ID: 356426
Sample Name: Request for Quotation.exe
Cookbook: default.jbs
Time: 07:35:17
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

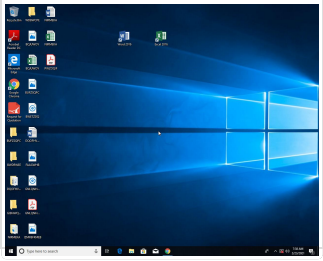
Analysis Report Request for Quotation.exe

Overview

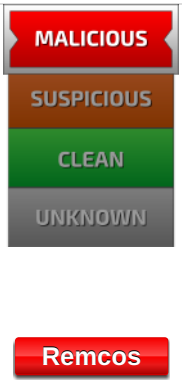
General Information

Sample Name:	Request for Quotation.exe
Analysis ID:	356426
MD5:	ae4bd6c5a7eaa5..
SHA1:	ab597cfc0433999..
SHA256:	8e51354c8b2f461..
Tags:	RemcosRAT

Most interesting Screenshot:



Detection



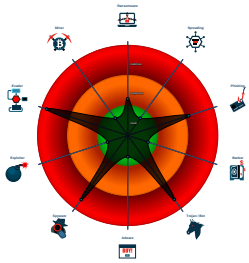
Remcos

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

Signatures

- Detected Remcos RAT
- Detected unpacking (changes PE se…
- Detected unpacking (overwrites its o…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Yara detected Remcos RAT
- C2 URLs / IPs found in malware con…
- Contains functionality to capture and…
- Contains functionality to inject code …
- Contains functionality to steal Chrom…
- Contains functionality to steal Firefo…

Classification



Startup

- **System is w10x64**
- Request for Quotation.exe (PID: 7164 cmdline: 'C:\Users\user\Desktop\Request for Quotation.exe' MD5: AE4BD6C5A7EAA50704D43D6054FC5DBD)
  - Request for Quotation.exe (PID: 612 cmdline: 'C:\Users\user\Desktop\Request for Quotation.exe' MD5: AE4BD6C5A7EAA50704D43D6054FC5DBD)
    - Request for Quotation.exe (PID: 6188 cmdline: 'C:\Users\user\Desktop\Request for Quotation.exe' /stext 'C:\Users\user\AppData\Local\Temp\hbieekorpghvpuxbpehxjpq' MD5: AE4BD6C5A7EAA50704D43D6054FC5DBD)
    - Request for Quotation.exe (PID: 6424 cmdline: 'C:\Users\user\Desktop\Request for Quotation.exe' /stext 'C:\Users\user\AppData\Local\Temp\rvowfdgtdozazitngptymckjrq' MD5: AE4BD6C5A7EAA50704D43D6054FC5DBD)
    - Request for Quotation.exe (PID: 5692 cmdline: 'C:\Users\user\Desktop\Request for Quotation.exe' /stext 'C:\Users\user\AppData\Local\Temp\uptpyvrmrwrfbohrpag sxhxaawaqan' MD5: AE4BD6C5A7EAA50704D43D6054FC5DBD)
- **cleanup**

Malware Configuration

Threatname: Remcos

```
{
  "Host:Port:Password": "103.89.88.238:4299:s%qDr",
  "Assigned name": "RemoteHost",
  "Connect interval": "1",
  "Install flag": "Disable",
  "Setup HKCU\\Run": "Enable",
  "Setup HKLM\\Run": "Disable",
  "Install path": "AppData",
  "Copy file": "excel.exe",
  "Startup value": "excel",
  "Hide file": "Disable",
  "Mutex": "excel-8OHAVR",
  "Keylog flag": "1",
  "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": "wikipedia;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": "0"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.903195414.000000000400000.00000040.00000001.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
00000001.00000002.903195414.000000000400000.00000040.00000001.sdmp	Remcos_1	Remcos Payload	kevoreilly	• 0x16510:$name: Remcos • 0x16888:$name: Remcos • 0x16de0:$name: Remcos • 0x16e33:$name: Remcos • 0x15674:$time: %02i:%02i:%02i:%03i • 0x156fc:$time: %02i:%02i:%02i:%03i • 0x16be4:$time: %02i:%02i:%02i:%03i • 0x3074:$crypto: 0F B6 D0 8B 45 08 89 16 8D 34 07 8B 01 03 C2 8B CB 99 F7 F9 8A 84 95 F8 FB FF FF 30 06 47 3B 7D ...
00000001.00000002.903195414.000000000400000.00000040.00000001.sdmp	REMCOS_RAT_variants	unknown	unknown	• 0x166f8:$str_a1: C:\Windows\System32\cmd.exe • 0x16714:$str_a3: /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWOR • 0x16714:$str_a4: /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWOR • 0x15dfc:$str_a5: \AppData\Local\Google\Chrome\User Data\Default\Login Data • 0x16400:$str_b1: CreateObject("Scripting.FileSystemObject").DeleteFile(Wscript.ScriptFullName) • 0x159e0:$str_b2: Executing file: • 0x16798:$str_b3: GetDirectListeningPort • 0x16240:$str_b4: Set fso = CreateObject("Scripting.FileSystemObject") • 0x16534:$str_b5: licence_code.txt • 0x1649c:$str_b6: \restart.vbs • 0x163c0:$str_b8: \uninstall.vbs • 0x1596c:$str_b9: Downloaded file: • 0x15998:$str_b10: Downloading file: • 0x15690:$str_b11: KeepAlive Enabled! Timeout: %i seconds • 0x159fc:$str_b12: Failed to upload file: • 0x167d8:$str_b13: StartForward • 0x167bc:$str_b14: StopForward • 0x16330:$str_b15: fso.DeleteFile " • 0x16394:$str_b16: On Error Resume Next • 0x162fc:$str_b17: fso.DeleteFolder " • 0x15a14:$str_b18: Uploaded file:
00000001.00000001.641497403.000000000400000.00020000.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000001.00000001.641497403.000000000400000.00000040.00020000.sdmp	Remcos_1	Remcos Payload	kevoreilly	• 0x16510:$name: Remcos • 0x16888:$name: Remcos • 0x16de0:$name: Remcos • 0x16e33:$name: Remcos • 0x15674:$time: %02i:%02i:%02i:%03i • 0x156fc:$time: %02i:%02i:%02i:%03i • 0x16be4:$time: %02i:%02i:%02i:%03i • 0x3074:$crypto: 0F B6 D0 8B 45 08 89 16 8D 34 07 8B 01 03 C2 8B CB 99 F7 F9 8A 84 95 F8 FB FF FF 30 06 47 3B 7D ...
Click to see the 7 entries				

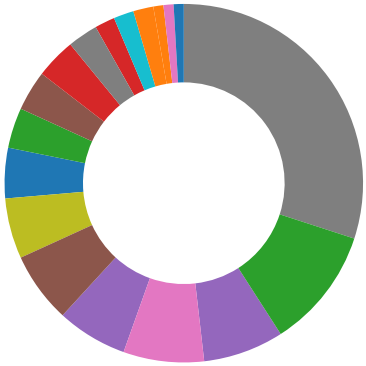
Unpacked PEs

Source	Rule	Description	Author	Strings
1.1.Request for Quotation.exe.400000.0.raw.unpack	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
1.1.Request for Quotation.exe.400000.0.raw.unpack	Remcos_1	Remcos Payload	kevoreilly	• 0x16510:$name: Remcos • 0x16888:$name: Remcos • 0x16de0:$name: Remcos • 0x16e33:$name: Remcos • 0x15674:$time: %02i:%02i:%02i:%03i • 0x156fc:$time: %02i:%02i:%02i:%03i • 0x16be4:$time: %02i:%02i:%02i:%03i • 0x3074:$crypto: 0F B6 D0 8B 45 08 89 16 8D 34 07 8B 01 03 C2 8B CB 99 F7 F9 8A 84 95 F8 FB FF FF 30 06 47 3B 7D ...
1.1.Request for Quotation.exe.400000.0.raw.unpack	REMCOS_RAT_variants	unknown	unknown	• 0x166f8:$str_a1: C:\Windows\System32\cmd.exe • 0x16714:$str_a3: /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWOR • 0x16714:$str_a4: /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWOR • 0x15dfc:$str_a5: \AppData\Local\Google\Chrome\User Data\Default\Login Data • 0x16400:$str_b1: CreateObject("Scripting.FileSystemObject").DeleteFile(Wscript.ScriptFullName) • 0x159e0:$str_b2: Executing file: • 0x16798:$str_b3: GetDirectListeningPort • 0x16240:$str_b4: Set fso = CreateObject("Scripting.FileSystemObject") • 0x16534:$str_b5: licence_code.txt • 0x1649c:$str_b6: \restart.vbs • 0x163c0:$str_b8: \uninstall.vbs • 0x1596c:$str_b9: Downloaded file: • 0x15998:$str_b10: Downloading file: • 0x15690:$str_b11: KeepAlive Enabled! Timeout: %i seconds • 0x159fc:$str_b12: Failed to upload file: • 0x167d8:$str_b13: StartForward • 0x167bc:$str_b14: StopForward • 0x16330:$str_b15: fso.DeleteFile " • 0x16394:$str_b16: On Error Resume Next • 0x162fc:$str_b17: fso.DeleteFolder " • 0x15a14:$str_b18: Uploaded file:
1.1.Request for Quotation.exe.400000.0.unpack	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
1.1.Request for Quotation.exe.400000.0.unpack	Remcos_1	Remcos Payload	kevoreilly	• 0x16510:$name: Remcos • 0x16888:$name: Remcos • 0x16de0:$name: Remcos • 0x16e33:$name: Remcos • 0x15674:$time: %02i:%02i:%02i:%03i • 0x156fc:$time: %02i:%02i:%02i:%03i • 0x16be4:$time: %02i:%02i:%02i:%03i • 0x3074:$crypto: 0F B6 D0 8B 45 08 89 16 8D 34 07 8B 01 03 C2 8B CB 99 F7 F9 8A 84 95 F8 FB FF FF 30 06 47 3B 7D ...
Click to see the 13 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Cryptography
- Compliance
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected Remcos RAT

Machine Learning detection for sample

Compliance:

Detected unpacking (overwrites its own PE header)

Uses 32bit PE files

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

Binary contains paths to debug symbols

Networking:

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Contains functionality to capture and log keystrokes

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

Data Obfuscation:

Detected unpacking (changes PE section rights)

Detected unpacking (overwrites its own PE header)

HIPS / PFW / Operating System Protection Evasion:

- Contains functionality to inject code into remote processes
- Injects a PE file into a foreign processes
- Maps a DLL or memory area into another process

Stealing of Sensitive Information:

- Yara detected Remcos RAT
- Contains functionality to steal Chrome passwords or cookies
- Contains functionality to steal Firefox passwords or cookies
- Tries to harvest and steal browser information (history, passwords, etc)
- Tries to steal Instant Messenger accounts or passwords
- Tries to steal Mail credentials (via file access)
- Tries to steal Mail credentials (via file registry)
- Yara detected WebBrowserPassView password recovery tool

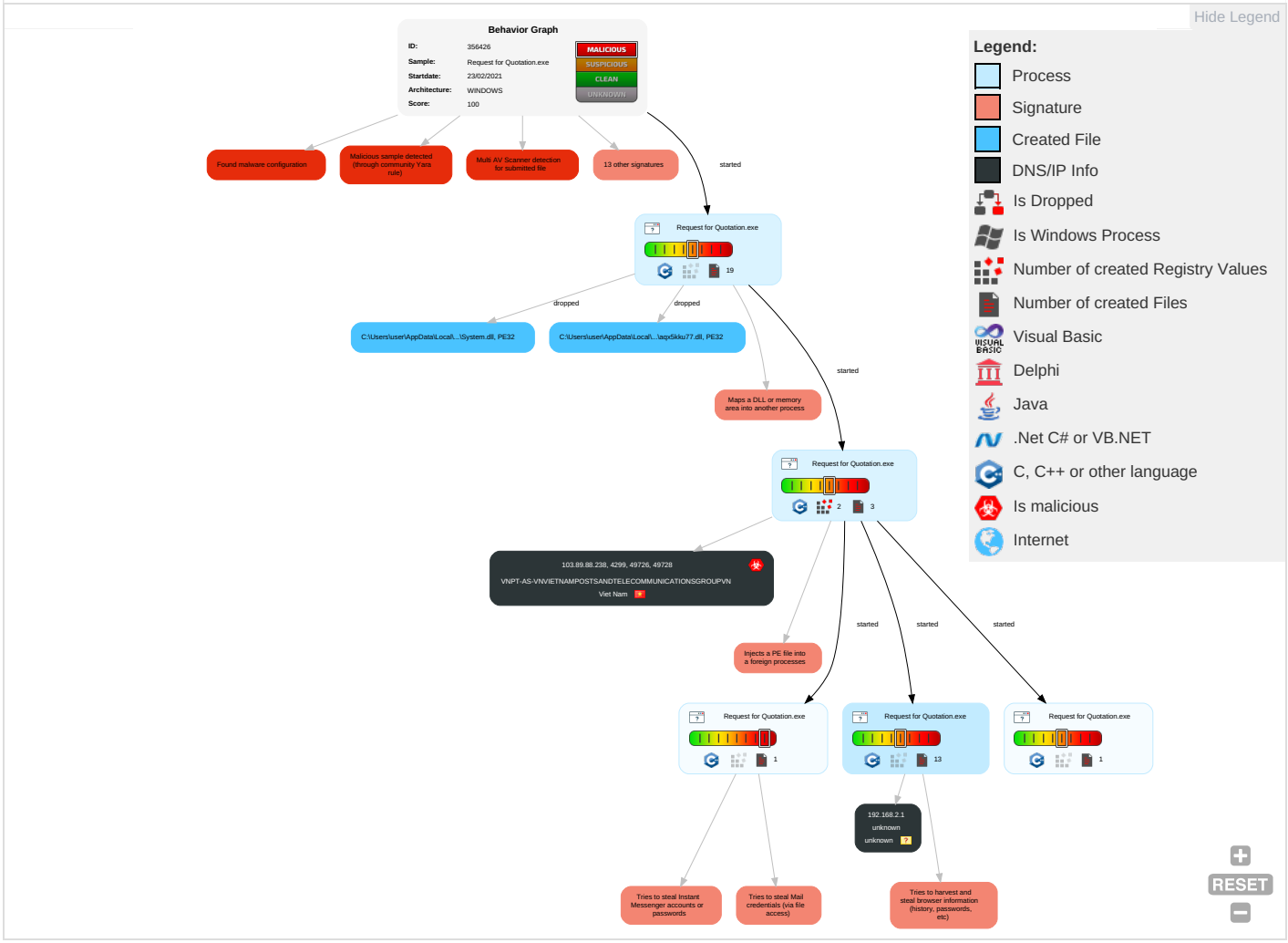
Remote Access Functionality:

- Detected Remcos RAT
- Yara detected Remcos RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	C a
Valid Accounts	Native API 1	Application Shimming 1	Application Shimming 1	Deobfuscate/Decode Files or Information 1	OS Credential Dumping 2	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	In Tr
Default Accounts	Command and Scripting Interpreter 1	Windows Service 1	Access Token Manipulation 1	Obfuscated Files or Information 3	Input Capture 1 1 1	Account Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Ex Cl
Domain Accounts	Service Execution 2	Logon Script (Windows)	Windows Service 1	Software Packing 2 2	Credentials in Registry 2	System Service Discovery 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	No Po
Local Accounts	At (Windows)	Logon Script (Mac)	Process Injection 3 2 2	Masquerading 1	Credentials In Files 3	File and Directory Discovery 3	Distributed Component Object Model	Input Capture 1 1 1	Scheduled Transfer	Re Se
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 2	LSA Secrets	System Information Discovery 4 8	SSH	Clipboard Data 2	Data Transfer Size Limits	Ap La Pr
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Access Token Manipulation 1	Cached Domain Credentials	Security Software Discovery 2 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	M Co
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 3 2 2	DCSync	Virtualization/Sandbox Evasion 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Co Us
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Process Discovery 4	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Ap La
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Application Window Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	W
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	System Owner/User Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	Fi Pr

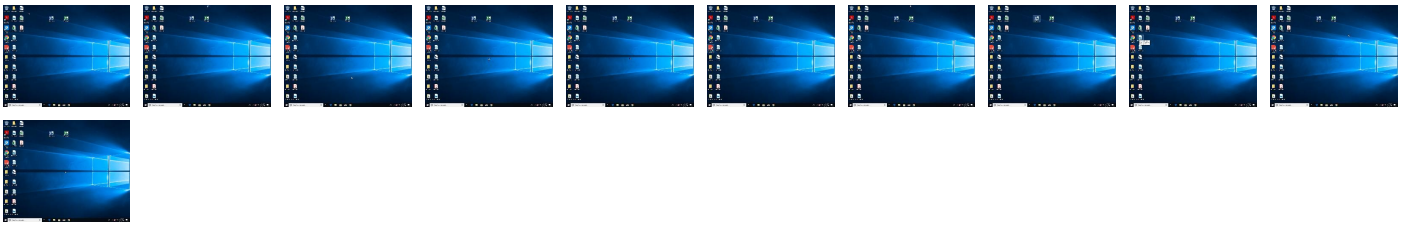
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Request for Quotation.exe	27%	Virustotal		Browse
Request for Quotation.exe	14%	Metadefender		Browse
Request for Quotation.exe	21%	ReversingLabs	Win32.Backdoor.Remcos	
Request for Quotation.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\aqx5kku77.dll	6%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsc77A8.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsc77A8.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.0.Request for Quotation.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
0.2.Request for Quotation.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
1.0.Request for Quotation.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
4.2.Request for Quotation.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1116590		Download File
5.0.Request for Quotation.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
1.1.Request for Quotation.exe.400000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
5.2.Request for Quotation.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1116590		Download File
4.0.Request for Quotation.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
0.2.Request for Quotation.exe.2a50000.5.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
3.2.Request for Quotation.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1116566		Download File
0.0.Request for Quotation.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
1.2.Request for Quotation.exe.400000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.imvu.comr	0%	Avira URL Cloud	safe	
103.89.88.238	0%	Avira URL Cloud	safe	
http://www.ebuddy.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

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

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://contextual.media.net/checksync.phphttps://contextual.media.net/medianet.php?cid=8CU157172&cr	Request for Quotation.exe, 00000003.00000003.653713973.00000000022C4000.00000004.00000001.sdmp	false		high
http://https://login.yahoo.com/config/login	Request for Quotation.exe	false		high
http://www.imvu.comr	Request for Quotation.exe, 00000004.00000002.652481642.00000000000400000.00000040.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://nsis.sf.net/NSIS_Error	Request for Quotation.exe	false		high
http://www.nirsoft.net	Request for Quotation.exe, 00000003.00000002.654097061.00000000000193000.00000004.00000010.sdmp	false		high
http://nsis.sf.net/NSIS_ErrorError	Request for Quotation.exe	false		high
http://www.nirsoft.net/	Request for Quotation.exe, Request for Quotation.exe, 00000005.00000001.652992004.0000000000400000.00000040.00020000.sdmp	false		high
http://https://contextual.media.net/checksync.php?&vsSync=1&cs=1&hb=1&cv=37&ndec=1&cid=8HBI57XIG&prvid=77%2	Request for Quotation.exe, 00000003.00000003.652133843.00000000022C3000.00000004.00000001.sdmp, Request for Quotation.exe, 00000003.00000003.653713973.00000000022C4000.00000004.00000001.sdmp	false		high
http://www.ebuddy.com	Request for Quotation.exe	false	• Avira URL Cloud: safe	unknown
http://www.imvu.com	Request for Quotation.exe	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.89.88.238	unknown	Viet Nam		135905	VNPT-AS-VNVIETNAMPOSTSANDTELECOMMUNICATIONSGROUPVN	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356426
Start date:	23.02.2021
Start time:	07:35:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Request for Quotation.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:	20
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.phis.troj.spyw.evad.winEXE@9/6@0/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 78.9% (good quality ratio 62.7%) • Quality average: 62.9% • Quality standard deviation: 39.3%
HCA Information:	• Successful, ratio: 89% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, UsoClient.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing disassembly code. • Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
07:36:03	API Interceptor	1081x Sleep call for process: Request for Quotation.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
103.89.88.238	quote.exe	Get hash	malicious	Browse	
	Quote.exe	Get hash	malicious	Browse	
	Quotation Request.exe	Get hash	malicious	Browse	
	payment.exe	Get hash	malicious	Browse	
	Quotation(6656).exe	Get hash	malicious	Browse	
	swift copy.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
VNPT-AS-VNVIETNAMPOSTSANDTELECOMMUNICATIONSGROUPVN	#U007einvoice#U007eSC00978656.xlsx	Get hash	malicious	Browse	• 103.99.1.145
	quote.exe	Get hash	malicious	Browse	• 103.89.88.238
	Our New Order Feb 22 2021 at 2.30_PVV440_PDF.exe	Get hash	malicious	Browse	• 103.114.107.184

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	RFQ Manual Supersucker en Espaol.xlsx	Get hash	malicious	Browse	• 103.141.138.128
	quotation10204168.dox.xlsx	Get hash	malicious	Browse	• 103.140.251.164
	notice of arrival.xlsx	Get hash	malicious	Browse	• 103.147.184.10
	22-2-2021 .xlsx	Get hash	malicious	Browse	• 103.141.138.118
	Shipping_Document.xlsx	Get hash	malicious	Browse	• 103.141.138.119
	Remittance copy.xlsx	Get hash	malicious	Browse	• 103.99.1.145
	CI + PL.xlsx	Get hash	malicious	Browse	• 103.141.138.121
	RFQ_Enquiry_0002379_.xlsx	Get hash	malicious	Browse	• 103.141.138.117
	purchase order.exe	Get hash	malicious	Browse	• 103.151.124.64
	IMAGE21200021118921000.exe	Get hash	malicious	Browse	• 103.151.123.132
	MV TEAL BULKERS.xlsx	Get hash	malicious	Browse	• 103.141.138.120
	ForeignRemittance_20210219_USD.xlsx	Get hash	malicious	Browse	• 103.147.184.10
	HBL VRNA00872.xlsx	Get hash	malicious	Browse	• 103.125.191.182
	statement.xlsx	Get hash	malicious	Browse	• 103.99.1.149
	MV SEASPAN EMERALD II.xlsx	Get hash	malicious	Browse	• 103.141.138.121
	_Doc_Shipment_330393_.xlsx	Get hash	malicious	Browse	• 103.141.138.117
	HBL VRN0924588.xlsx	Get hash	malicious	Browse	• 103.140.251.164

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\nsc77A8.tmp\System.dll	#U007einvoice#U007eSC00978656.xlsx	Get hash	malicious	Browse	
	Purchase Order___pdf _____.exe	Get hash	malicious	Browse	
	quote.exe	Get hash	malicious	Browse	
	Order83930.exe	Get hash	malicious	Browse	
	Invoice 6500TH21Y5674.exe	Get hash	malicious	Browse	
	Invoice 6500TH21Y5674.exe	Get hash	malicious	Browse	
	GPP.exe	Get hash	malicious	Browse	
	OrderSuppliesQuote0817916.exe	Get hash	malicious	Browse	
	ACCOUNT DETAILS.exe	Get hash	malicious	Browse	
	Quotation.com.exe	Get hash	malicious	Browse	
	Unterlagen PDF.exe	Get hash	malicious	Browse	
	QuotationInvoices.exe	Get hash	malicious	Browse	
	PO.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.TrojanSpy.MSIL.Agent.22886.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.FileRepMalware.24882.exe	Get hash	malicious	Browse	
	PDF_doc.exe	Get hash	malicious	Browse	
	09000000000000.jar	Get hash	malicious	Browse	
	quotation10204168.dox.xlsx	Get hash	malicious	Browse	
	notice of arrivalpdf.exe	Get hash	malicious	Browse	
	R5BNZ68i0f.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Temp\aqx5kku77.dll

Process:	C:\Users\user\Desktop\Request for Quotation.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	21504

C:\Users\user\AppData\Local\Temp\aqx5kku77.dll	
Entropy (8bit):	7.408207836374235
Encrypted:	false
SSDEEP:	384:OOCV5PqjbmDbusFpGZO7gOG4/yr5RdXF82WNbx/9gJTALB+deFk+riSlxV:O1zPmC/uaG46Rq/9gJALB4+t
MD5:	D58BF216C5DA94776AACA50132847A49
SHA1:	4444CBB553381C13409707562CED76CE6525879E
SHA-256:	04870A6CB3CF7B291FA4BB2378B3AEAE921E0C5D220A8420C327D779B7FD2180
SHA-512:	19E7F5EF052AE1195A01A993FC3B2E5DD464299A5E666DAA18132FE7F6264A9F354136CC2F3C90D0B20E7FCDC4BF9F8F55C2D63CB74DF0C6DA6F1FB1610AF4A
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 6%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....e.N.e.N.e.N.e.N.e.NI..N.e.N..cN.e.N..gN.e.N..dN.e.N..aN.e .NRich.e.N.....PE..L....84`.....!.....L..... .....@.....P$..I... .....d..... ....code..... ....rdata..... .....@..@.data....@...0...B.....@....rsrc.....P.....@..@.reloc.....R.....@..B..... ....

C:\Users\user\AppData\Local\Temp\hbieekorpghvpuxbpehxjpq	
Process:	C:\Users\user\Desktop\Request for Quotation.exe
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	..

C:\Users\user\AppData\Local\Temp\nsc77A8.tmp\System.dll	
Process:	C:\Users\user\Desktop\Request for Quotation.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	5.855045165595541
Encrypted:	false
SSDEEP:	192:xPtkiQJr7V9r3HcU17S8g1w5xzWxy6j2V7i77blbTc4v:g7VpNo8gmOyRsVc4
MD5:	FCCFF8CB7A1067E23FD2E2B63971A8E1
SHA1:	30E2A9E137C1223A78A0F7B0BF96A1C361976D91
SHA-256:	6FCEA34C8666B06368379C6C402B5321202C11B00889401C743FB96C516C679E
SHA-512:	F4335E84E6F8D70E462A22F1C93D2998673A7616C868177CAC3E8784A3BE1D7D0BB96F2583FA0ED82F4F2B6B8F5D9B33521C279A42E055D80A94B4F3F1791E0C
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: #U007einvoice#U007eSC00978656.xlsx, Detection: malicious, Browse • Filename: Purchase Order___pdf _____.exe, Detection: malicious, Browse • Filename: quote.exe, Detection: malicious, Browse • Filename: Order83930.exe, Detection: malicious, Browse • Filename: Invoice 6500TH21Y5674.exe, Detection: malicious, Browse • Filename: Invoice 6500TH21Y5674.exe, Detection: malicious, Browse • Filename: GPP.exe, Detection: malicious, Browse • Filename: OrderSuppliesQuote0817916.exe, Detection: malicious, Browse • Filename: ACCOUNT DETAILS.exe, Detection: malicious, Browse • Filename: Quotation.com.exe, Detection: malicious, Browse • Filename: Unterlagen PDF.exe, Detection: malicious, Browse • Filename: QuotationInvoices.exe, Detection: malicious, Browse • Filename: PO.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.TrojanSpy.MSIL.Agent.22886.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.FileRepMalware.24882.exe, Detection: malicious, Browse • Filename: PDF_doc.exe, Detection: malicious, Browse • Filename: 09000000000000.jar, Detection: malicious, Browse • Filename: quotation10204168.dox.xlsx, Detection: malicious, Browse • Filename: notice of arrivalpdf.exe, Detection: malicious, Browse • Filename: R5BNZ68i0f.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Temp\nsc77A8.tmp\System.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....ir*.-.D.-.D.-.D...J.*.D.-.E.>.D.....*.D.y0t.).D.N1n.,.D..3@.,.D.Rich-.D. .....PE..L....$_.....!.... .....!).....0.....`.....@.....2.....0..P.....P.....0..X..... .....text..... ..... ..`.rdata..c....0.....$.....@..@.data...h....@.....(.....@....reloc..|....P.....*.....@..B..... ....

C:\Users\user\AppData\Local\Temp\nsh7778.tmp	
Process:	C:\Users\user\Desktop\Request for Quotation.exe
File Type:	data
Category:	dropped
Size (bytes):	167858
Entropy (8bit):	7.8527235413443
Encrypted:	false
SSDEEP:	3072:f/h6lq6XCc3XMkVOx0E/fhZA1lVN1189+pvOCrEfAWUWISphqya8DJNt:f2XCcH9Oe2TA33k+B3rgUWISpmMt
MD5:	9DACD2D5556A613412125B915ACC0A25
SHA1:	E57BA62C9D50A89174C1666F095DEB590B2D4F7B
SHA-256:	E44512128A5ED7778937E92B409D600C2889EE1C6D47582423C46DC411D2F2F2
SHA-512:	04ECBB17A1F333DD33DFCD7F1EFCA692B3787A6D8470C1BFFC70A263BA18E3E3F8437F7AA267407CE03A7004B92E8BB0555F3CB65BFACB664A5A096C70455A 75
Malicious:	false
Reputation:	low
Preview:	.....,.....$..... .....J.....j..... ....

C:\Users\user\AppData\Local\Temp\oqhczwm.b	
Process:	C:\Users\user\Desktop\Request for Quotation.exe
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	**7.998518254143225**
Encrypted:	**true**
SSDEEP:	3072:Pc3XMkVOx0E/fhZA1lVN1189+pvOCrEfAWUWISphqya8DI:PcH9Oe2TA33k+B3rgUWISpmx
MD5:	E5F20C3168A73483F3A1619FB349F0D2
SHA1:	92F885A7E1F271335CC4231BF0D4E4F76EA34A62
SHA-256:	347D68209F4E393B9977D0C593727388C34EEE54787A3F77E7F13E39005B616C
SHA-512:	40E42444B382D6F666A8EFAE9EF6635E8E81DD1EEBAF27F4B0DB9C5675C837EAA50AE0B7105AC75103A719563ECA7FF267E3F23DAE0D960465EFC884DECDB1 0F
Malicious:	false
Reputation:	low
Preview:	.?E....o9.s.E....;.J..L6..S4. ..vp..;.0.....GR.:.tiU.k..i...~.....{..@.XE.....`.?U*{..-.N.....Zjpj.....- Z..tPm..zb...D.A../.%`..$(X#!{.S...E...-.....\_..$....?..*.{ul.)..``.:.....p.....2..:S..l.$.. ...h...85.>"..+.n....E..:LG..a"..h..<...!q.....e"..mgP..?..{.....xr,.....46.k..x....QE..kN.f...kA.;..b..r.P...y....><..k..#.H.7A.g.]..k.5@..G...OJ..bk..qQk.....2..^.T=..jl...j..H.w1.(.<..R.v.. {5.yl~.4o...9._~.P.....)....0.ex...gx]x..s>.....}...?._.....f...B}.@..K=...,.kF..CK....n.v.r)..z(o(G0...U..)Y...NE..M..c.....P.....O..#.0ec..ODK.....d.t...0.A./-...T..f.s...*..^.....W..T.. ..,?...WS..)..h.h..@\|8><$....L?0L....h.(..\n...i.&.....p...,.$..e.....\.....M...%....mXUz1d....<.....@.....T....Y,d.-d.5.....#V...3.N.!....g.\..)f=.J.l..-...f.....-*..7..\|...hPc3.R.b.xJ..X{g... cG..X.o..L7..X.F...r0.....4.~x....c.je)OvSNGK...w\|...#z.4.....9.".9.....JcP/.'S]...R..i.....ro\..rh.+..A.,Sl.....Nh#.$..h@3..4.c

C:\Users\user\AppData\Roaming\excel\logs.dat	
Process:	C:\Users\user\Desktop\Request for Quotation.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	74
Entropy (8bit):	4.673971569609487
Encrypted:	false
SSDEEP:	3:ttUHS4fWT9t8rA4RXMRPHv31aeo:tmFfbXqdHv3IP
MD5:	0073BB44B36B49586AF77FC9862DC123
SHA1:	E58E4867FEE6C88C8D161AAE1250C01D4066EE95
SHA-256:	6CFC8BC39002CDFF5F6CD53EB3E783EC612D3548E37270C04A84132180C8A60C
SHA-512:	1BC4F93CB13F9C9345FEA4479490BF9DD9F0B629C86199D773F312927A909C3F4EA76B9A1CF39AFE349B456E8AFA35628351AC8D485D420E7365AFF1EA170C9I
Malicious:	false
Reputation:	low
Preview:	..[2021/02/23 07:36:03 Offline Keylogger Started]....[Program Manager]..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.415276485535663
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Request for Quotation.exe
File size:	246893
MD5:	ae4bd6c5a7eaa50704d43d6054fc5dbd
SHA1:	ab597cfc0433999f2032c56fe2c9e17081bcab46
SHA256:	8e51354c8b2f461ab0cfb92409bc45bf4e06ae244080513e2d6224dc22f47771
SHA512:	b7b0b772a5e9e969f3d5389c1c12f053a5b3a7aa774fffa3a2dac8903df09a2a6b9d242a4f1fb63602d7581226ec647be44139d27aacd82dbec6242bcd3bab43
SSDEEP:	6144:M11Q0SiA9hfCmuW9e2TA3Hk+B3rUUWISpATi:zilfCmuWE20kMUISpAO
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1)..PG..PG..PG.*_...PG..PF.IPG.*_...PG..sw..PG..VA..PG.Rich.PG.....PE..L..._.$_.....f...L.....4.....@

File Icon

Icon Hash:	f0f06094c36ee8c2

Static PE Info

General

Entrypoint:	0x403486
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5F24D75F [Sat Aug 1 02:45:51 2020 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:	ea4e67a31ace1a72683a99b80cf37830

Entrypoint Preview

Instruction
sub esp, 00000184h
push ebx
push esi
push edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 0040A130h

Instruction
mov dword ptr [esp+20h], ebx
mov byte ptr [esp+14h], 00000020h
call dword ptr [004080B0h]
call dword ptr [004080C0h]
and eax, BFFFFFFFh
cmp ax, 00000006h
mov dword ptr [0042F44Ch], eax
je 00007F0B98DA98F3h
push ebx
call 00007F0B98DACA6Eh
cmp eax, ebx
je 00007F0B98DA98E9h
push 00000C00h
call eax
mov esi, 004082A0h
push esi
call 00007F0B98DAC9EAh
push esi
call dword ptr [004080B8h]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], bl
jne 00007F0B98DA98CDh
push 0000000Bh
call 00007F0B98DACA42h
push 00000009h
call 00007F0B98DACA3Bh
push 00000007h
mov dword ptr [0042F444h], eax
call 00007F0B98DACA2Fh
cmp eax, ebx
je 00007F0B98DA98F1h
push 0000001Eh
call eax
test eax, eax
je 00007F0B98DA98E9h
or byte ptr [0042F44Fh], 00000040h
push ebp
call dword ptr [00408038h]
push ebx
call dword ptr [00408288h]
mov dword ptr [0042F518h], eax
push ebx
lea eax, dword ptr [esp+38h]
push 00000160h
push eax
push ebx
push 00429878h
call dword ptr [0040816Ch]
push 0040A1ECh

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8544	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x38000	0xdc50	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x29c	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x65ad	0x6600	False	0.675628063725	data	6.48593060343	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x1380	0x1400	False	0.4634765625	data	5.26110074066	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x25558	0x600	False	0.470052083333	data	4.21916068772	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x30000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x38000	0xdc50	0xde00	False	0.0953160191441	data	3.75209988336	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x381d8	0xd228	data		
RT_DIALOG	0x45400	0x100	data	English	United States
RT_DIALOG	0x45500	0x11c	data	English	United States
RT_DIALOG	0x4561c	0x60	data	English	United States
RT_GROUP_ICON	0x4567c	0x14	data		
RT_VERSION	0x45690	0x280	data	English	United States
RT_MANIFEST	0x45910	0x340	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExA, RegEnumKeyA, RegQueryValueExA, RegSetValueExA, RegCloseKey, RegDeleteValueA, RegDeleteKeyA, AdjustTokenPrivileges, LookupPrivilegeValueA, OpenProcessToken, SetFileSecurityA, RegOpenKeyExA, RegEnumValueA
SHELL32.dll	SHGetFileInfoA, SHFileOperationA, SHGetPathFromIDListA, ShellExecuteExA, SHGetSpecialFolderLocation, SHBrowseForFolderA
ole32.dll	IIDFromString, OleInitialize, OleUninitialize, CoCreateInstance, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	SetClipboardData, CharPrevA, CallWindowProcA, PeekMessageA, DispatchMessageA, MessageBoxIndirectA, GetDlgItemTextA, SetDlgItemTextA, GetSystemMetrics, CreatePopupMenu, AppendMenuA, TrackPopupMenu, FillRect, EmptyClipboard, LoadCursorA, GetMessagePos, CheckDlgButton, GetSysColor, SetCursor, GetWindowLongA, SetClassLongA, SetWindowPos, IsWindowEnabled, GetWindowRect, GetSystemMenu, EnableMenuItem, RegisterClassA, ScreenToClient, EndDialog, GetClassInfoA, SystemParametersInfoA, CreateWindowExA, ExitWindowsEx, DialogBoxParamA, CharNextA, SetTimer, DestroyWindow, CreateDialogParamA, SetForegroundWindow, SetWindowTextA, PostQuitMessage, SendMessageTimeoutA, ShowWindow, wsprintfA, GetDlgItem, FindWindowExA, IsWindow, GetDC, SetWindowLongA, LoadImageA, InvalidateRect, ReleaseDC, EnableWindow, BeginPaint, SendMessageA, DefWindowProcA, DrawTextA, GetClientRect, EndPaint, IsWindowVisible, CloseClipboard, OpenClipboard
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectA, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetProcAddress, GetSystemDirectoryA, WideCharToMultiByte, MoveFileExA, GetTempFileNameA, RemoveDirectoryA, WriteFile, CreateDirectoryA, GetLastError, CreateProcessA, GlobalLock, GlobalUnlock, CreateThread, lstrcpynA, SetErrorMode, GetDiskFreeSpaceA, lstrlenA, GetCommandLineA, GetVersion, GetWindowsDirectoryA, SetEnvironmentVariableA, GetTempPathA, CopyFileA, GetCurrentProcess, ExitProcess, GetModuleFileNameA, GetFileSize, ReadFile, GetTickCount, Sleep, CreateFileA, GetFileAttributesA, SetCurrentDirectoryA, SetFileAttributesA, GetFullPathNameA, GetShortPathNameA, MoveFileA, CompareFileTime, SetFileTime, SearchPathA, lstrcmpiA, lstrcmpA, CloseHandle, GlobalFree, GlobalAlloc, ExpandEnvironmentStringsA, LoadLibraryExA, FreeLibrary, lstrcpyA, lstrcatA, FindClose, MultiByteToWideChar, WritePrivateProfileStringA, GetPrivateProfileStringA, SetFilePointer, GetModuleHandleA, FindNextFileA, FindFirstFileA, DeleteFileA, MulDiv

Version Infos

Description	Data

Description	Data
LegalCopyright	Copyright adroit
FileVersion	83.34.3.56
CompanyName	ironing
LegalTrademarks	Dagoman
Comments	diamond in the rough
ProductName	sarita devi
FileDescription	mons pubis
Translation	0x0409 0x04e4

Possible Origin

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

Network Behavior

TCP Packets

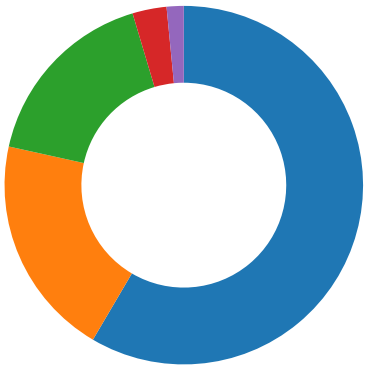
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 07:36:04.512733936 CET	49726	4299	192.168.2.4	103.89.88.238
Feb 23, 2021 07:36:04.737149000 CET	4299	49726	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:04.737268925 CET	49726	4299	192.168.2.4	103.89.88.238
Feb 23, 2021 07:36:04.739273071 CET	49726	4299	192.168.2.4	103.89.88.238
Feb 23, 2021 07:36:05.015842915 CET	4299	49726	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:05.016155958 CET	4299	49726	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:05.020406008 CET	49726	4299	192.168.2.4	103.89.88.238
Feb 23, 2021 07:36:05.248426914 CET	4299	49726	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:05.256908894 CET	49728	4299	192.168.2.4	103.89.88.238
Feb 23, 2021 07:36:05.296231031 CET	49726	4299	192.168.2.4	103.89.88.238
Feb 23, 2021 07:36:05.512660980 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:05.513061047 CET	49728	4299	192.168.2.4	103.89.88.238
Feb 23, 2021 07:36:05.513075113 CET	49728	4299	192.168.2.4	103.89.88.238
Feb 23, 2021 07:36:05.784974098 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:05.785022020 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:05.785065889 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:05.785105944 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:05.785306931 CET	49728	4299	192.168.2.4	103.89.88.238
Feb 23, 2021 07:36:05.785340071 CET	49728	4299	192.168.2.4	103.89.88.238
Feb 23, 2021 07:36:06.035861015 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.035887957 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.035904884 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.035921097 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.035942078 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.035959959 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.035964966 CET	49728	4299	192.168.2.4	103.89.88.238
Feb 23, 2021 07:36:06.035975933 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.035993099 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.036060095 CET	49728	4299	192.168.2.4	103.89.88.238
Feb 23, 2021 07:36:06.282720089 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.282752037 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.282772064 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.282793045 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.282813072 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.282830000 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.282845020 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.282855034 CET	49728	4299	192.168.2.4	103.89.88.238
Feb 23, 2021 07:36:06.282870054 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.282882929 CET	49728	4299	192.168.2.4	103.89.88.238

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 07:36:06.282892942 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.282912970 CET	49728	4299	192.168.2.4	103.89.88.238
Feb 23, 2021 07:36:06.282913923 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.282936096 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.282953024 CET	49728	4299	192.168.2.4	103.89.88.238
Feb 23, 2021 07:36:06.282958031 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.282979012 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.283000946 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.283004045 CET	49728	4299	192.168.2.4	103.89.88.238
Feb 23, 2021 07:36:06.283046007 CET	49728	4299	192.168.2.4	103.89.88.238
Feb 23, 2021 07:36:06.519969940 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.520035028 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.520073891 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.520106077 CET	49728	4299	192.168.2.4	103.89.88.238
Feb 23, 2021 07:36:06.520113945 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.520152092 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.520163059 CET	49728	4299	192.168.2.4	103.89.88.238
Feb 23, 2021 07:36:06.520189047 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.520229101 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.520251989 CET	49728	4299	192.168.2.4	103.89.88.238
Feb 23, 2021 07:36:06.520267963 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.520314932 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.520358086 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.520363092 CET	49728	4299	192.168.2.4	103.89.88.238
Feb 23, 2021 07:36:06.520395994 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.520405054 CET	49728	4299	192.168.2.4	103.89.88.238
Feb 23, 2021 07:36:06.520433903 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.520473957 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.520487070 CET	49728	4299	192.168.2.4	103.89.88.238
Feb 23, 2021 07:36:06.520514011 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.520553112 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.520579100 CET	49728	4299	192.168.2.4	103.89.88.238
Feb 23, 2021 07:36:06.520589113 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.520632982 CET	49728	4299	192.168.2.4	103.89.88.238
Feb 23, 2021 07:36:06.520637035 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.520678997 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.520715952 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.520726919 CET	49728	4299	192.168.2.4	103.89.88.238
Feb 23, 2021 07:36:06.520755053 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.520792007 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.520802975 CET	49728	4299	192.168.2.4	103.89.88.238
Feb 23, 2021 07:36:06.520828009 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.520869017 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.520874977 CET	49728	4299	192.168.2.4	103.89.88.238
Feb 23, 2021 07:36:06.520905972 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.520953894 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.520961046 CET	49728	4299	192.168.2.4	103.89.88.238
Feb 23, 2021 07:36:06.520996094 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.521034002 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.521044016 CET	49728	4299	192.168.2.4	103.89.88.238
Feb 23, 2021 07:36:06.521074057 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.521131039 CET	49728	4299	192.168.2.4	103.89.88.238
Feb 23, 2021 07:36:06.763292074 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.763318062 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.763334990 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.763353109 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.763369083 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.763390064 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.763407946 CET	4299	49728	103.89.88.238	192.168.2.4
Feb 23, 2021 07:36:06.763416052 CET	49728	4299	192.168.2.4	103.89.88.238
Feb 23, 2021 07:36:06.763425112 CET	4299	49728	103.89.88.238	192.168.2.4

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: Request for Quotation.exe PID: 7164 Parent PID: 5892

General

Start time:	07:36:00
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\Request for Quotation.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Request for Quotation.exe'
Imagebase:	0x400000
File size:	246893 bytes
MD5 hash:	AE4BD6C5A7EAA50704D43D6054FC5DBD
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: 00000000.00000002.644079874.0000000002A50000.00000004.00000001.sdmp, Author: Joe Security • Rule: Remcos_1, Description: Remcos Payload, Source: 00000000.00000002.644079874.0000000002A50000.00000004.00000001.sdmp, Author: kevoreilly • Rule: REMCOS_RAT_variants, Description: unknown, Source: 00000000.00000002.644079874.0000000002A50000.00000004.00000001.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C3	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsh7777.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E49	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\nsh7778.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E49	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C3	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C3	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C3	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C3	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C3	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\aqx5kku77.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E12	CreateFileA
C:\Users\user\AppData\Local\Temp\oqhczwm.b	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E12	CreateFileA
C:\Users\user\AppData\Local\Temp\nsc77A8.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E49	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C3	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C3	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C3	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C3	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4058C3	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsc77A8.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405883	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsc77A8.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405E12	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsh7777.tmp	success or wait	1	4036FD	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsc77A8.tmp	success or wait	1	405A44	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsh7778.tmp	unknown	22686	a2 0d 00 00 80 00 00 00 2c 01 00 00 02 00 00 00 ac 01 00 00 01 00 00 00 c4 05 00 00 24 00 00 00 b4 09 00 00 00 00 00 00 dc 0c 00 00 01 00 00 00 a2 0d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 00 ff 00 00 c6 00 00 00 f1 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	........,...................$.	success or wait	10	405EA7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\aqx5kku77.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 f1 04 c3 1d b5 65 ad 4e b5 65 ad 4e b5 65 ad 4e b5 65 ac 4e 9f 65 ad 4e 49 12 14 4e ba 65 ad 4e 92 a3 63 4e b4 65 ad 4e 92 a3 67 4e b4 65 ad 4e 92 a3 64 4e b4 65 ad 4e 92 a3 61 4e b4 65 ad 4e 52 69 63 68 b5 65 ad 4e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 b2 38 34 60 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0b 00 00 04 00 00 00 4c 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $............e.N.e.N.e.N.e.N.e .NI..N.e.N..cN.e.N..gN.e.N. .dN .e.N..aN.e.NRich.e.N......... .......PE..L....84`...........! ....L.....	success or wait	2	405EA7	WriteFile
C:\Users\user\AppData\Local\Temp\oqhczwm.b	unknown	16384	99 3f 45 14 02 89 e3 6f 39 90 73 bd 45 bc 1b 97 d3 3b cc 4a e7 f4 4c 36 f8 de 53 34 0f 20 f8 87 76 70 cb b8 bc 3b 04 30 92 e6 c9 dd dc 47 52 9a 3a d7 74 69 55 9e 6b a5 dd 69 d8 d2 fa 7e 80 9f 0a 10 c6 7b 13 ff 40 0b 58 45 8e ae 06 f3 fb 60 dd 3f 55 2a 7b 16 9e 2d 83 4e d3 84 f5 ec b2 81 8b 8d ad eb 5a 6a 70 6a 99 0f 98 f9 d8 8a 2d 20 5a ee f7 74 50 6d 84 10 7a 62 1f 09 8c 44 b9 41 97 b2 2f 8c 25 60 a0 96 24 28 58 23 21 7b c2 9d 53 8c 80 b5 45 c0 9d 07 2d d7 15 b8 9d 8f 1f 9d c4 ad 0a 1b 5f cf c5 24 f8 df ad d3 c8 3f eb ea a7 a4 2a ea 7b 75 6c e6 29 d8 ab ed 60 60 11 3a 83 13 b9 91 e2 e3 da 80 08 ca b1 16 f2 9c a8 70 b3 bc ae 9f ee 32 f9 1b 3a 53 05 ea bd 6c b8 24 f1 d1 89 f8 ef 8a af 95 68 1e ab c2 38 35 c8 3e 22 ff 05 2b 0c 6e 91 b9 8e 93 45 8a 1c 3a 4c	.?E....o9.s.E....;.J..L6..S4. ..vp...;.0.....GR.:.tiU.k..i.. .~.....{..@.XE.....`.?U*{..-.N ..........Zjpj......- Z..tPm.. zb...D.A../.%`..$(X#! {..S...E...- ...._..$.....?....*. {ul.)...``.:...............p.. ...2..:S...l.$........h...85.> "..+.n....E..:L	success or wait	8	405EA7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsc77A8.tmp\System.dll	unknown	11776	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 69 72 2a 92 2d 13 44 c1 2d 13 44 c1 2d 13 44 c1 ae 0f 4a c1 2a 13 44 c1 2d 13 45 c1 3e 13 44 c1 ee 1c 19 c1 2a 13 44 c1 79 30 74 c1 29 13 44 c1 4e 31 6e c1 2c 13 44 c1 d2 33 40 c1 2c 13 44 c1 52 69 63 68 2d 13 44 c1 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 a8 d5 24 5f 00 00 00 00 00 00 00 00 e0 00 2e 21 0b 01 06 00 00 20 00 00 00 0a 00 00 00 00 00 00 21 29 00 00 00 10 00	MZ......................@...... ....!..L.!This program cannot be run in DOS mode....$.......ir*.-.D.-.D.- .D...J.*.D.- .E.>.D.....*.D.y0t.).D.N1n. ,.D..3@.,.D.Rich- .D.........PE ..L.....$_...........!..... .. ..!).....	success or wait	1	405EA7	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Request for Quotation.exe	unknown	512	success or wait	178	405E78	ReadFile
C:\Users\user\Desktop\Request for Quotation.exe	unknown	16384	success or wait	10	405E78	ReadFile
C:\Users\user\AppData\Local\Temp\nsh7778.tmp	unknown	4	success or wait	1	405E78	ReadFile
C:\Users\user\AppData\Local\Temp\nsh7778.tmp	unknown	3490	success or wait	1	4032A5	ReadFile
C:\Users\user\AppData\Local\Temp\nsh7778.tmp	unknown	4	success or wait	3	405E78	ReadFile
C:\Users\user\AppData\Local\Temp\nsh7778.tmp	unknown	16384	success or wait	11	405E78	ReadFile
C:\Users\user\AppData\Local\Temp\oqhczwm.b	unknown	131072	success or wait	1	6EEE63B5	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	6EEE3853	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	6EEE3853	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	6EEE3853	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	6EEE3853	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	6EEE3853	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	6EEE3853	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	6EEE3853	ReadFile

Analysis Process: Request for Quotation.exe PID: 612 Parent PID: 7164

General

Start time:	07:36:01
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\Request for Quotation.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Request for Quotation.exe'
Imagebase:	0x400000
File size:	246893 bytes
MD5 hash:	AE4BD6C5A7EAA50704D43D6054FC5DBD
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: 00000001.00000002.903195414.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Remcos_1, Description: Remcos Payload, Source: 00000001.00000002.903195414.0000000000400000.00000040.00000001.sdmp, Author: kevoreilly • Rule: REMCOS_RAT_variants, Description: unknown, Source: 00000001.00000002.903195414.0000000000400000.00000040.00000001.sdmp, Author: unknown • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000001.00000001.641497403.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Remcos_1, Description: Remcos Payload, Source: 00000001.00000001.641497403.0000000000400000.00000040.00020000.sdmp, Author: kevoreilly • Rule: REMCOS_RAT_variants, Description: unknown, Source: 00000001.00000001.641497403.0000000000400000.00000040.00020000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\excel	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40564C	CreateDirectoryW
C:\Users\user\AppData\Roaming\excel\logs.dat	append data or add subdirectory or create pipe instance | read attributes | synchronize	device	synchronous io non alert | non directory file	success or wait	2	412D99	CreateFileW
C:\Users\user\AppData\Roaming\excel	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40564C	CreateDirectoryW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\rvowfdgtdozazitngptymckjrq	success or wait	1	40B1EA	DeleteFileW
C:\Users\user\AppData\Local\Temp\hbieekorpghvpuxbpehxjpq	success or wait	1	40B1B8	DeleteFileW
C:\Users\user\AppData\Local\Temp\uptpyvrmrwrfbohrpagsxhxaawaqan	success or wait	1	40B213	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\excel\logs.dat	unknown	51	0d 0a 5b 32 30 32 31 2f 30 32 2f 32 33 20 30 37 3a 33 36 3a 30 33 20 4f 66 66 6c 69 6e 65 20 4b 65 79 6c 6f 67 67 65 72 20 53 74 61 72 74 65 64 5d 0d 0a	..[2021/02/23 07:36:03 Offline Keylogger Started]..	success or wait	2	412DCC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\rvowfdgtdozazitngptymckjrq	unknown	0	success or wait	1	412E3A	ReadFile
C:\Users\user\AppData\Local\Temp\hbieekorpghvpuxbpehxjpq	unknown	2	success or wait	1	412E3A	ReadFile
C:\Users\user\AppData\Local\Temp\uptpyvrmrwrfbohrpagsxhxaawaqan	unknown	0	success or wait	1	412E3A	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\excel-8OHAVR\	success or wait	1	40B71B	RegCreateKeyA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\excel-8OHAVR	exepath	binary	C2 09 1E E7 54 3D 24 12 66 5C F1 80 61 D3 C5 61 3C 54 4D 80 97 D0 ED AB 72 B4 14 45 14 3A A6 38 EB E5 EC CD 28 23 66 E5 1F E8 CE 7F FE 06 E8 5C 4D C5 6B C7 A3 B3 9C A9 47 3D 82 85 30 E8 6D 77 4D 8E 59 75 9B BB 0E B8 63 5F 60 DE D3 FB 27 A6 71 7E 4E 04 63 69 F5 98 43 B0 1F 17 73 F9 86 76 25 FF	success or wait	1	40B747	RegSetValueExA
HKEY_CURRENT_USER\Software\excel-8OHAVR	licence	unicode	B9D471C1FE56542636F9C270446488 23	success or wait	1	40B747	RegSetValueExA

Analysis Process: Request for Quotation.exe PID: 6188 Parent PID: 612

General

Start time:	07:36:07
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\Request for Quotation.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Request for Quotation.exe' /stext 'C:\Users\user\AppData\Local\Temp \hbieekorpghvpuxbpehxjpq'
Imagebase:	0x400000
File size:	246893 bytes
MD5 hash:	AE4BD6C5A7EAA50704D43D6054FC5DBD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\hbieekorpghvpuxbpehxjpq	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4096F4	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\hbieekorpghvpuxbpehxjpq	unknown	2	ff fe	..	success or wait	1	40A32B	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	87300	success or wait	1	40A30C	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	100	success or wait	1	417623	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	2048	success or wait	1	417623	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	2048	success or wait	1	417623	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	2048	success or wait	1	417623	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	16	success or wait	1	417623	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	87300	success or wait	1	40A30C	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	100	success or wait	1	417623	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	2048	success or wait	1	417623	ReadFile

Analysis Process: Request for Quotation.exe PID: 6424 Parent PID: 612

General

Start time:	07:36:07
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\Request for Quotation.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Request for Quotation.exe' /stext 'C:\Users\user\AppData\Local\Temp\rvowfdgtdozazitngptymckjrq'
Imagebase:	0x400000
File size:	246893 bytes
MD5 hash:	AE4BD6C5A7EAA50704D43D6054FC5DBD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\rvowfdgtdozazitngptymckjrq	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4067EB	CreateFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	406EF3	ReadFile

Analysis Process: Request for Quotation.exe PID: 5692 Parent PID: 612

General

Start time:	07:36:08
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\Request for Quotation.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Request for Quotation.exe' /stext 'C:\Users\user\AppData\Local\Temp\uptpyvrmrwrfbohrpagsxhxaawaqan'
Imagebase:	0x400000
File size:	246893 bytes
MD5 hash:	AE4BD6C5A7EAA50704D43D6054FC5DBD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\uptpyvrmrwrfbohrpagsxhxaawaqan	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406AD0	CreateFileA

Disassembly

Code Analysis