/80) 0.15% • Windows Screen Saver (13104/52) 0.13% • Win16/32 Executable Delphi generic (2074/23) 0.02% • Generic Win/DOS Executable (2004/3) 0.02%
File name:	RFQ-Order_Sheet#43254363-Sept-21_signed-copy.exe
File size:	792576
MD5:	06534c059b111776b838f793c6444622
SHA1:	7ebda7124a60de107a00960d9fe0563fd3cd2760
SHA256:	933a4d2abfdf0f91550a102808d00adace6eb9df89ea9e254e2df7601b02dd8f
SHA512:	9e1498b78d6682f1cde8717a85570df742d4fa2d7c59d554afb938af4db1eeffb13522682068d81efc676ddd4dd80741abcf1b1ae94560b01ad2c4fdf69d9cdd
SSDEEP:	6144:5CZ5dEs7ZrwziKYDZ2/avaYvqfbUacyHeP/hz0Xkb5fjUOCMXjqfZPFVb/4rr7ZW:QZ5l7ZrwzLCMHHi5rUll64rimoAzyZV
File Content Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... ....

File Icon

Icon Hash:	acaca4b2a2968ea2

Static PE Info

General

Entrypoint:	0x45ef34
Entrypoint Section:	CODE
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, BYTES_REVERSED_LO, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, BYTES_REVERSED_HI
DLL Characteristics:	
Time Stamp:	0x2A425E19 [Fri Jun 19 22:22:17 1992 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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:	4dfd1417e7c3ef71650aaaaec402ef1c

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
CODE	0x1000	0x5df7c	0x5e000	False	0.528699509641	data	6.55764320265	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
DATA	0x5f000	0x47af4	0x47c00	False	0.249173154399	data	5.2159972367	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
BSS	0xa7000	0x53441	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.idata	0xfb000	0x234c	0x2400	False	0.3623046875	data	4.99388267016	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.tls	0xfe000	0x10	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rdata	0xff000	0x18	0x200	False	0.052734375	data	0.203013767787	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.reloc	0x100000	0x6a90	0x6c00	False	0.62037037037	data	6.66625425433	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.rsrc	0x107000	0x12600	0x12600	False	0.194608312075	data	3.98030669674	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/07/21-18:17:02.843080	TCP	2032776	ET TROJAN Remocs 3.x Unencrypted Checkin	49707	49151	192.168.2.5	204.44.86.179
09/07/21-18:17:03.200734	TCP	2032777	ET TROJAN Remocs 3.x Unencrypted Server Response	49151	49707	204.44.86.179	192.168.2.5

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 7, 2021 18:16:40.749583960 CEST	192.168.2.5	8.8.8.8	0x3851	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Sep 7, 2021 18:17:01.364059925 CEST	192.168.2.5	8.8.8.8	0xfb4b	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 7, 2021 18:17:11.635313988 CEST	192.168.2.5	8.8.8.8	0x8fbf	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 7, 2021 18:16:40.787383080 CEST	8.8.8.8	192.168.2.5	0x3851	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Sep 7, 2021 18:16:40.787383080 CEST	8.8.8.8	192.168.2.5	0x3851	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Sep 7, 2021 18:16:40.787383080 CEST	8.8.8.8	192.168.2.5	0x3851	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Sep 7, 2021 18:16:40.787383080 CEST	8.8.8.8	192.168.2.5	0x3851	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Sep 7, 2021 18:16:40.787383080 CEST	8.8.8.8	192.168.2.5	0x3851	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Sep 7, 2021 18:17:01.399791002 CEST	8.8.8.8	192.168.2.5	0xfb4b	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Sep 7, 2021 18:17:01.399791002 CEST	8.8.8.8	192.168.2.5	0xfb4b	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Sep 7, 2021 18:17:01.399791002 CEST	8.8.8.8	192.168.2.5	0xfb4b	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Sep 7, 2021 18:17:01.399791002 CEST	8.8.8.8	192.168.2.5	0xfb4b	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Sep 7, 2021 18:17:01.399791002 CEST	8.8.8.8	192.168.2.5	0xfb4b	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Sep 7, 2021 18:17:11.671046019 CEST	8.8.8.8	192.168.2.5	0x8fbf	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Sep 7, 2021 18:17:11.671046019 CEST	8.8.8.8	192.168.2.5	0x8fbf	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Sep 7, 2021 18:17:11.671046019 CEST	8.8.8.8	192.168.2.5	0x8fbf	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Sep 7, 2021 18:17:11.671046019 CEST	8.8.8.8	192.168.2.5	0x8fbf	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Sep 7, 2021 18:17:11.671046019 CEST	8.8.8.8	192.168.2.5	0x8fbf	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Sep 7, 2021 18:16:40.871368885 CEST	162.159.135.233	443	192.168.2.5	49699	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	Tue Jan 19 01:00:00 CET 2021 Mon Jan 27 13:48:08 CET 2020	Wed Jan 19 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Sep 7, 2021 18:17:01.542766094 CEST	162.159.135.233	443	192.168.2.5	49706	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	Tue Jan 19 01:00:00 CET 2021 Mon Jan 27 13:48:08 CET 2020	Wed Jan 19 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					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		
Sep 7, 2021 18:17:11.782536983 CEST	162.159.135.233	443	192.168.2.5	49708	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	Tue Jan 19 01:00:00 CET 2021 Mon Jan 27 13:48:08 CET 2020	Wed Jan 19 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					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

Click to jump to process

System Behavior

Analysis Process: RFQ-Order_Sheet#43254363-Sept-21_signed-copy.exe PID: 5256
Parent PID: 1456

General

Start time:	18:16:33
Start date:	07/09/2021
Path:	C:\Users\user\Desktop\RFQ-Order_Sheet#43254363-Sept-21_signed-copy.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\RFQ-Order_Sheet#43254363-Sept-21_signed-copy.exe'
Imagebase:	0x400000
File size:	792576 bytes
MD5 hash:	06534C059B111776B838F793C6444622
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities Show Windows behavior

Key Value Created

Analysis Process: Cshgvzx.exe PID: 5384 Parent PID: 3472

General

Start time:	18:16:52
Start date:	07/09/2021
Path:	C:\Users\Public\Libraries\Cshgvzx\Cshgvzx.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\Libraries\Cshgvzx\Cshgvzx.exe'
Imagebase:	0x400000
File size:	792576 bytes
MD5 hash:	06534C059B111776B838F793C6444622
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: mobsync.exe PID: 4692 Parent PID: 5256

General

Start time:	18:16:59
Start date:	07/09/2021
Path:	C:\Windows\SysWOW64\mobsync.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\mobsync.exe
Imagebase:	0x7ff797770000
File size:	93184 bytes
MD5 hash:	44C19378FA529DD88674BAF647EBDC3C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000008.00000002.492585881.00000000030E7000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000008.00000002.491601903.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: REMCOS_RAT_variants, Description: unknown, Source: 00000008.00000002.491601903.0000000000400000.00000040.00000001.sdmp, Author: unknown • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000008.00000002.492970715.0000000010590000.00000040.00000001.sdmp, Author: Joe Security • Rule: REMCOS_RAT_variants, Description: unknown, Source: 00000008.00000002.492970715.0000000010590000.00000040.00000001.sdmp, Author: unknown
Reputation:	moderate

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: Cshgvzx.exe PID: 5296 Parent PID: 3472

General

Start time:	18:17:00
Start date:	07/09/2021
Path:	C:\Users\Public\Libraries\Cshgvzx\Cshgvzx.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\Libraries\Cshgvzx\Cshgvzx.exe'
Imagebase:	0x400000
File size:	792576 bytes
MD5 hash:	06534C059B111776B838F793C6444622
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Reputation:	low

File Activities

Show Windows behavior

Analysis Process: dialer.exe PID: 6544 Parent PID: 5384

General

Start time:	18:17:20
Start date:	07/09/2021
Path:	C:\Windows\SysWOW64\dialer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\dialer.exe
Imagebase:	0xe10000
File size:	32768 bytes
MD5 hash:	F176211F7372248224D02AC023573870
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000012.00000002.331608026.0000000002F98000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000012.00000002.331374887.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: REMCOS_RAT_variants, Description: unknown, Source: 00000012.00000002.331374887.0000000000400000.00000040.00000001.sdmp, Author: unknown • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000012.00000002.331771013.0000000010590000.00000040.00000001.sdmp, Author: Joe Security • Rule: REMCOS_RAT_variants, Description: unknown, Source: 00000012.00000002.331771013.0000000010590000.00000040.00000001.sdmp, Author: unknown
Reputation:	moderate

Analysis Process: secinit.exe PID: 6672 Parent PID: 5296

General

Start time:	18:17:32
Start date:	07/09/2021
Path:	C:\Windows\SysWOW64\secinit.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\secinit.exe
Imagebase:	0x12a0000
File size:	9728 bytes
MD5 hash:	174A363BB5A2D88B224546C15DD10906
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000013.00000002.356743910.0000000000500000.00000040.00000001.sdmp, Author: Joe Security • Rule: REMCOS_RAT_variants, Description: unknown, Source: 00000013.00000002.356743910.0000000000500000.00000040.00000001.sdmp, Author: unknown • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000013.00000002.356991304.0000000010590000.00000040.00000001.sdmp, Author: Joe Security • Rule: REMCOS_RAT_variants, Description: unknown, Source: 00000013.00000002.356991304.0000000010590000.00000040.00000001.sdmp, Author: unknown • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000013.00000002.356879289.00000000006E8000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	moderate

Disassembly

Code Analysis