ID: 433221
Sample Name: HT210525 IV Quotation.exe
Cookbook: default.jbs
Time: 13:23:21
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

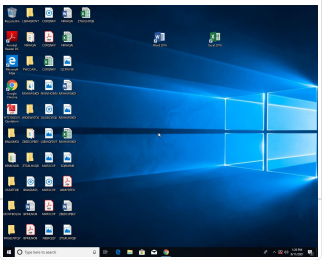
Analysis Report HT210525 IV Quotation.exe

Overview

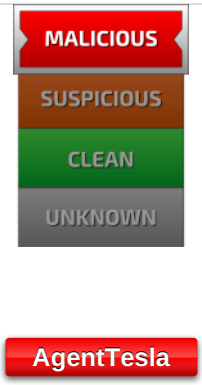
General Information

Sample Name:	HT210525 IV Quotation.exe
Analysis ID:	433221
MD5:	8ea3cb0d331f0a8.
SHA1:	4c690653287b4b..
SHA256:	e2b3c7e7061e68..
Tags:	AgentTesla exe
Infos:	

Most interesting Screenshot:



Detection

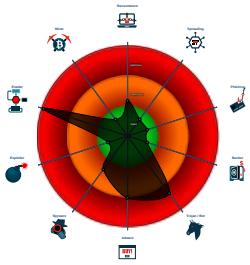


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected unpacking (changes PE se…
- Detected unpacking (overwrites its o…
- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains very larg…
- Hides that the sample has been dow…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w10x64**
- HT210525 IV Quotation.exe (PID: 6688 cmdline: 'C:\Users\user\Desktop\HT210525 IV Quotation.exe' MD5: 8EA3CB0D331F0A8414E5B2ECFCE3ABF3)
  - schtasks.exe (PID: 6588 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\KEehxxQTfXmag' /XML 'C:\Users\user\AppData\Local\Temp\tmpCED.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6576 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 6684 cmdline: {path} MD5: 2867A3817C9245F7CF518524DFD18F28)
  - RegSvcs.exe (PID: 6676 cmdline: {path} MD5: 2867A3817C9245F7CF518524DFD18F28)
- NewApp.exe (PID: 6868 cmdline: 'C:\Users\user\AppData\Roaming\NewApp\NewApp.exe' MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 3500 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- NewApp.exe (PID: 5396 cmdline: 'C:\Users\user\AppData\Roaming\NewApp\NewApp.exe' MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 5472 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "accounts@buynsell.com.pkTZaQ}N$m+6$vmail.buynsell.com.pkmaria@tradzilanilaw.co.za"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.446010791.0000000003AEA000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.446010791.0000000003AEA000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0000000D.00000002.595401687.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
0000000D.00000002.595401687.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0000000D.00000000.440537158.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 7 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.HT210525 IV Quotation.exe.3bb5278.3.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.HT210525 IV Quotation.exe.3bb5278.3.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.HT210525 IV Quotation.exe.3bb5278.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.HT210525 IV Quotation.exe.3bb5278.3.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
13.0.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 3 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview

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

Compliance:

Detected unpacking (overwrites its own PE header)

Spam, unwanted Advertisements and Ransom Demands:

Modifies the hosts file

System Summary:

.NET source code contains very large array initializations

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

Detected unpacking (changes PE section rights)

Detected unpacking (overwrites its own PE header)

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 AntiVM3

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:

Injects a PE file into a foreign processes

Modifies the hosts file

Sample uses process hollowing technique

Writes to foreign memory regions

Lowering of HIPS / PFW / Operating System Security Settings:

Modifies the hosts file

Stealing of Sensitive Information:

Yara detected AgentTesla

Yara detected AgentTesla

Remote Access Functionality:

Yara detected AgentTesla

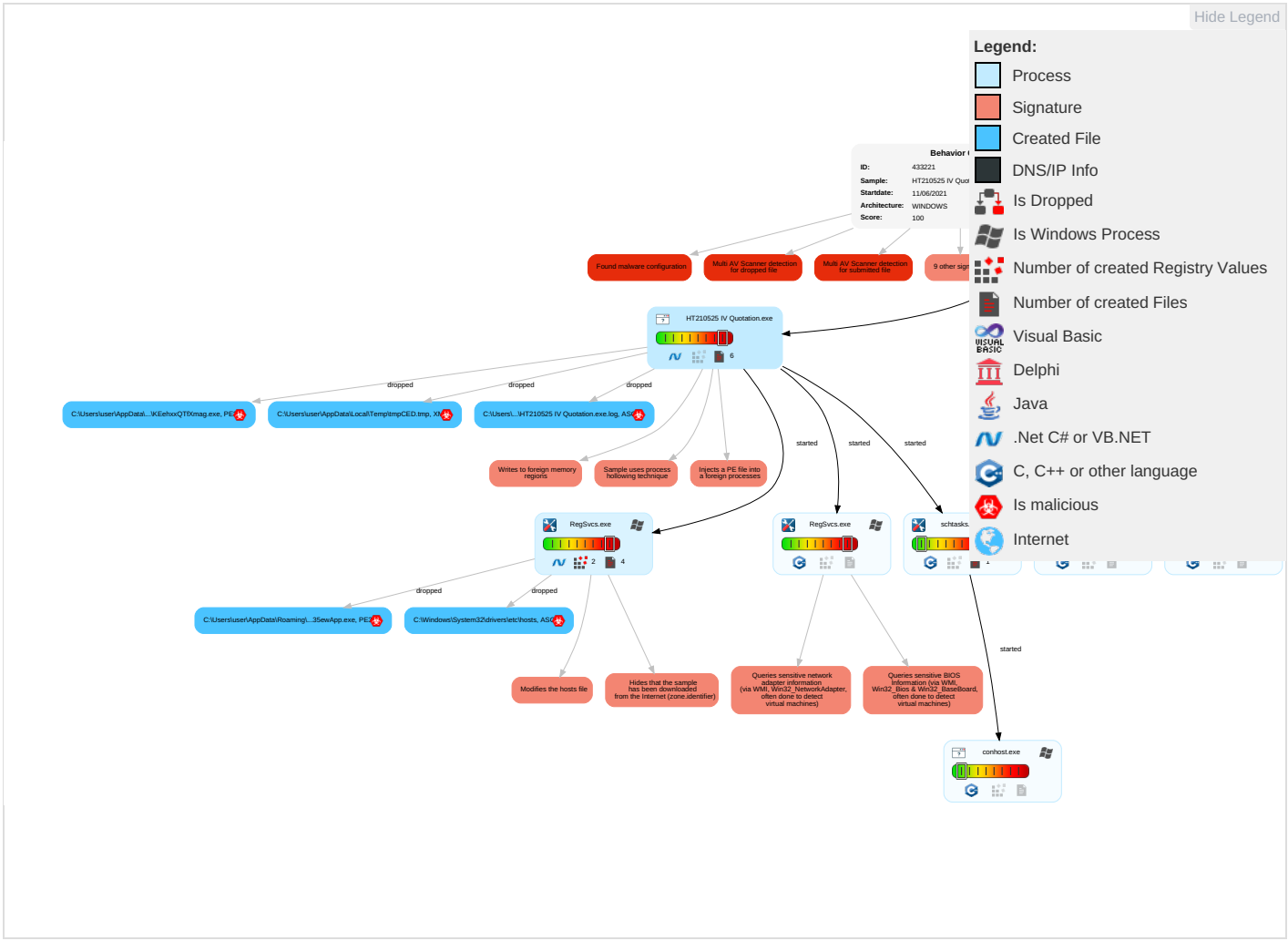
Yara detected AgentTesla

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 3 1 2	Masquerading 1	Input Capture 1	Security Software Discovery 3 2 1	Remote Services	Input Capture 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	File and Directory Permissions Modification 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Junk Data
Domain Accounts	Shared Modules 1	Logon Script (Windows)	Registry Run Keys / Startup Folder 1	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 1 5 1	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Steganography
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 1 5 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 3 1 2	LSA Secrets	Account Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Owner/User Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Hidden Files and Directories 1	DCSync	File and Directory 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	Obfuscated Files or Information 2	Proc Filesystem	System Information Discovery 1 1 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Software Packing 2 2	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols

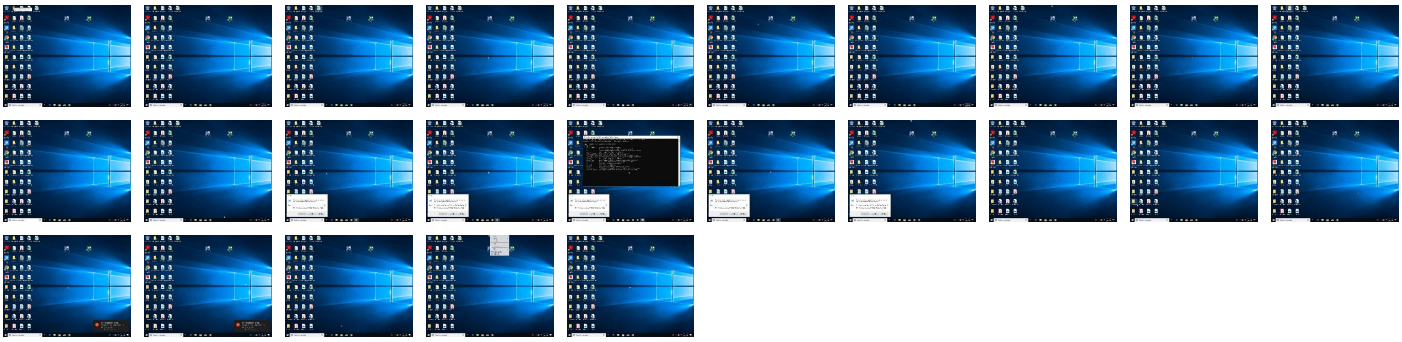
Behavior Graph



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
HT210525 IV Quotation.exe	39%	Virustotal		Browse
HT210525 IV Quotation.exe	59%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\KEehxxQTfXmag.exe	59%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\NewApp\NewApp.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Roaming\NewApp\NewApp.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
13.0.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
13.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
0.2.HT210525 IV Quotation.exe.540000.0.unpack	100%	Avira	HEUR/AGEN.1123468		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://www.founder.com.cn/cnak	0%	Avira URL Cloud	safe	
http://www.carterandcone.comn-u	0%	URL Reputation	safe	
http://www.carterandcone.comn-u	0%	URL Reputation	safe	
http://www.carterandcone.comn-u	0%	URL Reputation	safe	
http://www.carterandcone.comn-u	0%	URL Reputation	safe	
http://IsXVMb.com	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.founder.c	0%	URL Reputation	safe	
http://www.founder.c	0%	URL Reputation	safe	
http://www.founder.c	0%	URL Reputation	safe	
http://www.founder.c	0%	URL Reputation	safe	
http://www.urwpp.deFr(	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.founder.com.cn/cnt-p	0%	Avira URL Cloud	safe	
http://www.goodfont.co.krny	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.dewa	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	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://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://www.goodfont.co.krg	0%	Avira URL Cloud	safe	
http://www.tiro.comslntp	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr=	0%	Avira URL Cloud	safe	
http://www.urwpp.de#	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	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://www.founder.com.cn/cnuct	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kru	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://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.fontbureau.como$	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krn	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/nt	0%	Avira URL Cloud	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.come.com	0%	URL Reputation	safe	
http://www.fontbureau.come.com	0%	URL Reputation	safe	
http://www.fontbureau.come.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433221
Start date:	11.06.2021
Start time:	13:23:21
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	HT210525 IV Quotation.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	27
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.evad.winEXE@12/8@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1.6% (good quality ratio 1.1%) • Quality average: 45.5% • Quality standard deviation: 37.1%
HCA Information:	• Successful, ratio: 95% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
13:25:17	API Interceptor	389x Sleep call for process: RegSvcs.exe modified
13:25:30	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run NewApp C:\Users\user\AppData\Roaming\NewApp\NewApp.exe
13:25:38	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run NewApp C:\Users\user\AppData\Roaming\NewApp\NewApp.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Roaming\NewApp\NewApp.exe	Bank_payment information.exe	Get hash	malicious	Browse	
	HT210525 IV Quotation.exe	Get hash	malicious	Browse	
	Proforma Invoice No. 14214.exe	Get hash	malicious	Browse	
	KCTC International Ltd.exe	Get hash	malicious	Browse	
	NEW PO#70-02110-00739.exe	Get hash	malicious	Browse	
	New quote.exe	Get hash	malicious	Browse	
	Bank payment information.exe	Get hash	malicious	Browse	
	MESCO TQZ24 QUOTE.exe	Get hash	malicious	Browse	
	SWIFT Msg of USD 78,000.exe	Get hash	malicious	Browse	
	OM PHOENIX TRADERS.exe	Get hash	malicious	Browse	
	ORDER #2348478.exe	Get hash	malicious	Browse	
	1029BA046DF67EE328AD9D21BFD1E6D31C5CEDC4D4EAD.exe	Get hash	malicious	Browse	
	Quotation 2000051165.exe	Get hash	malicious	Browse	
	IMG-20191224-WA0050.jpg.exe	Get hash	malicious	Browse	
	Note0093746573.exe	Get hash	malicious	Browse	
	RYJzamn1HwAEPyy.exe	Get hash	malicious	Browse	
	11.exe	Get hash	malicious	Browse	
	OM PHOENIX TRADERS.exe	Get hash	malicious	Browse	
	NEW Quotation.exe	Get hash	malicious	Browse	
	tB15iC3ImLK3MFX.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\HT210525 IV Quotation.exe.log	
Process:	C:\Users\user\Desktop\HT210525 IV Quotation.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:ML9E4Ks29E4Kx1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MxHKX9HKx1qHiYHKhQnoPtHoxHhAHKzr
MD5:	B666A4404B132B2BF6C04FBF848EB948
SHA1:	D2EFB3D43F8B8806544D3A47F7DAEE8534981739
SHA-256:	7870616D981C8C0DE9A54E7383CD035470DB20CBF75ACDF729C32889D4B6ED96
SHA-512:	00E955EE9F14CEAE07E571A8EF2E103200CF421BAE83A66ED9F9E1AA6A9F449B653EDF1BFDB662A364D58ECF9B5FE4BB69D590DB2653F2F46A09F4D47719A862
Malicious:	**true**
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\HT210525 IV Quotation.exe.log	
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..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",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\NewApp.exe.log	
Process:	C:\Users\user\AppData\Roaming\NewApp\NewApp.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:	804A47494D9A462FFA6F39759480700ECBE5A7F3A15EC3A6330176ED9C04695D2684BF6BF85AB86286D52E7B727436D0BB2E8DA96E20D47740B5CE3F856B5D0F
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\tmpCED.tmp	
Process:	C:\Users\user\Desktop\HT210525 IV Quotation.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1658
Entropy (8bit):	5.16390772990795
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7h2ulNMFp2O/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB3oztn:cbha7JlNQV/rydbz9I3YODOLNdq3i
MD5:	407D163CED10E31402B2CADD4767DB34
SHA1:	31DCF29A9E58547B0E124FCE165B47E5DDF98DD4
SHA-256:	F44BF3B2B491CDD6F5E5C6D7F8DB4B7A9674CC0A4FC093E3BDC6D62174FC2F04
SHA-512:	7C13256812F14A6370D5B8C5ADEA0E24425BAE2944068B9C2ADC0597A4F40FA45211105FB40F9700C7E88628F4B69C330B9E5487802152BA4086697A19F0877B
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>.. <StartWhenAvail

C:\Users\user\AppData\Roaming\KEehxxQTfXmag.exe	
Process:	C:\Users\user\Desktop\HT210525 IV Quotation.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1129472
Entropy (8bit):	7.09477588573758
Encrypted:	false
SSDEEP:	24576:+Dv3KLaq4zaohfxhbyoHsCCRKumxfrvvdH0:2v3e34O+5pxsxRKumxfrt
MD5:	8EA3CB0D331F0A8414E5B2ECFCE3ABF3
SHA1:	4C690653287B4B783B46EC4991D71D81CA527DBC
SHA-256:	E2B3C7E7061E68AA31813371C589B7B0B11B12750FAB1CE87F5EA7CCA9740563
SHA-512:	04E819765B5D5D78B5834EA02226E4D3E4F65D9AE244C02D0F718DBBF65FCFED6839BA604B9F5E766A80E89004273923E70FBA0CE80B92DC5DE9D35CE37C6E3
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 59%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....0..<.....[... ...`....@.. ....@.....[..K....`.....`..... ....H.....text....;... ...<..... ..`.rsrc.....`.....>.....@..@.reloc.....` .....:.....@..B.....[.....H.....x.....r.....0.....(....(....*..0..U.....r...p. .M. .Q..a%...^E.....a.....8.....(.... ..C.+.,. .J..%+. .$.%&. ...Za+..(....(....r...p(....-. OF~u%+. ..'"%&. ...,Za8g....r...p(....(....-. }.A.%+. ..%&. x\ADZa89...(..... .3[.8).....s....(....%.(.....(.... .{/.8....r9..p(..... .'QZ ..9'a8.....r;. .p(....(....,. ....%+. V...%&. ;+T.Za8....*....0.....(0...*..0..

C:\Users\user\AppData\Roaming\NewApp\NewApp.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: Bank_payment information.exe, Detection: malicious, Browse • Filename: HT210525 IV Quotation.exe, Detection: malicious, Browse • Filename: Proforma Invoice No. 14214.exe, Detection: malicious, Browse • Filename: KCTC International Ltd.exe, Detection: malicious, Browse • Filename: NEW PO#70-02110-00739.exe, Detection: malicious, Browse • Filename: New quote.exe, Detection: malicious, Browse • Filename: Bank payment information.exe, Detection: malicious, Browse • Filename: MESCO TQZ24 QUOTE.exe, Detection: malicious, Browse • Filename: SWIFT Msg of USD 78,000.exe, Detection: malicious, Browse • Filename: OM PHOENIX TRADERS.exe, Detection: malicious, Browse • Filename: ORDER #2348478.exe, Detection: malicious, Browse • Filename: 1029BA046DF67EE328AD9D21BFD1E6D31C5CEDC4D4EAD.exe, Detection: malicious, Browse • Filename: Quotation 2000051165.exe, Detection: malicious, Browse • Filename: IMG-20191224-WA0050.jpg.exe, Detection: malicious, Browse • Filename: Note0093746573.exe, Detection: malicious, Browse • Filename: RYJzamn1HwAEPyy.exe, Detection: malicious, Browse • Filename: 11.exe, Detection: malicious, Browse • Filename: OM PHOENIX TRADERS.exe, Detection: malicious, Browse • Filename: NEW Quotation.exe, Detection: malicious, Browse • Filename: tB15iC3ImLK3MFX.exe, Detection: malicious, Browse
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**
Preview:	..127.0.0.1

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

\Device\ConDrv	
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):	7.09477588573758
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	HT210525 IV Quotation.exe
File size:	1129472
MD5:	8ea3cb0d331f0a8414e5b2ecfce3abf3
SHA1:	4c690653287b4b783b46ec4991d71d81ca527dbc
SHA256:	e2b3c7e7061e68aa31813371c589b7b0b11b12750fab1ce87f5ea7cca9740563
SHA512:	04e819765b5d5d78b5834ea02226e4d3e4f65d9ae244c02d0f718dbbf65fcfed6839ba604b9f5e766a80e89004273923e70fba0ce80b92dc5de9d35ce37c6e83
SSDEEP:	24576:+Dv3KLaq4zaohfxhbyoHsCCRKumxfrvvdH0:2v3e34O+5pxsxRKumxfrt
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....0..<.....[... ...`....@.. .....@.....

File Icon

Icon Hash:	929296929e9e8eb2

Static PE Info

General

Entrypoint:	0x4e5bce
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
Time Stamp:	0x60C1FEA2 [Thu Jun 10 11:59:30 2021 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

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xe3bd4	0xe3c00	False	0.665810879185	data	7.09066912036	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xe6000	0x2fbe8	0x2fc00	False	0.364002167866	data	6.27676522509	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x116000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: HT210525 IV Quotation.exe PID: 6688 Parent PID: 6040

General

Start time:	13:24:14
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\HT210525 IV Quotation.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\HT210525 IV Quotation.exe'
Imagebase:	0x540000
File size:	1129472 bytes
MD5 hash:	8EA3CB0D331F0A8414E5B2ECFCE3ABF3
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: 00000000.00000002.446010791.0000000003AEA000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.446010791.0000000003AEA000.00000004.00000001.sdmp, Author: Joe Security

Reputation:	low

File Activities — Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 6588 Parent PID: 6688

General

Start time:	13:25:05
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\KEehxxQTfXmag' /XML 'C:\Users\user\AppData\Local\Temp\tmpCED.tmp'
Imagebase:	0x1320000
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 — Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 6576 Parent PID: 6588

General

Start time:	13:25:06
Start date:	11/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: 6684 Parent PID: 6688

General

Start time:	13:25:06
Start date:	11/06/2021

Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x400000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegSvcs.exe PID: 6676 Parent PID: 6688

General

Start time:	13:25:07
Start date:	11/06/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x960000
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: 0000000D.00000002.595401687.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000D.00000002.595401687.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000D.00000000.440537158.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000D.00000000.440537158.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000D.00000002.597350034.0000000002C81000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000D.00000002.597350034.0000000002C81000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: NewApp.exe PID: 6868 Parent PID: 3440

General

Start time:	13:25:38

Start date:	11/06/2021
Path:	C:\Users\user\AppData\Roaming\NewApp\NewApp.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\NewApp\NewApp.exe'
Imagebase:	0xd20000
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:	high

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 3500 Parent PID: 6868

General

Start time:	13:25:38
Start date:	11/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: NewApp.exe PID: 5396 Parent PID: 3440

General

Start time:	13:25:46
Start date:	11/06/2021
Path:	C:\Users\user\AppData\Roaming\NewApp\NewApp.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\NewApp\NewApp.exe'
Imagebase:	0x6c0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities Show Windows behavior

File Written

File Read

Analysis Process: conhost.exe PID: 5472 Parent PID: 5396

General

Start time:	13:25:46
Start date:	11/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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