ID: 433447
Sample Name: shipping documents for PO#813-25319 192-463-56-265-3327.exe
Cookbook: default.jbs
Time: 21:11:13
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

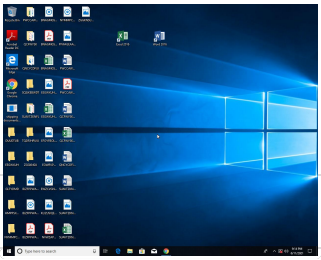
Analysis Report shipping documents for PO#813-25319 …

Overview

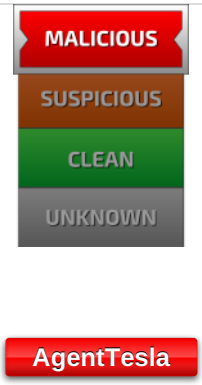
General Information

Sample Name:	shipping documents for PO#813-25319 192-463-56-265-3327.exe
Analysis ID:	433447
MD5:	1b323fcf40192af…
SHA1:	57b9c62162a645..
SHA256:	2ebf28b25bd92fc..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

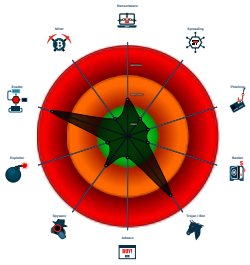


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains very larg…
- .NET source code contains very larg…
- Executable has a suspicious name (…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…

Classification



Process Tree

- **System is w10x64**
- shipping documents for PO#813-25319 192-463-56-265-3327.exe (PID: 6452 cmdline: 'C:\Users\user\Desktop\shipping documents for PO#813-25319 192-463-56-265-3327.exe' MD5: 1B323FCF40192AFD8C2D85ACCA658E7C)
  - schtasks.exe (PID: 4908 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\NkYArXVCGCJ' /XML 'C:\Users\user\AppData\Local\Temp\tmp4F70.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5092 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - shipping documents for PO#813-25319 192-463-56-265-3327.exe (PID: 5568 cmdline: {path} MD5: 1B323FCF40192AFD8C2D85ACCA658E7C)
  - shipping documents for PO#813-25319 192-463-56-265-3327.exe (PID: 5736 cmdline: {path} MD5: 1B323FCF40192AFD8C2D85ACCA658E7C)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "sales1@ashtavinayaka.com123456789smtpout.secureserver.net"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000B.00000002.469314122.0000000002A41000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000B.00000002.469314122.0000000002A41000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
0000000B.00000000.284322277.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000B.00000000.284322277.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
0000000B.00000002.466209715.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 9 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
11.0.shipping documents for PO#813-25319 192-463-56-265-3327.exe.400000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
11.0.shipping documents for PO#813-25319 192-463-56-265-3327.exe.400000.1.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.shipping documents for PO#813-25319 192-463-56-265-3327.exe.3f81588.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.shipping documents for PO#813-25319 192-463-56-265-3327.exe.3f81588.3.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
11.2.shipping documents for PO#813-25319 192-463-56-265-3327.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 5 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

Machine Learning detection for dropped file

Machine Learning detection for sample

System Summary:

.NET source code contains very large array initializations

.NET source code contains very large strings

Executable has a suspicious name (potential lure to open the executable)

Initial sample is a PE file and has a suspicious name

Boot Survival:

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

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

Stealing of Sensitive Information:

Yara detected AgentTesla

Yara detected AgentTesla

Remote Access Functionality:

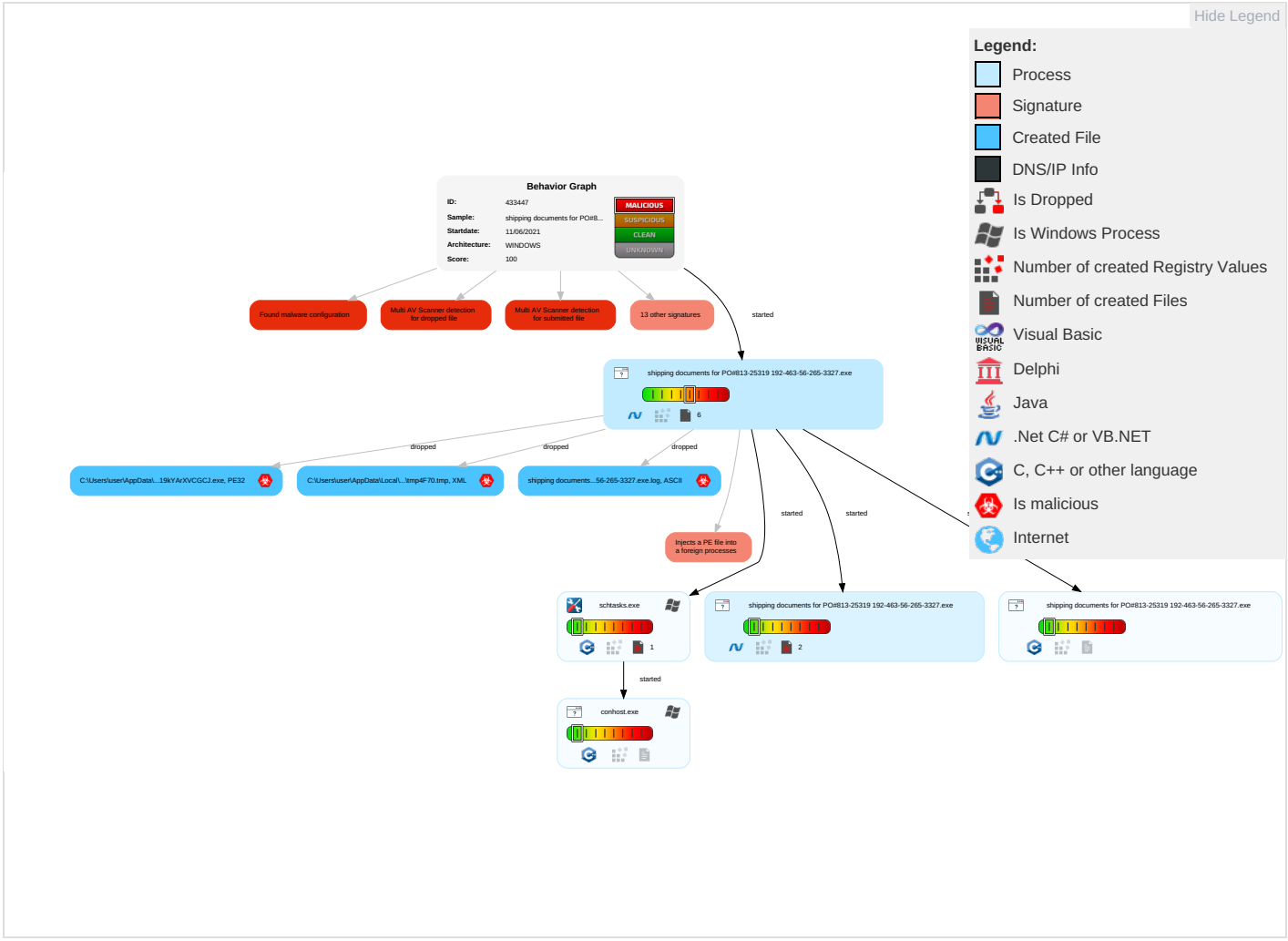
Yara detected AgentTesla

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	I
Valid Accounts	Windows Management Instrumentation 2 1 1	Scheduled Task/Job 1	Process Injection 1 1 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 3 2 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	I I I (
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	I I (
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1 4 1	Security Account Manager	Virtualization/Sandbox Evasion 1 4 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	I - I
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	S S
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	I I (
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	System Information Discovery 1 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	, I S
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	I A

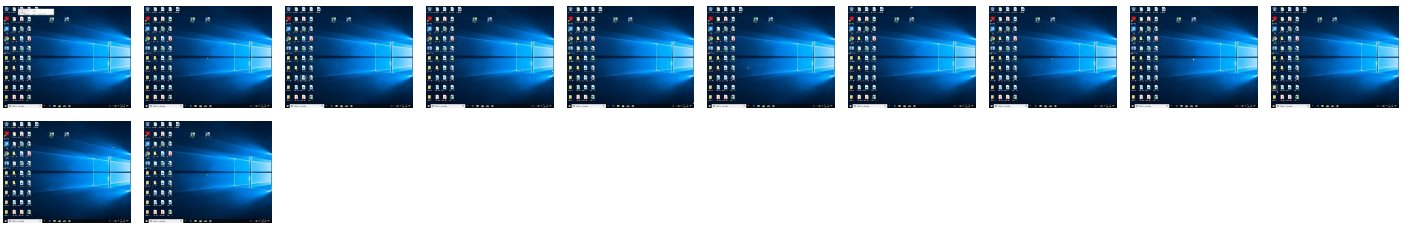
Behavior Graph



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
shipping documents for PO#813-25319 192-463-56-265-3327.exe	24%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
shipping documents for PO#813-25319 192-463-56-265-3327.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\NkYArXVCGCJ.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\NkYArXVCGCJ.exe	24%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
11.2.shipping documents for PO#813-25319 192-463-56-265-3327.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
11.0.shipping documents for PO#813-25319 192-463-56-265-3327.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://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/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://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://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.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.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	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	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	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.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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.deDPlease	0%	URL Reputation	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.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://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://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://kqfOpU.com	0%	Avira URL Cloud	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:	433447
Start date:	11.06.2021
Start time:	21:11:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	shipping documents for PO#813-25319 192-463-56-265-3327.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:	29
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default

Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@8/3@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.2% (good quality ratio 0.1%) • Quality average: 61.6% • Quality standard deviation: 33.1%
HCA Information:	• Successful, ratio: 97% • 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
21:12:50	API Interceptor	571x Sleep call for process: shipping documents for PO#813-25319 192-463-56-265-3327.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\shipping documents for PO#813-25319 192-463-56-265-3327.exe.log

Process:	C:\Users\user\Desktop\shipping documents for PO#813-25319 192-463-56-265-3327.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\shipping documents for PO#813-25319 192-463-56-265-3327.exe.log	
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Temp\tmp4F70.tmp	
Process:	C:\Users\user\Desktop\shipping documents for PO#813-25319 192-463-56-265-3327.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1644
Entropy (8bit):	5.206057226052344
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBto0tn:cbh47TlNQ//rydbz9l3YODOLNdq3j
MD5:	7B73EF087D2C095531D38AC617ECE4A4
SHA1:	D7B8B661A43DDF2681E31E5C999661D9FB80C0B8
SHA-256:	DC475B27B0F42A49B627BCF66ED7A933B2BAA4198F312AE041DF234FB10C6F4E
SHA-512:	6B5C89EB068C9915CCDEC28C1A69867830EB91A83CA1919FED96C2A885BF202B50B95DEF577EC6D792ACC03EB4384FA4FFF11806ED3CC185897A5C32D9618D 7
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\NkYArXVCGCJ.exe	
Process:	C:\Users\user\Desktop\shipping documents for PO#813-25319 192-463-56-265-3327.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	452096
Entropy (8bit):	7.761846193878433
Encrypted:	false
SSDEEP:	6144:zq0f9rlcph/61jE7pGczlztrJ4ZU/yJq8EIGNv7kZ1G/G1b68anUtAMH+3ZrqP:zqu9Gph/61k/zlNHZIgv7kq8yUJHmS
MD5:	1B323FCF40192AFD8C2D85ACCA658E7C
SHA1:	57B9C62162A645602E8EB059272BBB8BFCFF8D67
SHA-256:	2EBF28B25BD92FCB406458CAE714C8740A3FA162E664EC66B404C06990BB5D5F
SHA-512:	B9B731DE239467D7593FD20954F07AA028C7E2AEA8EF0E88891C309EEE70D35E3EEF15C05D8EDB92ED2F6573F36E210AB4070A7FAB80BDE8E21C831CACEF8E 84
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 24%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....0.....v.... .....@.. .....@..... ..@.....$...O..... ..... ..... ..H.....text...|.... ..... ..`.rsrc.....@..@.reloc..... .....@..B.....X.....H....._....r.....0.....{.....+..*..*"(.....*"(.....*....0.....,s....z*&..(.....*.....s.....s.....s .....*..0..].....~.....,?.~.....(.....~.....,..(...+.....,..(.....~.....+...*.....*E.....s.....*.0.....~.....+..*..0..P.....~.....(.....~.....,..s..... .~....r...p o.....,..(.....*.....:C.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.761846193878433

General

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:	shipping documents for PO#813-25319 192-463-56-265-3327.exe
File size:	452096
MD5:	1b323fcf40192afd8c2d85acca658e7c
SHA1:	57b9c62162a645602e8eb059272bbb8bfcff8d67
SHA256:	2ebf28b25bd92fcb406458cae714c8740a3fa162e664ec66b404c06990bb5d5f
SHA512:	b9b731de239467d7593fd20954f07aa028c7e2aea8ef0e88891c309eee70d35e3eef15c05d8edb92ed2f6573f36e210ab4070a7fab80bde8e21c831cacef8e84
SSDEEP:	6144:zq0f9rlcph/61jE7pGczlztrJ4ZU/yJq8EIGNv7kZ1G/G1b68anUtAMH+3ZrqP:zqu9Gph/61k/zlNHZIgv7kq8yUJHmS
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....0.....v.... .....@.. .....@.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x46fa76
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:	0x60C39E04 [Fri Jun 11 17:31:48 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	0x6da7c	0x6dc00	False	0.889724071042	data	7.77523245185	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x70000	0x5a4	0x600	False	0.419921875	data	4.071391437	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x72000	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: shipping documents for PO#813-25319 192-463-56-265-3327.exe PID: 6452 Parent PID: 5900

General

Start time:	21:11:59
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\shipping documents for PO#813-25319 192-463-56-265-3327.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\shipping documents for PO#813-25319 192-463-56-265-3327.exe'
Imagebase:	0x900000
File size:	452096 bytes
MD5 hash:	1B323FCF40192AFD8C2D85ACCA658E7C
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: 00000000.00000002.287835589.0000000003EBC000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.287835589.0000000003EBC000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.288101589.000000000404D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.288101589.000000000404D000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 4908 Parent PID: 6452

General

Start time:	21:12:37
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\NkYArXVCGCJ' /XML 'C:\Users\user\AppData\Local\Temp\tmp4F70.tmp'
Imagebase:	0x300000
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: 5092 Parent PID: 4908

General

Start time:	21:12:38
Start date:	11/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: shipping documents for PO#813-25319 192-463-56-265-3327.exe PID: 5568 Parent PID: 6452

General

Start time:	21:12:38
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\shipping documents for PO#813-25319 192-463-56-265-3327.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x150000
File size:	452096 bytes

MD5 hash:	1B323FCF40192AFD8C2D85ACCA658E7C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: shipping documents for PO#813-25319 192-463-56-265-3327.exe PID: 5736 Parent PID: 6452

General

Start time:	21:12:39
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\shipping documents for PO#813-25319 192-463-56-265-3327.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x650000
File size:	452096 bytes
MD5 hash:	1B323FCF40192AFD8C2D85ACCA658E7C
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: 0000000B.00000002.469314122.0000000002A41000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000B.00000002.469314122.0000000002A41000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000B.00000000.284322277.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000B.00000000.284322277.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000B.00000002.466209715.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000B.00000002.466209715.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Disassembly

Code Analysis