

ID: 715073
Sample Name: INV NO - 609983773 60983768.exe
Cookbook: default.jbs
Time: 15:56:20
Date: 03/10/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report INV NO -609983773 60983768.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Remcos 4
Yara Signatures 5
Memory Dumps 5
Unpacked PEs 5
Sigma Signatures 6
Snort Signatures 6
Joe Sandbox Signatures 6
AV Detection 6
Networking 6
E-Banking Fraud 6
System Summary 6
HIPS / PFW / Operating System Protection Evasion 7
Stealing of Sensitive Information 7
Remote Access Functionality 7
Mitre Att&ck Matrix 7
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 9
URLs 9
Domains and IPs 10
Contacted Domains 10
Contacted URLs 10
URLs from Memory and Binaries 10
World Map of Contacted IPs 10
General Information 10
Warnings 11
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 11
ASNs 11
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\INV NO -609983773 60983768.exe.log 12
Static File Info 12
General 12
File Icon 12
Static PE Info 12
General 12
Entrypoint Preview 13
Data Directories 13
Sections 13
Resources 13
Network Behavior 13
Statistics 14
Behavior 14
System Behavior 14
Analysis Process: INV NO -609983773 60983768.exePID: 6048, Parent PID: 3320 14
General 14
File Activities 14
File Created 14
File Written 14
File Read 15
Analysis Process: RegAsm.exePID: 5168, Parent PID: 6048 15
General 15
Analysis Process: RegAsm.exePID: 6140, Parent PID: 6048 16
General 16

Copyright Joe Security LLC 2022

Analysis Process: RegAsm.exePID: 6096, Parent PID: 6048 16
General 16
Analysis Process: RegAsm.exePID: 6112, Parent PID: 6048 16
General 16
Analysis Process: RegAsm.exePID: 6116, Parent PID: 6048 16
General 16
Disassembly 17

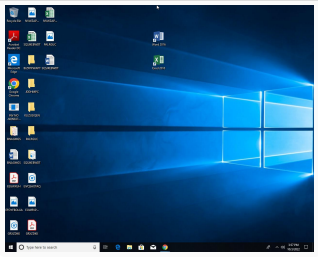
Windows Analysis Report

INV NO -609983773 60983768.exe

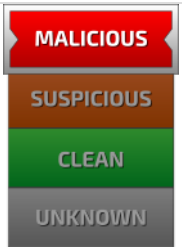
Overview

General Information

Sample Name:	INV NO -609983773 60983768.exe
Analysis ID:	715073
MD5:	4e06d9889629e7.
SHA1:	11db4a20ec8fc4…
SHA256:	341b6ff76b63e3e.
Tags:	exe
Infos:	



Detection



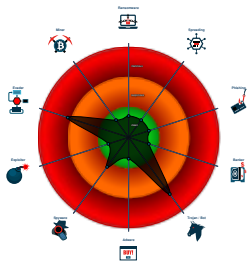
Remcos

Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected Remcos RAT
- C2 URLs / IPs found in malware con…
- .NET source code references suspic…
- Machine Learning detection for sam…
- PE file does not import any functions
- Queries the volume information (nam…
- Yara signature match
- Sample file is different than original …
- May sleep (evasive loops) to hinder…
- Uses code obfuscation techniques (…

Classification



Process Tree

- **System is w10x64**
- INV NO -609983773 60983768.exe (PID: 6048 cmdline: C:\Users\user\Desktop\INV NO -609983773 60983768.exe MD5: 4E06D9889629E7FF0FABA3B139DCC950)
  - RegAsm.exe (PID: 5168 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\RegAsm.exe MD5: 2B5D765B33C67EBA41E9F47954227BC3)
  - RegAsm.exe (PID: 6140 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\RegAsm.exe MD5: 2B5D765B33C67EBA41E9F47954227BC3)
  - RegAsm.exe (PID: 6096 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\RegAsm.exe MD5: 2B5D765B33C67EBA41E9F47954227BC3)
  - RegAsm.exe (PID: 6112 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\RegAsm.exe MD5: 2B5D765B33C67EBA41E9F47954227BC3)
  - RegAsm.exe (PID: 6116 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\RegAsm.exe MD5: 2B5D765B33C67EBA41E9F47954227BC3)
- **cleanup**

Malware Configuration

Threatname: Remcos

Copyright Joe Security LLC 2022

```
{
  "Version": "3.8.0 Pro",
  "Host:Port:Password": "172.111.234.110:5888",
  "Assigned name": "RemoteHost",
  "Connect interval": "1",
  "Install flag": "Disable",
  "Setup HKCU\\Run": "Enable",
  "Setup HKLM\\Run": "Enable",
  "Install path": "Application path",
  "Copy file": "remcos.exe",
  "Startup value": "Remcos",
  "Hide file": "Disable",
  "Mutex": "Rmc-O7I9HK",
  "Keylog flag": "0",
  "Keylog path": "Application path",
  "Keylog file": "logs.dat",
  "Keylog crypt": "Disable",
  "Hide keylog file": "Disable",
  "Screenshot flag": "Disable",
  "Screenshot time": "10",
  "Take Screenshot option": "Disable",
  "Take screenshot title": "",
  "Take screenshot time": "5",
  "Screenshot path": "AppData",
  "Screenshot file": "Screenshots",
  "Screenshot crypt": "Disable",
  "Mouse option": "Disable",
  "Delete file": "Disable",
  "Audio record time": "5"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.244325962.0000013DB3EAF000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
00000000.00000002.244325962.0000013DB3EAF000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_Remcos_b296e965	unknown	unknown	• 0x68438:$a1: Remcos restarted by watchdog! • 0x68990:$a3: %02i:%02i:%02i:%03i • 0x68d15:$a4: * Remcos v
00000000.00000002.245237358.0000013DB3F8F000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
00000000.00000002.245237358.0000013DB3F8F000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_Remcos_b296e965	unknown	unknown	• 0x1b83c0:$a1: Remcos restarted by watchdog! • 0x1b8918:$a3: %02i:%02i:%02i:%03i • 0x1b8c9d:$a4: * Remcos v
Process Memory Space: INV NO -609983773 60983768.exe PID: 6048	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	

Click to see the 1 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.INV NO -609983773 60983768.exe.13db3eafa58.3.unpack	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
0.2.INV NO -609983773 60983768.exe.13db3eafa58.3.unpack	INDICATOR_SUSPICIOUS_EXE_UACBypass_EventViewer	detects Windows exceutables potentially bypassing UAC using eventvwr.exe	ditekSHen	• 0x60100:$s1: \Classes\mscfile\shell\open\command • 0x60160:$s1: \Classes\mscfile\shell\open\command • 0x60148:$s2: eventvwr.exe
0.2.INV NO -609983773 60983768.exe.13db3eafa58.3.unpack	Windows_Trojan_Remcos_b296e965	unknown	unknown	• 0x661e0:$a1: Remcos restarted by watchdog! • 0x66738:$a3: %02i:%02i:%02i:%03i • 0x66abd:$a4: * Remcos v

Copyright Joe Security LLC 2022

Source	Rule	Description	Author	Strings
0.2.INV NO -609983773 60983768.exe.13db3eafa58.3.unpack	REMCOS_RAT_variants	unknown	unknown	• 0x611e4:$str_a1: C:\Windows\System32\cmd.exe • 0x61160:$str_a3: /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWOR • 0x61160:$str_a4: /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWOR • 0x60610:$str_a5: \AppData\Local\Google\Chrome\User Data\Default\Login Data • 0x60e48:$str_b1: CreateObject("Scripting.FileSystemObject").DeleteFile(Wscript.ScriptFullName) • 0x6020c:$str_b2: Executing file: • 0x61328:$str_b3: GetDirectListeningPort • 0x60c08:$str_b4: Set fso = CreateObject("Scripting.FileSystemObject") • 0x60e30:$str_b7: \update.vbs • 0x60234:$str_b9: Downloaded file: • 0x60220:$str_b10: Downloading file: • 0x602c4:$str_b12: Failed to upload file: • 0x612f0:$str_b13: StartForward • 0x61310:$str_b14: StopForward • 0x60dd8:$str_b15: fso.DeleteFile " • 0x60d6c:$str_b16: On Error Resume Next • 0x60e08:$str_b17: fso.DeleteFolder " • 0x602b4:$str_b18: Uploaded file: • 0x60274:$str_b19: Unable to delete: • 0x60da0:$str_b20: while fso.FileExists(" • 0x60749:$str_c0: [Firefox StoredLogins not found]
0.2.INV NO -609983773 60983768.exe.13db409f9a8.5.raw.unpack	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
Click to see the 11 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection



Multi AV Scanner detection for submitted file

Yara detected Remcos RAT

Machine Learning detection for sample

Networking



C2 URLs / IPs found in malware configuration

E-Banking Fraud



Yara detected Remcos RAT

System Summary



Malicious sample detected (through community Yara rule)

HIPS / PFW / Operating System Protection Evasion



.NET source code references suspicious native API functions

Stealing of Sensitive Information



Yara detected Remcos RAT

Remote Access Functionality

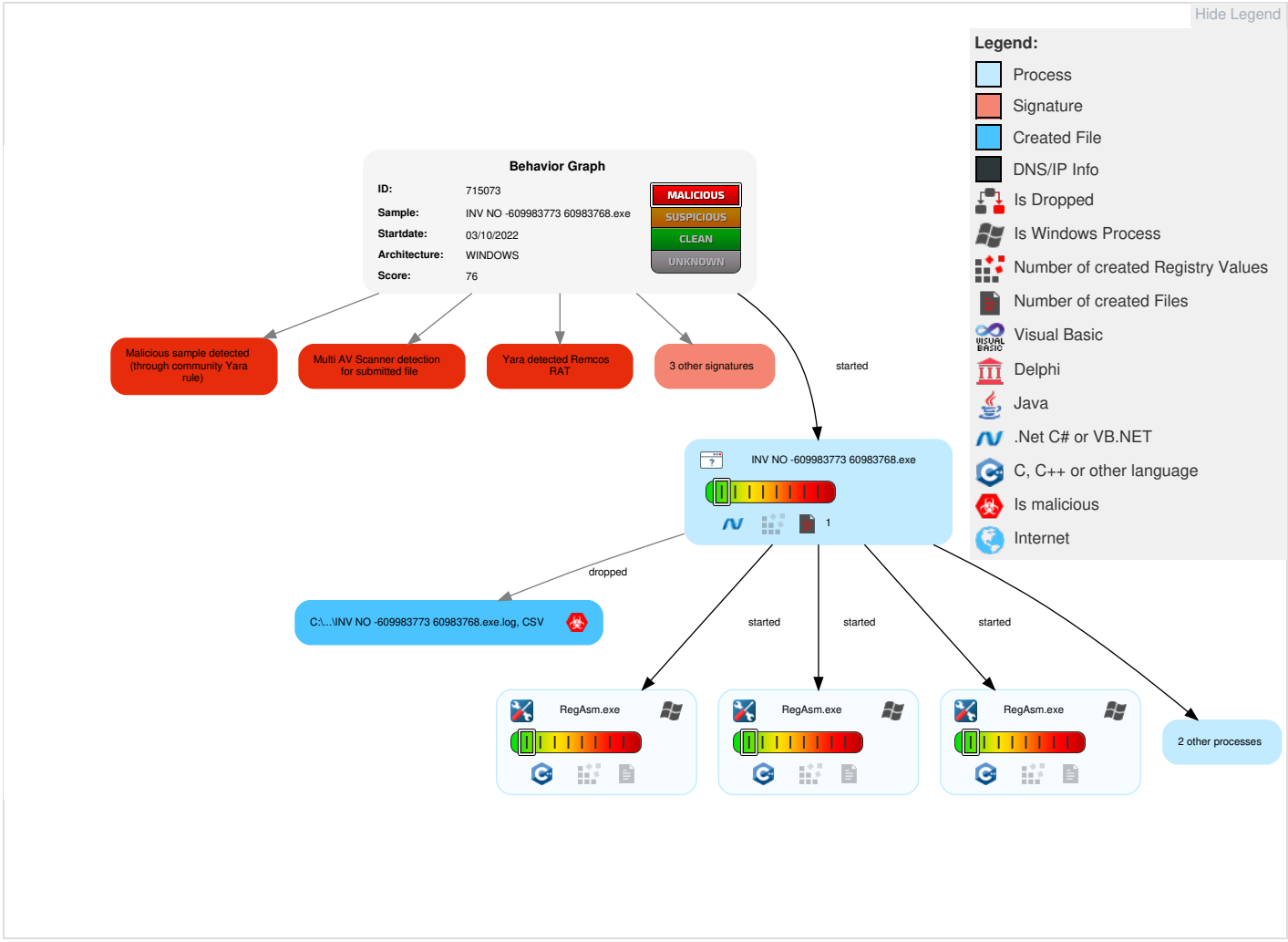


Yara detected Remcos RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Native API	Path Interception	1 1 Process Injection	1 Masquerading	OS Credential Dumping	1 Process Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Application Layer Protocol	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	2 1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	1 2 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Software Packing	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 1 Process Injection	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Obfuscated Files or Information	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

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
INV NO -609983773 60983768.exe	2%	ReversingLabs	ByteCode-MSIL.Backdoor.Remcos	
INV NO -609983773 60983768.exe	10%	Virustotal		Browse
INV NO -609983773 60983768.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://geoplugin.net/json.gp/C	0%	URL Reputation	safe	
http://https://opensource.bulkpdf.de/Whttps://opensource.bulkpdf.de/documentation	0%	Virustotal		Browse
172.111.234.110	5%	Virustotal		Browse
http://https://opensource.bulkpdf.de/documentation	0%	Avira URL Cloud	safe	
172.111.234.110	0%	Avira URL Cloud	safe	
http://https://opensource.bulkpdf.de/	0%	Avira URL Cloud	safe	
http://https://opensource.bulkpdf.de/Whttps://opensource.bulkpdf.de/documentation	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
172.111.234.110	true	• 5%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://opensource.bulkpdf.de/Whttps://opensource.bulkpdf.de/documentation	INV NO -609983773 60983768.exe	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://opensource.bulkpdf.de/documentation	INV NO -609983773 60983768.exe	false	• Avira URL Cloud: safe	unknown
http://https://opensource.bulkpdf.de/	INV NO -609983773 60983768.exe	false	• Avira URL Cloud: safe	unknown
http://fsf.org/	INV NO -609983773 60983768.exe	false		high
http://geoplugin.net/json.gp/C	INV NO -609983773 60983768.exe, 00000000.00000002.244325962.0000013DB3EAF000.00000004.00000800.00020000.00000000.sdmp, INV NO -609983773 60983768.exe, 00000000.00000002.245237358.0000013DB3F8F000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://itextpdf.com/terms-of-use/	INV NO -609983773 60983768.exe	false		high
http://www.gnu.org/licenses	INV NO -609983773 60983768.exe	false		high
http://www.gnu.org/licenses/gpl-faq.html#FontException	INV NO -609983773 60983768.exe	false		high
http://www.gnu.org/licenses/	INV NO -609983773 60983768.exe	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	715073
Start date and time:	2022-10-03 15:56:20 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	INV NO -609983773 60983768.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	6

Copyright Joe Security LLC 2022

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:	mal76.troj.evad.winEXE@11/1@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 17.9% (good quality ratio 11.2%) • Quality average: 42% • Quality standard deviation: 36.9%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Stop behavior analysis, all processes terminated

Warnings

- Excluded IPs from analysis (whitelisted): 23.50.105.163
- Excluded domains from analysis (whitelisted): fs.microsoft.com, e16604.g.akamaiedge.net, prod.fs.microsoft.com.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\INV NO -609983773 60983768.exe.log	
Process:	C:\Users\user\Desktop\INV NO -609983773 60983768.exe
File Type:	CSV text
Category:	dropped
Size (bytes):	654
Entropy (8bit):	5.374391981354885
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPTxAIOKbbDLI4MWuPOKN08JOKhap+92n4MNQpN9tv:ML9E4KrgKDE4KGKN08AKh6+84xpNT
MD5:	C8A62E39DE7A3F805D39384E8BABB1E0
SHA1:	B32B1257401F17A2D1D5D3CC1D8C1E072E3FEE31
SHA-256:	A7BC127854C5327ABD50C86000BF10586B556A5E085BB23523B07A15DD4C5383
SHA-512:	7DB2825131F5CDA6AF33A179D9F7CD0A206FF34AE50D6E66DE9E99BE2CD1CB985B88C00F0EDE72BBC4467E7E42B5DC6132403AA2EC1A0A7A6D11766C438B10C3
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll",0..3,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.V9921e851#\f2e0589ed6d670f264a5f65dd0ad000f\Microsoft.VisualBasic.ni.dll",0..

Static File Info

General

File type:	PE32+ executable (GUI) x86-64 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.355734908257647
TrID:	• Win64 Executable GUI Net Framework (217006/5) 49.88% • Win64 Executable GUI (202006/5) 46.43% • Win64 Executable (generic) (12005/4) 2.76% • Generic Win/DOS Executable (2004/3) 0.46% • DOS Executable Generic (2002/1) 0.46%
File name:	INV NO -609983773 60983768.exe
File size:	860672
MD5:	4e06d9889629e7ff0faba3b139dcc950
SHA1:	11db4a20ec8fc4a88bc5b75dc5de730e719b9f57
SHA256:	341b6ff76b63e3e74b8fd97b301462f9a6544405946271b7766c4ff4c8c28150
SHA512:	03e2bea6b7407de7ea9e62729239c7dff3766ef502d97f9855957a9686876939e8fc3592ddb0bf1737cef965090ffd28c7b689b8bd0dc225e7ad81a1654b3eba
SSDEEP:	12288:iEP6d1Ttnv8aidSXH1tRBme/yVaBzx1cYYymqn+7F7kBzxopLsk:ie6d1pnv2dE1tRke/e61Ln+eQp9
TLSH:	7305AE1037966249CC560F711932C2D947793E27BE38C21D74AE708EAF73A278723B66
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d....U:c....."...0.c..... ....@..... .....`.....`.....

File Icon



Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x400000
Entrypoint Section:	
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x633A5515 [Mon Oct 3 03:20:53 2022 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:	

Entrypoint Preview

Instruction
dec ebp
pop edx
nop
add byte ptr [ebx], al
add byte ptr [eax], al
add byte ptr [eax+eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xd4000	0x388	.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	
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	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2000	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xd1a63	0xd1c00	False	0.6498947780095352	data	7.3605775158149305	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xd4000	0x388	0x400	False	0.3857421875	data	2.94473135225856	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

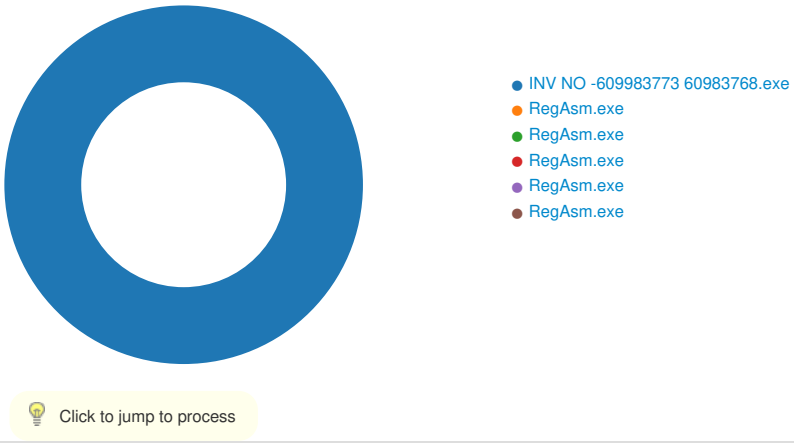
Name	RVA	Size	Type	Language	Country
RT_VERSION	0xd4058	0x330	data		

Network Behavior

No network behavior found

Statistics

Behavior



System Behavior

Analysis Process: INV NO -609983773 60983768.exe PID: 6048, Parent PID: 3320

General

Target ID:	0
Start time:	15:57:14
Start date:	03/10/2022
Path:	C:\Users\user\Desktop\INV NO -609983773 60983768.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\INV NO -609983773 60983768.exe
Imagebase:	0x13da1f40000
File size:	860672 bytes
MD5 hash:	4E06D9889629E7FF0FABA3B139DCC950
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000000.00000002.244325962.0000013DB3EAF000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Remcos_b296e965, Description: unknown, Source: 00000000.00000002.244325962.0000013DB3EAF000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000000.00000002.245237358.0000013DB3F8F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Remcos_b296e965, Description: unknown, Source: 00000000.00000002.245237358.0000013DB3F8F000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\INV NO -609983773 60983768.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFE236586ED	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\INV NO-609983773 60983768.exe.log	0	654	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 36 34 5c 53 79 73 74 65 6d 5c 31 30 61 31 37 31 33 39 31 38 32 61 39 65 66 64 35 36 31 66 30 31 66 61 64 61 39 36 38 38 61 35 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30	1,"fusion","GAC",01,"WinRT","NotApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",03,"System.Core, Version=4.0.0	success or wait	1	7FFE23658769	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFE230BB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFE230BB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFE231912E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFE230C2625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFE231912E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFE231912E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.V9921e851#\f2e0589ed6d670f264a5f65dd0ad000f\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	7FFE231912E7	ReadFile

Analysis Process: RegAsm.exe PID: **5168**, Parent PID: **6048**

General

Target ID:	1
Start time:	15:57:16
Start date:	03/10/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\RegAsm.exe
Imagebase:	0x265ffed0000
File size:	64096 bytes
MD5 hash:	2B5D765B33C67EBA41E9F47954227BC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: RegAsm.exe PID: **6140**, Parent PID: **6048**

General	
Target ID:	2
Start time:	15:57:16
Start date:	03/10/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\RegAsm.exe
Imagebase:	0x14bb8e80000
File size:	64096 bytes
MD5 hash:	2B5D765B33C67EBA41E9F47954227BC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: RegAsm.exe PID: **6096**, Parent PID: **6048**

General	
Target ID:	3
Start time:	15:57:16
Start date:	03/10/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\RegAsm.exe
Imagebase:	0x17a583d0000
File size:	64096 bytes
MD5 hash:	2B5D765B33C67EBA41E9F47954227BC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: RegAsm.exe PID: **6112**, Parent PID: **6048**

General	
Target ID:	4
Start time:	15:57:16
Start date:	03/10/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\RegAsm.exe
Imagebase:	0x2bc03340000
File size:	64096 bytes
MD5 hash:	2B5D765B33C67EBA41E9F47954227BC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: RegAsm.exe PID: **6116**, Parent PID: **6048**

General	
Target ID:	5
Start time:	15:57:17

Start date:	03/10/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\RegAsm.exe
Imagebase:	0x24bc9810000
File size:	64096 bytes
MD5 hash:	2B5D765B33C67EBA41E9F47954227BC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Disassembly

No disassembly