ID: 626030
Sample Name: 63.exe
Cookbook: default.jbs
Time: 14:03:35
Date: 13/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report 63.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Telegram RAT 4
Threatname: Agenttesla 4
Yara Signatures 4
Memory Dumps 4
Unpacked PEs 5
Sigma Signatures 5
Snort Signatures 5
Joe Sandbox Signatures 5
AV Detection 5
Networking 5
System Summary 6
Malware Analysis System Evasion 6
HIPS / PFW / Operating System Protection Evasion 6
Stealing of Sensitive Information 6
Remote Access Functionality 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 9
URLs 9
Domains and IPs 9
Contacted Domains 9
URLs from Memory and Binaries 9
World Map of Contacted IPs 9
General Information 10
Warnings 10
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 11
ASNs 11
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\63.exe.log 11
C:\Users\user\AppData\Local\Temp\851a6346-8539-40b9-b694-d1d5343c092e\o.dll 11
C:\Users\user\AppData\Local\Temp\RegAsm.exe 12
Static File Info 12
General 12
File Icon 12
Static PE Info 12
General 12
Entrypoint Preview 13
Data Directories 14
Sections 15
Resources 15
Imports 15
Version Infos 15
Network Behavior 15
Statistics 15
Behavior 16
System Behavior 16
Analysis Process: 63.exePID: 6408, Parent PID: 1832 16
General 16
File Activities 16
File Created 16
File Written 17
File Read 18
Analysis Process: RegAsm.exePID: 5680, Parent PID: 6408 18
General 18

File Activities 19
File Created 19
File Read 19
Disassembly 20

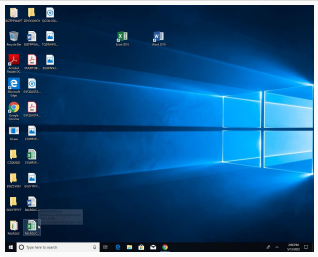
Windows Analysis Report

63.exe

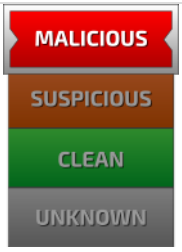
Overview

General Information

Sample Name:	63.exe
Analysis ID:	626030
MD5:	638161fea451ac..
SHA1:	0ebd57241094f5..
SHA256:	f144a51298e1e0..
Tags:	exe
Infos:	



Detection



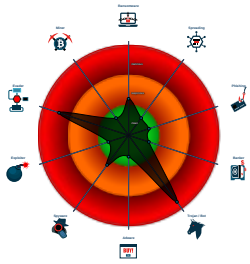
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected Telegram RAT
- Yara detected AgentTesla
- Antivirus / Scanner detection for sub…
- Writes to foreign memory regions
- Machine Learning detection for sam…
- Allocates memory in foreign process…
- Injects a PE file into a foreign proce…
- Yara detected Generic Downloader
- .NET source code contains very larg…

Classification



Process Tree

- **System is w10x64**
- 63.exe (PID: 6408 cmdline: "C:\Users\user\Desktop\63.exe" MD5: 638161FEA451AC9D2CFF99A9B9A7446C)
  - RegAsm.exe (PID: 5680 cmdline: C:\Users\user\AppData\Local\Temp\RegAsm.exe MD5: 6FD7592411112729BF6B1F2F6C34899F)
- **cleanup**

Malware Configuration

Threatname: Telegram RAT

```
{
  "C2 url": "https://api.telegram.org/bot1160330796:AAF3SAwgW-OTi9M5kDhSZUlENwhKRvFOWe8/sendMessage"
}
```

Threatname: Agenttesla

```
{
  "Exfil Mode": "Telegram",
  "Chat id": "1354205151",
  "Chat URL": "https://api.telegram.org/bot1160330796:AAF3SAwgW-OTi9M5kDhSZUlENwhKRvFOWe8/sendDocument"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000010.00000000.425108271.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000010.00000000.425108271.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000010.00000000.424683140.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000010.00000000.424683140.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000010.00000002.531353991.0000000002C51000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 13 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
16.0.RegAsm.exe.400000.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
16.0.RegAsm.exe.400000.4.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
16.0.RegAsm.exe.400000.4.unpack	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	
16.0.RegAsm.exe.400000.4.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x30013:$s1: get_kbok • 0x3092d:$s2: get_CHoo • 0x31538:$s3: set_passwordIsSet • 0x2fe29:$s4: get_enableLog • 0x3445e:$s8: torbrowser • 0x32e1d:$s10: logins • 0x326f6:$s11: credential • 0x2f254:$g1: get_Clipboard • 0x2f262:$g2: get_Keyboard • 0x2f26f:$g3: get_Password • 0x307dd:$g4: get_CtrlKeyDown • 0x307ed:$g5: get_ShiftKeyDown • 0x307fe:$g6: get_AltKeyDown
16.0.RegAsm.exe.400000.10.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 19 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Machine Learning detection for sample

Networking

Yara detected Generic Downloader

System Summary

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Malware Analysis System Evasion

Tries to detect virtualization through RDTSC time measurements

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

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

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected Telegram RAT

Yara detected AgentTesla

Remote Access Functionality

Yara detected Telegram RAT

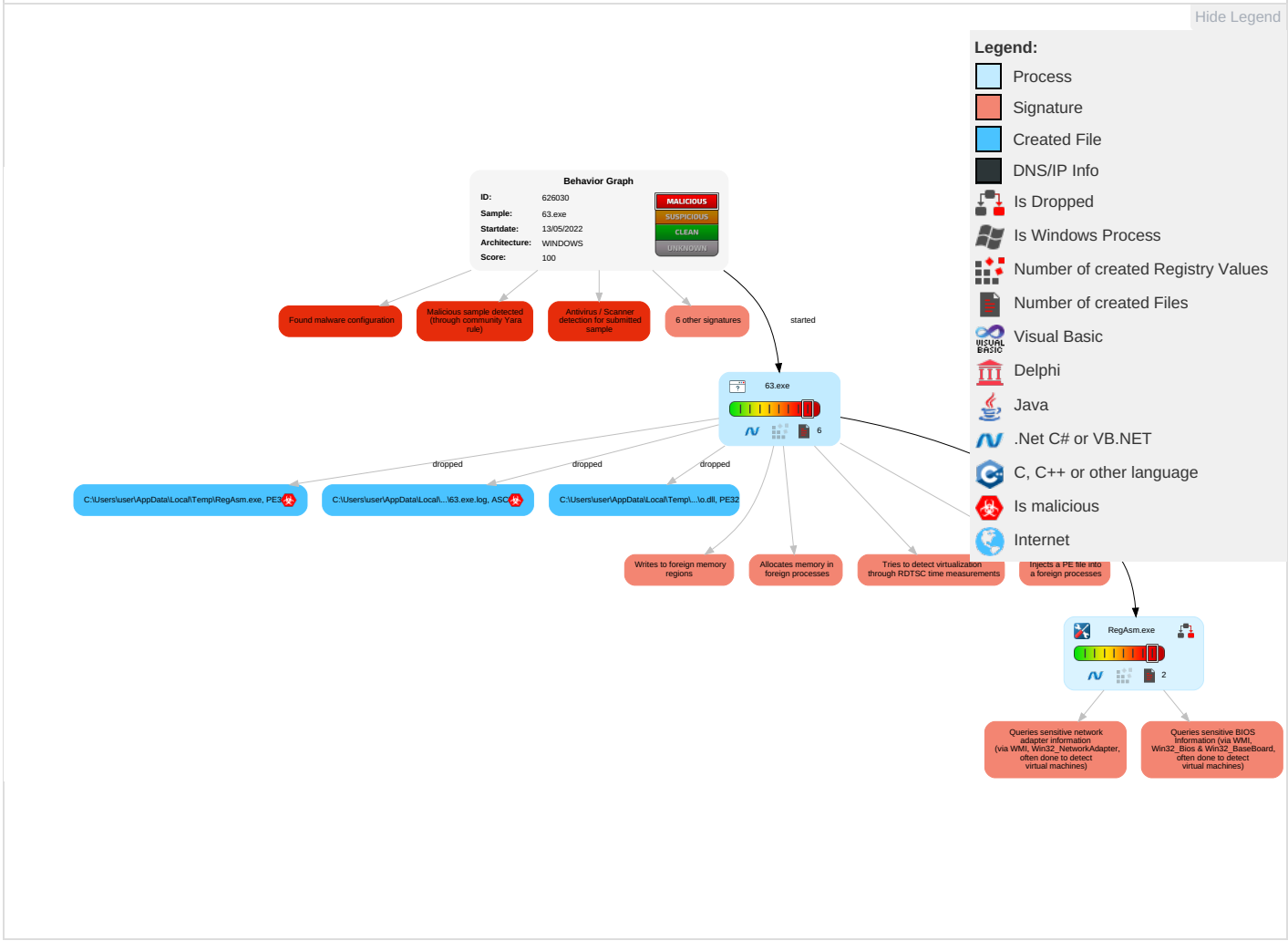
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	1 DLL Side-Loading	3 1 1 Process Injection	1 Masquerading	OS Credential Dumping	2 1 Security Software Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 Disable or Modify Tools	LSASS Memory	1 Process Discovery	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)	1 3 1 Virtualization/Sandbox Evasion	Security Account Manager	1 3 1 Virtualization/Sandbox Evasion	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)	3 1 1 Process Injection	NTDS	1 Application Window 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 Deobfuscate/Decode Files or Information	LSA Secrets	2 1 3 System Information 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
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 Software Packing	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 DLL Side-Loading	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

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
63.exe	68%	Virustotal		Browse
63.exe	65%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
63.exe	100%	Avira	HEUR/AGEN.1202787	
63.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\851a6346-8539-40b9-b694-d1d5343c092e\o.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\851a6346-8539-40b9-b694-d1d5343c092e\o.dll	2%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\RegAsm.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\RegAsm.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
16.2.RegAsm.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
16.0.RegAsm.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File

Source	Detection	Scanner	Label	Link	Download
16.0.RegAsm.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
0.0.63.exe.7c0000.0.unpack	100%	Avira	HEUR/AGEN.1202787		Download File
16.0.RegAsm.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
16.0.RegAsm.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
16.0.RegAsm.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://ZPEHvd.com	0%	Avira URL Cloud	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	RegAsm.exe, 00000010.00000002.531353991.0000000002C51000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	RegAsm.exe, 00000010.00000002.531353991.0000000002C51000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.telegram.org/bot1160330796:AAF3SAwgW-OTi9M5kDhSZUlENwhKRvFOWe8/sendDocumentdocument-----	RegAsm.exe, 00000010.00000002.531353991.0000000002C51000.00000004.00000800.00020000.00000000.sdmp	false		high
http://crl.thawte.com/ThawteTimestampingCA.crl0	o.dll.0.dr	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	RegAsm.exe, 00000010.00000002.531353991.0000000002C51000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.symauth.com/cps0(	o.dll.0.dr	false		high
http://www.symauth.com/rpa00	o.dll.0.dr	false		high
http://https://api.telegram.org/bot1160330796:AAF3SAwgW-OTi9M5kDhSZUlENwhKRvFOWe8/	RegAsm.exe, 00000010.00000000.425108271.0000000000402000.00000040.00000400.00020000.00000000.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	RegAsm.exe, 00000010.00000000.425108271.0000000000402000.00000040.00000400.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ocsp.thawte.com0	o.dll.0.dr	false	• URL Reputation: safe	unknown
http://ZPEHvd.com	RegAsm.exe, 00000010.00000002.531353991.0000000002C51000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.ipify.orgGETMozilla/5.0	RegAsm.exe, 00000010.00000002.531353991.0000000002C51000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626030
Start date and time: 13/05/202214:03:35	2022-05-13 14:03:35 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 5s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	63.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	24
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@3/3@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 0.2% (good quality ratio 0.2%) • Quality average: 64.9% • Quality standard deviation: 24%
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 • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
14:05:44	API Interceptor	87x Sleep call for process: 63.exe modified

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_32\UsageLogs\63.exe.log

Process:	C:\Users\user\Desktop\63.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1871
Entropy (8bit):	5.35489297593518
Encrypted:	false
SSDEEP:	48:MxHKXeHKlEHU0YHKhQnouHIW7HKjntHoxHhAHKzvGHKx1qHj:iqXeqm00YqhQnouRqjntIxHeqz+qxwD
MD5:	D5C4F072A3F0ED8C0079814E68AF222D
SHA1:	D2ACD6634158C5B881919FCE628716B7C3E519EB
SHA-256:	DAAD0CC8592CA67F6ACCFCB2127FC9D08F514D4165F8617E0150FE1784808FC5
SHA-512:	635C0F7EEF16AD97257E63D6489284CF529A01CAB450A6ABEFD72FBCC78F209770EA3452B8703F637DA15938251CAD5D89A8FA8CB35903F2974A96D893456FA
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_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"PresentationCore, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll",0..3,"PresentationFramework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"WindowsBase, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Wi

C:\Users\user\AppData\Local\Temp\851a6346-8539-40b9-b694-d1d5343c092e\o.dll

Process:	C:\Users\user\Desktop\63.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	96664
Entropy (8bit):	5.567444078679915
Encrypted:	false
SSDEEP:	1536:JKQ7ZLTFq31bfnHSukoY1IPtan1sBrGxEm5g:JKc/FM1bfnyNNdkrGxJg
MD5:	14FF402962AD21B78AE0B4C43CD1F194
SHA1:	F8A510EB26666E875A5BDD1CADAD40602763AD72
SHA-256:	FB9646CB956945BDC503E69645F6B5316D3826B780D3C36738D6B944E884D15B
SHA-512:	DAA7A08BF3709119A944BCE28F6EBDD24E54A22B18CD9F86A87873E958DF121A3881DCDD5E162F6B4E543238C7AEF20F657C9830DF01D4C79290F7C9A4FCC5B
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 2%
Reputation:	moderate, very likely benign file

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....jr..jr..jr..8...ir.....kr.....cr..jr..9r..8...kr.....sr.....kr....x.kr..jr..kr.....kr..Richjr.....PE..L...5 .\.....!.....F.....0.....Z.....@.....C.....0b..d.....b.....4...`A..8.....x7..@.....`..0....p..`.....text...h..... ..`.rdata.....0.....".....@..@.data.....P.....:.....@....idata.....`.....<.....@..@.didat..a....p.....J.....@....00cfg.....N.....@..@.rsrc.....P.....@..@.reloc.....X.....@..B.....

C:\Users\user\AppData\Local\Temp\RegAsm.exe

Process:	C:\Users\user\Desktop\63.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	64616
Entropy (8bit):	6.037264560032456
Encrypted:	false
SSDEEP:	768:J8XcJiMjm2ieHlPyCsSuJbn8dBhFVBSMQ6Iq8TSYDKpgLaDViRLNdr:9YMaNylPYSAb8dBnTHv8DKKaDVkX
MD5:	6FD7592411112729BF6B1F2F6C34899F
SHA1:	5E5C839726D6A43C478AB0B95DBF52136679F5EA
SHA-256:	FFE4480CCC81B061F725C54587E9D1BA96547D27FE28083305D75796F2EB3E74
SHA-512:	21EFCC9DEE3960F1A64C6D8A44871742558666BB792D77ACE91236C7DBF42A6CA77086918F363C4391D9C00904C55A952E2C18BE5FA1A67A509827BFC630070
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...xX.Z.....0.....^.... .....@.. ....`.....O.....8.....h>..... ..... .H.....text...d.... ..... ..`.rsrc...8.....@..@.reloc..... .....@..B.....@.....H.....A...p.....T.....~P...-.r...p.....(....(....s.....P...*..0..".....(.....-.r...p.rl..p(....s....z.*...0.....(....~P.....o.....*..(....*n(.....(.....%...(....*~(.....(.....%...%...(....*.(.....(.....%...%...%...(....*V.(.....}Q.....}R...*..{Q...*..{R...*...0.....(.....i.=...}S.....i.@...}T.....i.@...}U.....+m...(....o.....r]..p.o!...,..{T.....{U.....o"....+(.ra..p.o!...,..{T.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.501105460847332
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.97% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	63.exe
File size:	454656
MD5:	638161fea451ac9d2cff99a9b9a7446c
SHA1:	0ebd57241094f53ce80470edd61bfc0c8361eb2a
SHA256:	f144a51298e1e037133ad60094a271af9d65501a3ab5e41527efb6bcb56ccf58
SHA512:	2fb6f70458b40cc4d6566714873623e2ad6769fe6d5ebbf9c7fa514c9359870ea62acbd718edb96ac10c214f6b2e6f53bde59ff4b29d08866be059b7b36c3d3f
SSDEEP:	6144:DKf9ojc7FRWwDFSs5Og4HzABTOZozWIvRgDpIMRMjPjKNThg:2bRWwpSsMBHkBTkSWMjWg
TLSH:	8CA45CB73D52687DCA6E0675046A84C1FAB617CB3F908B0DB19F830C0E15A6BEB63517
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....F._..... ... .@.. .....`.....`.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x47050e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000

Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT, HIGH_ENTROPY_VA
Time Stamp:	0x5FAA4607 [Tue Nov 10 07:49:27 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [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	0x704c0	0x4b	.text

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x72000	0x4d6	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x74000	0xc	.reloc
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	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	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	0x6e514	0x6e600	False	0.685783550396	SysEx File - Moog	7.51647686445	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x72000	0x4d6	0x600	False	0.380859375	data	3.78443747428	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x74000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x720a0	0x24c	data		
RT_MANIFEST	0x722ec	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

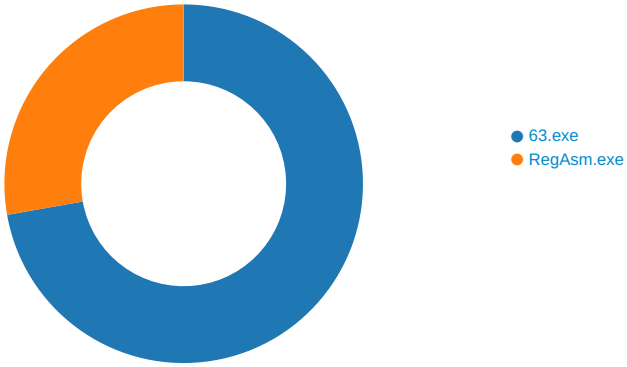
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	
Assembly Version	0.0.0.0
InternalName	DOCUMENT.exe
FileVersion	0.0.0.0
ProductVersion	0.0.0.0
FileDescription	
OriginalFilename	DOCUMENT.exe

Network Behavior

No network behavior found

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: 63.exe PID: **6408**, Parent PID: **1832**

General

Target ID:	0
Start time:	14:04:44
Start date:	13/05/2022
Path:	C:\Users\user\Desktop\63.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\63.exe"
Imagebase:	0x7c0000
File size:	454656 bytes
MD5 hash:	638161FEA451AC9D2CFF99A9B9A7446C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6DC1CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DC1CF06	unknown
C:\Users\user\AppData\Local\Temp\851a6346-8539-40b9-b694-d1d5343c092e	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C26BEFF	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\851a6346-8539-40b9-b694-d1d5343c092e\o.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C261E60	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\RegAsm.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	294BFE9	CopyFileExW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\63.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DF2C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\851a6346-8539-40b9-b694-d1d5343c092e\o.dll	0	96664	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 2e 13 fd fd 6a 72 fd fd 6a 72 fd fd 6a 72 fd fd 38 1a fd fd 69 72 fd fd 05 16 fd fd 6b 72 fd fd 05 16 fd fd 63 72 fd fd 6a 72 fd fd 39 72 fd fd 38 1a fd fd 6b 72 fd fd fd 1b fd fd 73 72 fd fd fd 1b fd fd 6b 72 fd fd fd 1b 78 fd 6b 72 fd fd 6a 72 10 fd 6b 72 fd fd fd 1b fd fd 6b 72 fd fd 52 69 63 68 6a 72 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 08	MZ@!L!This program cannot be run in DOS mode.$.jrjrjr8irkrcr jr9r8krsrkrxkrjrkrkrRichjrPEL	success or wait	1	6C261B4F	WriteFile
C:\Users\user\AppData\Local\Temp\RegAsm.exe	0	64616	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 78 58 fd 5a 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 fd 00 00 00 0c 00 00 00 00 00 00 5e fd 00 00 00 20 00 00 00 fd 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 20 01 00 00 02 00 00 fd fd 01 00 03 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELxXZ0^ @ `	success or wait	1	294BFE9	CopyFileExW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\63.exe.log	0	1871	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 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 50 72 65 73 65 6e 74 61 74 69 6f 6e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d	1,"fusion","GAC",01,"WinRT","NotApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",03,"PresentationCore, Version=	success or wait	1	6DF2C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DBF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DB503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6DB503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6DB503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DB503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6DB503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DB503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xaml\8c85184f1e0cfe359eea86373661a3f8\System.Xaml.ni.dll.aux	unknown	572	success or wait	1	6DB503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DBF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\clrjit.dll	unknown	523400	success or wait	1	72BFB80F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DB503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DB503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C261B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C261B4F	ReadFile

Analysis Process: RegAsm.exe PID: **5680**, Parent PID: **6408**

General

Target ID:	16
Start time:	14:05:59
Start date:	13/05/2022
Path:	C:\Users\user\AppData\Local\Temp\RegAsm.exe

Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\RegAsm.exe
Imagebase:	0x950000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000010.00000000.425108271.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000010.00000000.425108271.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000010.00000000.424683140.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000010.00000000.424683140.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000010.00000002.531353991.0000000002C51000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000010.00000002.531353991.0000000002C51000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000010.00000002.531353991.0000000002C51000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_AgentTeslaV3, Description: AgentTeslaV3 infostealer payload, Source: 00000010.00000002.531353991.0000000002C51000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000010.00000000.424295986.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000010.00000000.424295986.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000010.00000002.529314857.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000010.00000002.529314857.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000010.00000000.423853193.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000010.00000000.423853193.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6DC1CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DC1CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DBF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DB503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DB503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DBF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DB503DE	ReadFile

Disassembly

No disassembly