ID: 433208
Sample Name: shipping document -813-25319 192-463-56-265-3327.exe
Cookbook: default.jbs
Time: 13:02:16
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

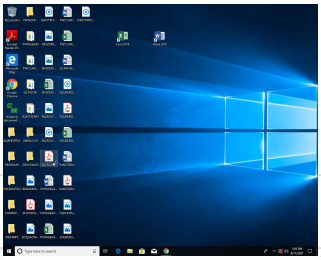
Analysis Report shipping document -813-25319 192-463…

Overview

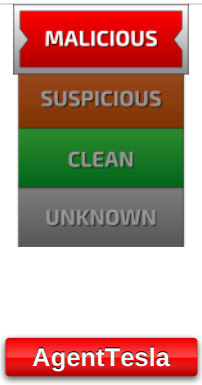
General Information

Sample Name:	shipping document -813-25319 192-463-56-265-3327.exe
Analysis ID:	433208
MD5:	4feedf906175f23…
SHA1:	77678c78e2d226..
SHA256:	f4888e1ee79c601.
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

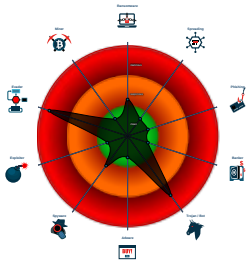


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- 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 (…
- Hides that the sample has been dow…
- Initial sample is a PE file and has a …

Classification



Process Tree

- **System is w10x64**
- shipping document -813-25319 192-463-56-265-3327.exe (PID: 4160 cmdline: 'C:\Users\user\Desktop\shipping document -813-25319 192-463-56-265-3327.exe' MD5: 4FEEDF906175F2357DCC2ABBFCDB5EC0)
  - schtasks.exe (PID: 4684 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\nclvXUThk' /XML 'C:\Users\user\AppData\Local\Temp\tmpD653.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 3880 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - shipping document -813-25319 192-463-56-265-3327.exe (PID: 3680 cmdline: {path} MD5: 4FEEDF906175F2357DCC2ABBFCDB5EC0)
- vaklXcs.exe (PID: 5732 cmdline: 'C:\Users\user\AppData\Local\Temp\vaklXcs\vaklXcs.exe' MD5: 4FEEDF906175F2357DCC2ABBFCDB5EC0)
  - schtasks.exe (PID: 5176 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\nclvXUThk' /XML 'C:\Users\user\AppData\Local\Temp\tmpF02F.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5548 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - vaklXcs.exe (PID: 1784 cmdline: {path} MD5: 4FEEDF906175F2357DCC2ABBFCDB5EC0)
  - vaklXcs.exe (PID: 3144 cmdline: {path} MD5: 4FEEDF906175F2357DCC2ABBFCDB5EC0)
  - vaklXcs.exe (PID: 4552 cmdline: {path} MD5: 4FEEDF906175F2357DCC2ABBFCDB5EC0)
- vaklXcs.exe (PID: 1332 cmdline: 'C:\Users\user\AppData\Local\Temp\vaklXcs\vaklXcs.exe' MD5: 4FEEDF906175F2357DCC2ABBFCDB5EC0)
  - schtasks.exe (PID: 476 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\nclvXUThk' /XML 'C:\Users\user\AppData\Local\Temp\tmp150D.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5540 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - vaklXcs.exe (PID: 244 cmdline: {path} MD5: 4FEEDF906175F2357DCC2ABBFCDB5EC0)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "comite.etica@uis.com.mxUIS30012019mail.uis.com.mx"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000021.00000002.478018686.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000021.00000002.478018686.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000021.00000000.464650955.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000021.00000000.464650955.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0000001E.00000000.445729425.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 25 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
20.2.vaklXcs.exe.37d2b48.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
20.2.vaklXcs.exe.37d2b48.3.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
13.0.shipping document -813-25319 192-463-56-265-3 327.exe.400000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
13.0.shipping document -813-25319 192-463-56-265-3 327.exe.400000.1.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
30.0.vaklXcs.exe.400000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 18 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

Networking:

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

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

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

Stealing of Sensitive Information:

Yara detected AgentTesla

Yara detected AgentTesla

Remote Access Functionality:

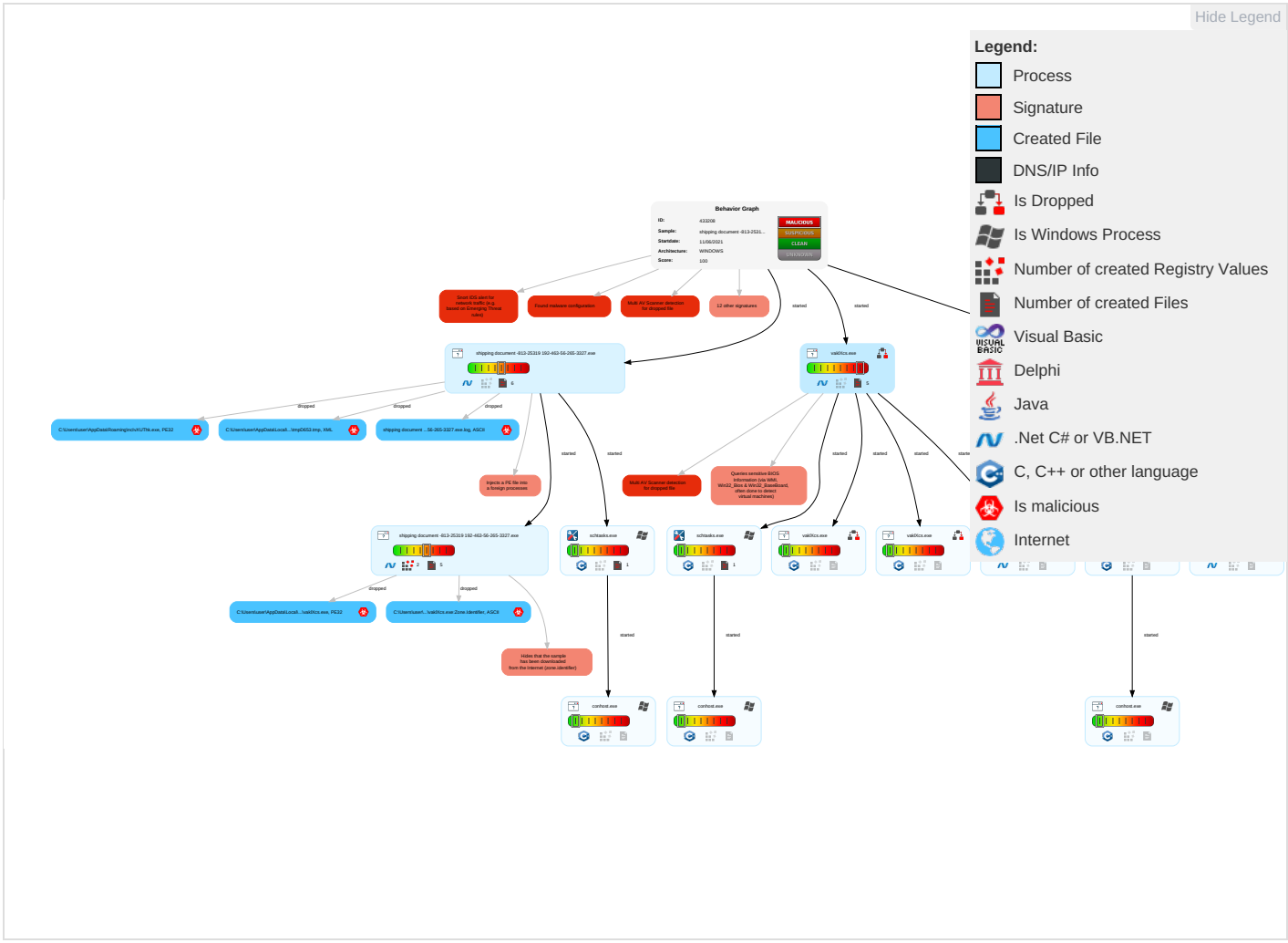
Yara detected AgentTesla

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 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
Default Accounts	Command and Scripting Interpreter 2	Registry Run Keys / Startup Folder 1	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
Domain Accounts	Scheduled Task/Job 1	Logon Script (Windows)	Registry Run Keys / Startup Folder 1	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
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
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
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	System Information Discovery 1 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 2	DCSync	Network Sniffing	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	Software Packing 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol

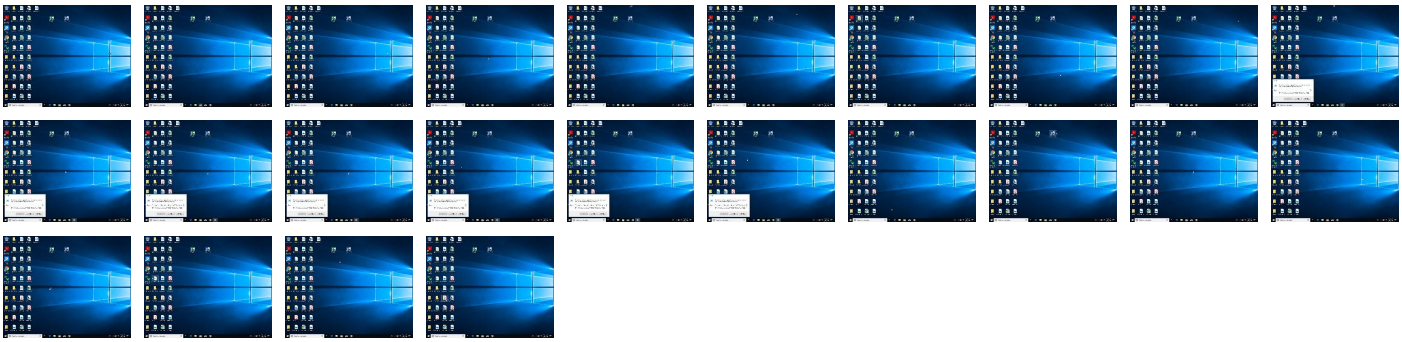
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
shipping document -813-25319 192-463-56-265-3327.exe	26%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\vaklXcs\vaklXcs.exe	26%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Roaming\nclvXUThk.exe	26%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
13.0.shipping document -813-25319 192-463-56-265-3327.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File
30.0.vaklXcs.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File
33.0.vaklXcs.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File
33.2.vaklXcs.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.carterandcone.comvi$	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	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.carterandcone.comTCW	0%	Avira URL Cloud	safe	
http://www.carterandcone.comzh	0%	Avira URL Cloud	safe	
http://xdqqbS.com	0%	Avira URL Cloud	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.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/:	0%	Avira URL Cloud	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.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.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/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://www.fontbureau.comgrita	0%	URL Reputation	safe	
http://www.fontbureau.comgrita	0%	URL Reputation	safe	
http://www.fontbureau.comgrita	0%	URL Reputation	safe	
http://www.carterandcone.comC	0%	URL Reputation	safe	
http://www.carterandcone.comC	0%	URL Reputation	safe	
http://www.carterandcone.comC	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/2	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/2	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/2	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.carterandcone.comThB	0%	Avira URL Cloud	safe	
http://www.carterandcone.comdnl	0%	Avira URL Cloud	safe	
http://www.carterandcone.com~f	0%	Avira URL Cloud	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	
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	

Source	Detection	Scanner	Label	Link
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.founder.com.cn/cnl-p	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.fontbureau.comce:	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cntan	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.carterandcone.comW	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/P	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/P	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/P	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/W:	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/F	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/F	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/F	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	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.carterandcone.com.i	0%	Avira URL Cloud	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	

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:	433208
Start date:	11.06.2021
Start time:	13:02:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	shipping document -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:	34
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@22/8@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 3.2% (good quality ratio 2.1%) • Quality average: 31.7% • Quality standard deviation: 26.3%
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
13:03:56	API Interceptor	510x Sleep call for process: shipping document -813-25319 192-463-56-265-3327.exe modified
13:04:09	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run vaklXcs C:\Users\user\AppData\Local\Temp\vaklXcs\vaklXcs.exe
13:04:17	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run vaklXcs C:\Users\user\AppData\Local\Temp\vaklXcs\vaklXcs.exe

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 document -813-25319 192-463-56-265-3327.exe.log	
Process:	C:\Users\user\Desktop\shipping document -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
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\Microsoft\CLR_v4.0_32\UsageLogs\vaklXcs.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\vaklXcs\vaklXcs.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
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	false
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\tmp150D.tmp	
Process:	C:\Users\user\AppData\Local\Temp\vaklXcs\vaklXcs.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1642
Entropy (8bit):	5.189154204067787
Encrypted:	false

C:\Users\user\AppData\Local\Temp\tmp150D.tmp	
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBu0tn:cbh47TlNQ//rydbz9I3YODOLNdq3b
MD5:	2CBB4E8E4660BB0E8CFB114D958EF15E
SHA1:	AD0DB5DE2F1194FC78B0DD3100D1CA5C4B5DF061
SHA-256:	0938E885DCD7EEDD10975EBDDF8AC3CC0B420146C36A2DE1E5365A0F883A3425
SHA-512:	8E2C788FC02EAF5DD1AA31B5EB37D9FEA0C3C126FB155363C98E9F3A141CC34A329D55022ADF105B80EE31CE5862BFB9CFDC661391CC53C5D955940743DA4 2
Malicious:	false
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\Local\Temp\tmpD653.tmp	
Process:	C:\Users\user\Desktop\shipping document -813-25319 192-463-56-265-3327.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1642
Entropy (8bit):	5.189154204067787
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBu0tn:cbh47TlNQ//rydbz9I3YODOLNdq3b
MD5:	2CBB4E8E4660BB0E8CFB114D958EF15E
SHA1:	AD0DB5DE2F1194FC78B0DD3100D1CA5C4B5DF061
SHA-256:	0938E885DCD7EEDD10975EBDDF8AC3CC0B420146C36A2DE1E5365A0F883A3425
SHA-512:	8E2C788FC02EAF5DD1AA31B5EB37D9FEA0C3C126FB155363C98E9F3A141CC34A329D55022ADF105B80EE31CE5862BFB9CFDC661391CC53C5D955940743DA4 2
Malicious:	**true**
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\Local\Temp\tmpF02F.tmp	
Process:	C:\Users\user\AppData\Local\Temp\vaklXcs\vaklXcs.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1642
Entropy (8bit):	5.189154204067787
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBu0tn:cbh47TlNQ//rydbz9I3YODOLNdq3b
MD5:	2CBB4E8E4660BB0E8CFB114D958EF15E
SHA1:	AD0DB5DE2F1194FC78B0DD3100D1CA5C4B5DF061
SHA-256:	0938E885DCD7EEDD10975EBDDF8AC3CC0B420146C36A2DE1E5365A0F883A3425
SHA-512:	8E2C788FC02EAF5DD1AA31B5EB37D9FEA0C3C126FB155363C98E9F3A141CC34A329D55022ADF105B80EE31CE5862BFB9CFDC661391CC53C5D955940743DA4 2
Malicious:	false
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\Local\Temp\vaklXcs\vaklXcs.exe	
Process:	C:\Users\user\Desktop\shipping document -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):	491520
Entropy (8bit):	7.657455226599555
Encrypted:	false
SSDEEP:	12288:AL5Mzm8gHdafEpNqBDfC4JoTmKU2pC5j9:AL5o0a6NKDfjoFvC5h
MD5:	4FEEDF906175F2357DCC2ABBFCDB5EC0
SHA1:	77678C78E2D226FE55BE6927436899129E47967E

C:\Users\user\AppData\Local\Temp\vaklXcs\vaklXcs.exe	
SHA-256:	F4888E1EE79C601D42020575CE5B79958C4C62E308D970F4A4F4C17B51EBC6E9
SHA-512:	438599FE3604A9737FFFB37E685847A612A5C9D409E9C7A96F12B2679F0A1844B3A7A011C5A31C8AF0AF39D88DB4A96A57C6C7C5AAEE6BD32F4E72B8F3D4904
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 26%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....0..j..... .....@.. ..... ..@.....\...O.....\..... ..... ..H.....text....h... ...j..... ..`.rsrc...\.....l.....@..@.reloc..... .....~.....@..B.....H.....@.....?....w..@.....^.(.....}.....}....*.0.....t.....t.....o.....{....o....o.....o....{....o....o.....o.....{....o....o... ..o.....{....o....o.....(.....{.....,....e..+.....+...*..0.....}.....(.....(.....r...p.(....(....o.....{.....(....o.....{...r...po.....{.....(....o.....{.....(....o.....{.....(....o.....*..0.._.....(.....(.....o .....,)....t.....o....r!..p(.....,..o....

C:\Users\user\AppData\Local\Temp\vaklXcs\vaklXcs.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\shipping document -813-25319 192-463-56-265-3327.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
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**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\nclvXUThk.exe	
Process:	C:\Users\user\Desktop\shipping document -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):	491520
Entropy (8bit):	7.657455226599555
Encrypted:	false
SSDEEP:	12288:AL5Mzm8gHdafEpNqBDfC4JoTmKU2pC5j9:AL5o0a6NKDfjoFvC5h
MD5:	4FEEDF906175F2357DCC2ABBFCDB5EC0
SHA1:	77678C78E2D226FE55BE6927436899129E47967E
SHA-256:	F4888E1EE79C601D42020575CE5B79958C4C62E308D970F4A4F4C17B51EBC6E9
SHA-512:	438599FE3604A9737FFFB37E685847A612A5C9D409E9C7A96F12B2679F0A1844B3A7A011C5A31C8AF0AF39D88DB4A96A57C6C7C5AAEE6BD32F4E72B8F3D4904
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 26%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....0..j..... .....@.. ..... ..@.....\...O.....\..... ..... ..H.....text....h... ...j..... ..`.rsrc...\.....l.....@..@.reloc..... .....~.....@..B.....H.....@.....?....w..@.....^.(.....}.....}....*.0.....t.....t.....o.....{....o....o.....o....{....o....o.....o.....{....o....o... ..o.....{....o....o.....(.....{.....,....e..+.....+...*..0.....}.....(.....(.....r...p.(....(....o.....{.....(....o.....{...r...po.....{.....(....o.....{.....(....o.....{.....(....o.....*..0.._.....(.....(.....o .....,)....t.....o....r!..p(.....,..o....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.657455226599555
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	shipping document -813-25319 192-463-56-265-3327.exe
File size:	491520
MD5:	4feedf906175f2357dcc2abbfcdb5ec0
SHA1:	77678c78e2d226fe55be6927436899129e47967e

General

SHA256:	f4888e1ee79c601d42020575ce5b79958c4c62e308d970 4a4f4c17b51ebc6e9
SHA512:	438599fe3604a9737fffb37e685847a612a5c9d409e9c7a 96f12b2679f0a1844b3a7a011c5a31c8af0af39d88db4a9 6a57c6c7c5aaee6bd32f4e72b8f3d49041
SSDEEP:	12288:AL5Mzm8gHdafEpNqBDfC4JoTmKU2pC5j9:AL5 o0a6NKDfjoFvC5h
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....PE..L..... .`.....0..j..... .....@.. ..... @.....

File Icon

Icon Hash:	18da1abcb2d2d2b0

Static PE Info

General

Entrypoint:	0x4788ae
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:	0x60C315DF [Fri Jun 11 07:50:55 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	0x768b4	0x76a00	False	0.865322872761	data	7.69114169634	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x7a000	0x105c	0x1200	False	0.270616319444	data	2.85467003783	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x7c000	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 document -813-25319 192-463-56-265-3327.exe PID: 4160 Parent PID: 5780

General

Start time:	13:03:02
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\shipping document -813-25319 192-463-56-265-3327.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\shipping document -813-25319 192-463-56-265-3327.exe'
Imagebase:	0xdc0000
File size:	491520 bytes
MD5 hash:	4FEEDF906175F2357DCC2ABBFCDB5EC0
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: 00000000.00000002.293199809.0000000004262000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.293199809.0000000004262000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.292688727.00000000040C9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.292688727.00000000040C9000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 4684 Parent PID: 4160

General

Start time:	13:03:41
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\ncIvXUThk' /XML 'C:\Users\user\AppData\Local\Temp\tmpD653.tmp'
Imagebase:	0xbe0000
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: 3880 Parent PID: 4684

General

Start time:	13:03:42
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 document -813-25319 192-463-56-265-3327.exe PID: 3680 Parent PID: 4160

General

Start time:	13:03:43
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\shipping document -813-25319 192-463-56-265-3327.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x760000
File size:	491520 bytes
MD5 hash:	4FEEDF906175F2357DCC2ABBFCDB5EC0
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.00000000.288112439.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000D.00000000.288112439.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Registry Activities — Show Windows behavior

Key Value Created

Analysis Process: vaklXcs.exe PID: 5732 Parent PID: 3388

General

Start time:	13:04:18
Start date:	11/06/2021
Path:	C:\Users\user\AppData\Local\Temp\vaklXcs\vaklXcs.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\vaklXcs\vaklXcs.exe'
Imagebase:	0x340000
File size:	491520 bytes
MD5 hash:	4FEEDF906175F2357DCC2ABBFCDB5EC0
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: 00000014.00000002.450985230.0000000003709000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000014.00000002.450985230.0000000003709000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000014.00000002.448006469.0000000002701000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 26%, ReversingLabs
Reputation:	low

File Activities — Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: vaklXcs.exe PID: 1332 Parent PID: 3388

General

Start time:	13:04:26
Start date:	11/06/2021
Path:	C:\Users\user\AppData\Local\Temp\vaklXcs\vaklXcs.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\vaklXcs\vaklXcs.exe'
Imagebase:	0xa0000
File size:	491520 bytes
MD5 hash:	4FEEDF906175F2357DCC2ABBFCDB5EC0
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: 00000016.00000002.473675525.0000000003639000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000016.00000002.473675525.0000000003639000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000016.00000002.471880084.0000000002684000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 5176 Parent PID: 5732

General

Start time:	13:04:54
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\ncIvXUThk' /XML 'C:\Users\user\AppData\Local\Temp\tmpF02F.tmp'
Imagebase:	0x190000
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: 5548 Parent PID: 5176

General

Start time:	13:04:54
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: vaklXcs.exe PID: 1784 Parent PID: 5732

General

Start time:	13:04:55
Start date:	11/06/2021
Path:	C:\Users\user\AppData\Local\Temp\vaklXcs\vaklXcs.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x40000
File size:	491520 bytes
MD5 hash:	4FEEDF906175F2357DCC2ABBFCDB5EC0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: vaklXcs.exe PID: 3144 Parent PID: 5732

General

Start time:	13:04:55
Start date:	11/06/2021
Path:	C:\Users\user\AppData\Local\Temp\vaklXcs\vaklXcs.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x140000
File size:	491520 bytes
MD5 hash:	4FEEDF906175F2357DCC2ABBFCDB5EC0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: vaklXcs.exe PID: 4552 Parent PID: 5732

General

Start time:	13:04:56
Start date:	11/06/2021
Path:	C:\Users\user\AppData\Local\Temp\vaklXcs\vaklXcs.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xa10000
File size:	491520 bytes
MD5 hash:	4FEEDF906175F2357DCC2ABBFCDB5EC0
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: 0000001E.00000000.445729425.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000001E.00000000.445729425.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: schtasks.exe PID: 476 Parent PID: 1332

General

Start time:	13:05:03
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\ncIvXUThk' /XML 'C:\Users\user\AppData\Local\Temp\tmp150D.tmp'
Imagebase:	0x190000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 5540 Parent PID: 476

General

Start time:	13:05:04
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: vaklXcs.exe PID: 244 Parent PID: 1332

General

Start time:	13:05:04
Start date:	11/06/2021
Path:	C:\Users\user\AppData\Local\Temp\vaklXcs\vaklXcs.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x7f0000
File size:	491520 bytes
MD5 hash:	4FEEDF906175F2357DCC2ABBFCDB5EC0
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: 00000021.00000002.478018686.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000021.00000002.478018686.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000021.00000000.464650955.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000021.00000000.464650955.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000021.00000002.481631193.0000000002BD1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000021.00000002.481631193.0000000002BD1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Disassembly

Code Analysis