ID: 764027
Sample Name: ORDER (6256 OS)#391 PI.exe
Cookbook: default.jbs
Time: 10:18:09
Date: 09/12/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

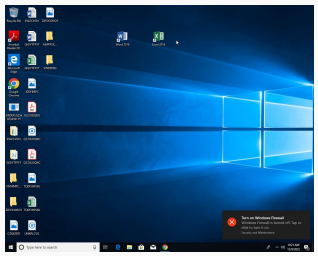
Windows Analysis Report

ORDER (6256 OS)#391 PI.exe

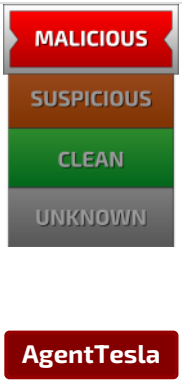
Overview

General Information

Sample Name:	ORDER (6256 OS)#391 PI.exe
Analysis ID:	764027
MD5:	19081ef2a08f678.
SHA1:	e86acea06a600f..
SHA256:	2f356283c20940..
Tags:	agenttesla exe
Infos:	



Detection



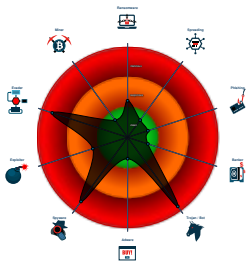
AgentTesla

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected Telegram RAT
- Yara detected AgentTesla
- Yara detected AntiVM3
- Sigma detected: Scheduled temp fil…
- Multi AV Scanner detection for drop…
- Snort IDS alert for network traffic
- Installs a global keyboard hook
- Tries to steal Mail credentials (via fi…
- Initial sample is a PE file and has a…
- Tries to harvest and steal Putty / W…

Classification



Process Tree

- **System is w10x64**
- ORDER (6256 OS)#391 PI.exe (PID: 1688 cmdline: C:\Users\user\Desktop\ORDER (6256 OS)#391 PI.exe MD5: 19081EF2A08F678A3203B29124043C41)
  - schtasks.exe (PID: 5964 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\WsdnBq" /XML "C:\Users\user\AppData\Local\Temp\tmpF47D.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 2236 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - ORDER (6256 OS)#391 PI.exe (PID: 5052 cmdline: {path} MD5: 19081EF2A08F678A3203B29124043C41)
  - ORDER (6256 OS)#391 PI.exe (PID: 1948 cmdline: {path} MD5: 19081EF2A08F678A3203B29124043C41)
- WsdnBq.exe (PID: 6004 cmdline: C:\Users\user\AppData\Roaming\WsdnBq.exe MD5: 19081EF2A08F678A3203B29124043C41)
  - schtasks.exe (PID: 2224 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\WsdnBq" /XML "C:\Users\user\AppData\Local\Temp\tmp645E.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 1496 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - WsdnBq.exe (PID: 1328 cmdline: {path} MD5: 19081EF2A08F678A3203B29124043C41)
- **cleanup**

Malware Configuration

Threatname: Telegram RAT

```
{
  "C2 url": "https://api.telegram.org/bot5962712783:AAFVWYP7zptQlynX_9COtuxYcx3Dl7EnfUQ/sendMessage"
}
```

Threatname: Agenttesla

```
{
  "Exfil Mode": "Telegram",
  "Telegram Url": "https://api.telegram.org/bot5962712783:AAFVWYP7zptQlynX_9COtuxYcx3Dl7EnfUQ/sendMessage?chat_id=1644584536"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.565934222.0000000002C20000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000008.00000002.566251641.00000000032BF000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000000.334155357.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x22d8b:$a20: get_LastAccessed • 0x24dde:$a30: set_GuidMasterKey • 0x22e59:$a33: get_Clipboard • 0x22e67:$a34: get_Keyboard • 0x23f96:$a35: get_ShiftKeyDown • 0x23fa7:$a36: get_AltKeyDown • 0x22e74:$a37: get_Password • 0x23882:$a38: get_PasswordHash • 0x246a9:$a39: get_DefaultCredentials
00000000.00000002.343033622.0000000003FC9000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0xfb66b:$a20: get_LastAccessed • 0x12368b:$a20: get_LastAccessed • 0xfd6be:$a30: set_GuidMasterKey • 0x1256de:$a30: set_GuidMasterKey • 0xfb739:$a33: get_Clipboard • 0x123759:$a33: get_Clipboard • 0xfb747:$a34: get_Keyboard • 0x123767:$a34: get_Keyboard • 0xfc876:$a35: get_ShiftKeyDown • 0x124896:$a35: get_ShiftKeyDown • 0xfc887:$a36: get_AltKeyDown • 0x1248a7:$a36: get_AltKeyDown • 0xfb754:$a37: get_Password • 0x123774:$a37: get_Password • 0xfc162:$a38: get_PasswordHash • 0x124182:$a38: get_PasswordHash • 0xfcf89:$a39: get_DefaultCredentials • 0x124fa9:$a39: get_DefaultCredentials
Process Memory Space: ORDER (6256 OS)#391 PI.exe PID: 1688	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Click to see the 9 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.ORDER (6256 OS)#391 PI.exe.40a16e0.1.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x24777:$s10: logins • 0x242b0:$s11: credential • 0x21259:$g1: get_Clipboard • 0x21267:$g2: get_Keyboard • 0x21274:$g3: get_Password • 0x22386:$g4: get_CtrlKeyDown • 0x22396:$g5: get_ShiftKeyDown • 0x223a7:$g6: get_AltKeyDown
0.2.ORDER (6256 OS)#391 PI.exe.40a16e0.1.unpack	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x2118b:$a20: get_LastAccessed • 0x231de:$a30: set_GuidMasterKey • 0x21259:$a33: get_Clipboard • 0x21267:$a34: get_Keyboard • 0x22396:$a35: get_ShiftKeyDown • 0x223a7:$a36: get_AltKeyDown • 0x21274:$a37: get_Password • 0x21c82:$a38: get_PasswordHash • 0x22aa9:$a39: get_DefaultCredentials
4.0.ORDER (6256 OS)#391 PI.exe.400000.0.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x26577:$s10: logins • 0x260b0:$s11: credential • 0x23059:$g1: get_Clipboard • 0x23067:$g2: get_Keyboard • 0x23074:$g3: get_Password • 0x24186:$g4: get_CtrlKeyDown • 0x24196:$g5: get_ShiftKeyDown • 0x241a7:$g6: get_AltKeyDown
4.0.ORDER (6256 OS)#391 PI.exe.400000.0.unpack	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x22f8b:$a20: get_LastAccessed • 0x24fde:$a30: set_GuidMasterKey • 0x23059:$a33: get_Clipboard • 0x23067:$a34: get_Keyboard • 0x24196:$a35: get_ShiftKeyDown • 0x241a7:$a36: get_AltKeyDown • 0x23074:$a37: get_Password • 0x23a82:$a38: get_PasswordHash • 0x248a9:$a39: get_DefaultCredentials

Source	Rule	Description	Author	Strings
0.2.ORDER (6256 OS)#391 PI.exe.40a16e0.1.raw.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x26577:$s10: logins • 0x4e597:$s10: logins • 0x260b0:$s11: credential • 0x4e0d0:$s11: credential • 0x23059:$g1: get_Clipboard • 0x4b079:$g1: get_Clipboard • 0x23067:$g2: get_Keyboard • 0x4b087:$g2: get_Keyboard • 0x23074:$g3: get_Password • 0x4b094:$g3: get_Password • 0x24186:$g4: get_CtrlKeyDown • 0x4c1a6:$g4: get_CtrlKeyDown • 0x24196:$g5: get_ShiftKeyDown • 0x4c1b6:$g5: get_ShiftKeyDown • 0x241a7:$g6: get_AltKeyDown • 0x4c1c7:$g6: get_AltKeyDown
Click to see the 3 entries				

Sigma Signatures

Persistence and Installation Behavior

Sigma detected: Scheduled temp file as task from temp location

Snort Signatures

ETPRO TROJAN Agent Tesla Telegram Exfil - Source IP: 192.168.2.4 - Destination IP: 149.154.167.220 −

Timestamp:	192.168.2.4149.154.167.220496964432851779 12/09/22-10:19:40.984166
SID:	2851779
Source Port:	49696
Destination Port:	443
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Agent Tesla Telegram Exfil - Source IP: 192.168.2.4 - Destination IP: 149.154.167.220 −

Timestamp:	192.168.2.4149.154.167.220496984432851779 12/09/22-10:20:17.013980
SID:	2851779
Source Port:	49698
Destination Port:	443
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted 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

Uses the Telegram API (likely for C&C communication)

May check the online IP address of the machine

Key, Mouse, Clipboard, Microphone and Screen Capturing

Installs a global keyboard hook

Contains functionality to register a low level keyboard hook

System Summary

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

.NET source code contains very large array initializations

Boot Survival

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

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

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected Telegram RAT

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 Telegram RAT

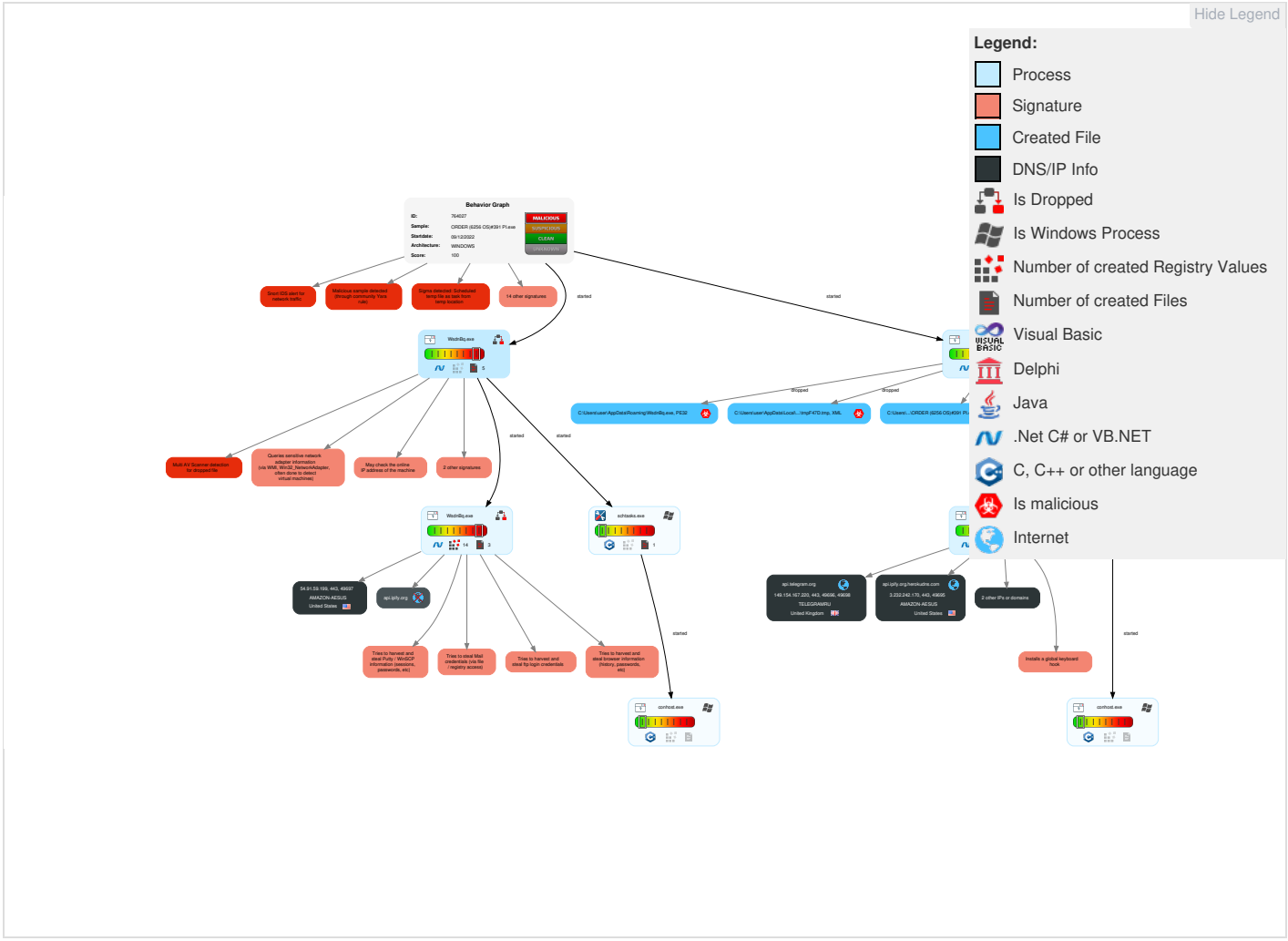
Yara detected AgentTesla

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	1 1 1 Process Injection	1 Disable or Modify Tools	2 OS Credential Dumping	1 File and Directory Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Web Service	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	1 Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Scheduled Task/Job	1 Deobfuscate/Decode Files or Information	2 1 Input Capture	1 1 4 System Information Discovery	Remote Desktop Protocol	2 Data from Local System	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	3 Obfuscated Files or Information	1 Credentials in Registry	3 1 1 Security Software Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	1 1 Encrypted Channel	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	2 Software Packing	NTDS	1 Process Discovery	Distributed Component Object Model	2 1 Input Capture	Scheduled Transfer	3 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Masquerading	LSA Secrets	1 3 1 Virtualization/Sandbox Evasion	SSH	1 Clipboard Data	Data Transfer Size Limits	1 4 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 3 1 Virtualization/Sandbox Evasion	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 1 1 Process Injection	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	Indicator Removal from Tools	Proc Filesystem	1 System Network Configuration Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

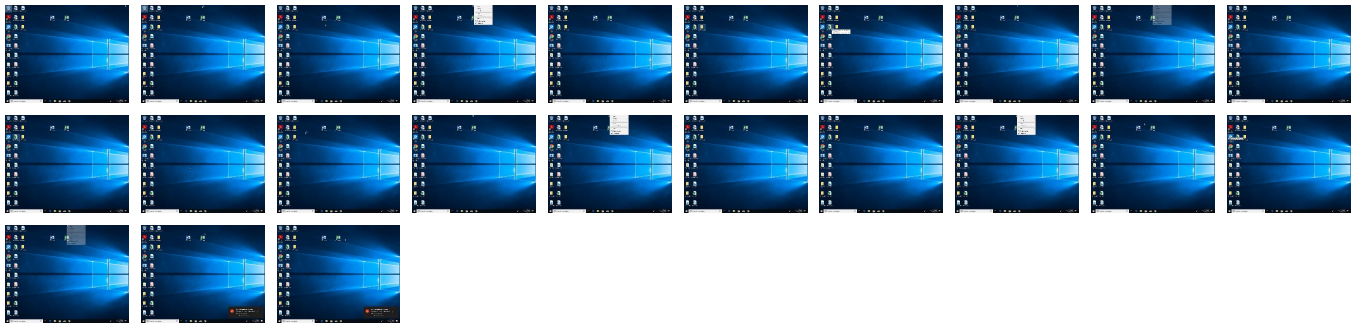
Behavior Graph



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
ORDER (6256 OS)#391 PI.exe	31%	ReversingLabs	ByteCode-MSIL.Trojan.Taskun	
ORDER (6256 OS)#391 PI.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\WsdnBq.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\WsdnBq.exe	31%	ReversingLabs	ByteCode-MSIL.Trojan.Taskun	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.0.ORDER (6256 OS)#391 PI.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1203035		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.fontbureau.comT.TTF	0%	URL Reputation	safe	
http://www.fontbureau.comiona	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/9	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://https://api.telegram.org4	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/.	0%	URL Reputation	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.fontbureau.com9	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fontbureau.comR.TTF	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/T	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/K	0%	URL Reputation	safe	
http://www.fontbureau.comto	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/oie.	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.comFQO	0%	Avira URL Cloud	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.fontbureau.comedFB	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Y0-eo	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.fontbureau.comals	0%	URL Reputation	safe	
http://www.fontbureau.comttod	0%	Avira URL Cloud	safe	
http://www.fontbureau.comd.	0%	Avira URL Cloud	safe	
http://www.fontbureau.comessedK	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/QO	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/hu-h	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htmY	0%	Avira URL Cloud	safe	
http://https://VEVgTqSNHWikc.orgD	0%	Avira URL Cloud	safe	
http://www.carterandcone.comigXje	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Y0m	0%	Avira URL Cloud	safe	
http://www.fontbureau.comalsq	0%	Avira URL Cloud	safe	
http://www.fontbureau.comsivFf	0%	Avira URL Cloud	safe	
http://www.fontbureau.comK	0%	Avira URL Cloud	safe	
http://www.fontbureau.comonyT	0%	Avira URL Cloud	safe	
http://www.fontbureau.comF.	0%	Avira URL Cloud	safe	
http://www.fontbureau.come.comQO	0%	Avira URL Cloud	safe	
http://www.fontbureau.comtalik	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.fontbureau.comW.TTF0	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/FL	0%	Avira URL Cloud	safe	
http://www.fontbureau.comtop/	0%	Avira URL Cloud	safe	
http://www.fontbureau.commB	0%	Avira URL Cloud	safe	
http://https://VEVgTqSNHWikc.org	0%	Avira URL Cloud	safe	
http://https://api.ipify.orgMozilla/5.0	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
api.ipify.org.herokudns.com	3.232.242.170	true	false		unknown
api.telegram.org	149.154.167.220	true	false		high
api.ipify.org	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://api.telegram.org/bot5962712783:AAFVWYP7zptQlynX_9COtuxYcx3DI7EnfUQ/sendDocument	false		high
http://https://api.ipify.org/	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	ORDER (6256 OS)#391 PI.exe, 00000000.00000002.349859716.00000000070E2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	ORDER (6256 OS)#391 PI.exe, 00000000.00000002.349859716.00000000070E2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	ORDER (6256 OS)#391 PI.exe, 00000000.00000002.349859716.00000000070E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.telegram.org	ORDER (6256 OS)#391 PI.exe, 00000004.00000002.567037453.0000000002CAF000.00000004.00000800.00020000.00000000.sdmp, WsdnBq.exe, 00000008.00000002.566476117.00000000032DE000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comFQO	ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306418196.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306179537.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306112026.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305947057.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305872051.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305902033.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306146868.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306356978.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306084469.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306295180.0000000005F18000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	ORDER (6256 OS)#391 PI.exe, 00000000.00000002.349859716.00000000070E2000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/hu-h	ORDER (6256 OS)#391 PI.exe, 00000000.00000003.302586272.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.302546639.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.302387437.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.302439715.0000000005F18000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/oie.	ORDER (6256 OS)#391 PI.exe, 00000000.00000003.302586272.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.302546639.0000000005F18000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.telegram.org/bot5962712783:AAFVWYP7zptQlynX_9COtuxYcx3DI7EnfUQ/1644584536appdatamacDpmac	WsdnBq.exe, 00000008.00000002.565696055.0000000003271000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comttod	ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306418196.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306179537.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305459409.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306112026.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305947057.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305334059.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305363596.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305872051.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306630165.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305405967.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305302404.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305688249.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305902033.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305793816.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306146868.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306356978.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306084469.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305838697.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306295180.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305649023.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306583635.0000000005F18000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.tiro.com	ORDER (6256 OS)#391 PI.exe, 00000000.00000002.349859716.00000000070E2000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.301411124.0000000005F0A000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.301391011.0000000005F09000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	ORDER (6256 OS)#391 PI.exe, 00000000.00000002.349859716.00000000070E2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	ORDER (6256 OS)#391 PI.exe, 00000000.00000002.349859716.00000000070E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comd.	ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304733777.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304498697.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3047 11949.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304659358.000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304523813.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305041614.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3047 57622.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304920069.000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304553639.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304474473.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3048 69319.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304627606.000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304797825.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304682884.0000000005F18000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/QO	ORDER (6256 OS)#391 PI.exe, 00000000.00003.302586272.0000000005F18000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comT.TTF	ORDER (6256 OS)#391 PI.exe, 00000000.00003.304733777.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305041614.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3047 57622.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304920069.000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304869319.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304797825.0000000005F18000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comiona	ORDER (6256 OS)#391 PI.exe, 00000000.00000003.309947315.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.309780990.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.309765831.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.311674086.0000000005F19000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000002.349633653.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.313163883.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.309806910.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.312483314.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.313647928.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.312816194.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.314195895.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.312692455.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.313408101.0000000005F19000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.312978255.0000000005F19000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.311583708.0000000005F19000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.312951679.0000000005F18000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	ORDER (6256 OS)#391 PI.exe, 00000000.00000002.349859716.00000000070E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/9	ORDER (6256 OS)#391 PI.exe, 00000000.00000003.302714801.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.302783202.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.302814290.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.302586272.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.302546639.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.302387437.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.302439715.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.302630012.0000000005F18000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	ORDER (6256 OS)#391 PI.exe, 00000000.00000002.349859716.00000000070E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comedFB	ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305110962.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305041614.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304757622.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305148691.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304920069.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305302404.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305217303.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304869319.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304797825.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305176599.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305196320.0000000005F18000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/cThe	ORDER (6256 OS)#391 PI.exe, 00000000.00000002.349859716.00000000070E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htmY	ORDER (6256 OS)#391 PI.exe, 00000000.00000003.307573750.0000000005F1B000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.307547855.0000000005F1B000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.307630920.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.307593958.0000000005F1B000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.307525322.0000000005F18000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	ORDER (6256 OS)#391 PI.exe, 00000000.00000002.349859716.00000000070E2000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000002.349450295.0000000005EDA000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.ipify.org	ORDER (6256 OS)#391 PI.exe, 00000004.00000002.565396808.0000000002BD1000.00000004.00000800.00020000.00000000.sdmp, WsdnBq.exe, 00000008.00000002.565696055.0000000003271000.00000004.00000800.00020000.00000000.sdmp	false		high
http://fontfabrik.com	ORDER (6256 OS)#391 PI.exe, 00000000.00000002.349859716.00000000070E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.telegram.org4	ORDER (6256 OS)#391 PI.exe, 00000004.00000002.567037453.0000000002CAF000.00000004.00000800.00020000.00000000.sdmp, WsdnBq.exe, 00000008.00000002.566476117.00000000032DE000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comessedK	ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304419984.0000000005F18000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/0	ORDER (6256 OS)#391 PI.exe, 00000000.00000003.302319712.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.302714801.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.302783202.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.302814290.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.302586272.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.302345072.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.302546639.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.302387437.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.302299146.0000000005F17000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.302439715.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.302630012.0000000005F18000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0-eo	ORDER (6256 OS)#391 PI.exe, 00000000.00000003.302714801.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.302783202.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.302814290.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.302630012.0000000005F18000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://VEVgTqSNHWikc.orgD	ORDER (6256 OS)#391 PI.exe, 00000004.00000002.567037453.0000000002CAF000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/.	ORDER (6256 OS)#391 PI.exe, 00000000.000 00003.304178747.0000000005F18000.0000000 4.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .303423712.0000000005F18000.00000004.000 00800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3027 14801.0000000005F18000.00000004.00000800 .00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.303953142.000000000 5F18000.00000004.00000800.00020000.00000 000.sdmp, ORDER (6256 OS)#391 PI.exe, 00 000000.00000003.302783202.0000000005F180 00.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .302814290.0000000005F18000.00000004.000 00800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3034 91476.0000000005F18000.00000004.00000800 .00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.303547143.000000000 5F18000.00000004.00000800.00020000.00000 000.sdmp, ORDER (6256 OS)#391 PI.exe, 00 000000.00000003.303113304.0000000005F180 00.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .304121403.0000000005F18000.00000004.000 00800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3039 24617.0000000005F18000.00000004.00000800 .00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.303459883.000000000 5F18000.00000004.00000800.00020000.00000 000.sdmp, ORDER (6256 OS)#391 PI.exe, 00 000000.00000003.303190453.0000000005F180 00.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .303711642.0000000005F18000.00000004.000 00800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3032 88048.0000000005F18000.00000004.00000800 .00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304203849.000000000 5F18000.00000004.00000800.00020000.00000 000.sdmp, ORDER (6256 OS)#391 PI.exe, 00 000000.00000003.304055892.0000000005F180 00.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .304005746.0000000005F18000.00000004.000 00800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3032 59684.0000000005F18000.00000004.00000800 .00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.303777091.000000000 5F18000.00000004.00000800.00020000.00000 000.sdmp, ORDER (6256 OS)#391 PI.exe, 00 000000.00000003.303357363.0000000005F180 00.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comigXje	ORDER (6256 OS)#391 PI.exe, 00000000.000 00003.301936890.0000000005ED3000.0000000 4.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/Y0m	ORDER (6256 OS)#391 PI.exe, 00000000.000 00003.302546639.0000000005F18000.0000000 4.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .302387437.0000000005F18000.00000004.000 00800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3024 39715.0000000005F18000.00000004.00000800 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	WsdnBq.exe, 00000008.00000002.565696055. 0000000003271000.00000004.00000800.00020 000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/	ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304733777.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305041614.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304757622.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304920069.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304869319.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304797825.0000000005F18000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.galapagosdesign.com/DPlease	ORDER (6256 OS)#391 PI.exe, 00000000.00000002.349859716.00000000070E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0	ORDER (6256 OS)#391 PI.exe, 00000000.00000003.302439715.0000000005F18000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com9	ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304203849.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304228747.0000000005F18000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comalsq	ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306418196.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306179537.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305459409.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306112026.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305947057.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305872051.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305605967.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305688249.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305902033.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305793816.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306146868.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306356978.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306084469.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305838697.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306295180.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305649023.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305517979.0000000005F18000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comsivFf	ORDER (6256 OS)#391 PI.exe, 00000000.000 00003.306418196.0000000005F18000.0000000 4.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .306179537.0000000005F18000.00000004.000 00800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3061 12026.0000000005F18000.00000004.00000800 .00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305947057.000000000 5F18000.00000004.00000800.00020000.00000 000.sdmp, ORDER (6256 OS)#391 PI.exe, 00 000000.00000003.305872051.0000000005F180 00.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .305902033.0000000005F18000.00000004.000 00800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3061 46868.0000000005F18000.00000004.00000800 .00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306356978.000000000 5F18000.00000004.00000800.00020000.00000 000.sdmp, ORDER (6256 OS)#391 PI.exe, 00 000000.00000003.306084469.0000000005F180 00.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .306295180.0000000005F18000.00000004.000 00800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.ascendercorp.com/typedesigners.html	ORDER (6256 OS)#391 PI.exe, 00000000.000 00003.307345140.0000000005F13000.0000000 4.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .304196469.0000000005F13000.00000004.000 00800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3046 51333.0000000005F13000.00000004.00000800 .00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304139159.000000000 5F13000.00000004.00000800.00020000.00000 000.sdmp, ORDER (6256 OS)#391 PI.exe, 00 000000.00000003.305855891.0000000005F130 00.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .306476107.0000000005F13000.00000004.000 00800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3044 91242.0000000005F13000.00000004.00000800 .00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.303482107.000000000 5F13000.00000004.00000800.00020000.00000 000.sdmp, ORDER (6256 OS)#391 PI.exe, 00 000000.00000003.305929932.0000000005F130 00.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .304437139.0000000005F13000.00000004.000 00800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3073 12499.0000000005F13000.00000004.00000800 .00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304413252.000000000 5F13000.00000004.00000800.00020000.00000 000.sdmp, ORDER (6256 OS)#391 PI.exe, 00 000000.00000003.306400487.0000000005F130 00.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .303216869.0000000005F13000.00000004.000 00800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3031 04333.0000000005F13000.00000004.00000800 .00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306139248.000000000 5F13000.00000004.00000800.00020000.00000 000.sdmp, ORDER (6256 OS)#391 PI.exe, 00 000000.00000003.304750887.0000000005F130 00.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .304466931.0000000005F13000.00000004.000 00800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3053 54155.0000000005F13000.00000004.00000800 .00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.303996945.000000000 5F13000.00000004.00000800.00020000.00000 000.sdmp, ORDER (6256 OS)#391 PI.exe, 00 000000.00000003.303155186.0000000005F130 00.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fonts.com	ORDER (6256 OS)#391 PI.exe, 00000000.00000002.349859716.00000000070E2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	ORDER (6256 OS)#391 PI.exe, 00000000.00000002.349859716.00000000070E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	ORDER (6256 OS)#391 PI.exe, 00000000.00000002.349859716.00000000070E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	ORDER (6256 OS)#391 PI.exe, 00000000.00000002.349859716.00000000070E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	ORDER (6256 OS)#391 PI.exe, 00000000.00000002.338224910.0000000002FC1000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000004.00000002.565396808.0000000002BD1000.00000004.00000800.00020000.00000000.sdmp, WsdnBq.exe, 00000005.00000002.398697821.0000000002D41000.00000004.00000800.00020000.00000000.sdmp, WsdnBq.exe, 00000008.00000002.565696055.0000000003271000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	ORDER (6256 OS)#391 PI.exe, 00000000.00000002.349859716.00000000070E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comF.	ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306418196.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306179537.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306112026.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305947057.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306146868.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306356978.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306084469.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306295180.0000000005F18000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comR.TTF	ORDER (6256 OS)#391 PI.exe, 00000000.000 00003.304733777.0000000005F18000.0000000 4.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .304498697.0000000005F18000.00000004.000 00800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3051 10962.0000000005F18000.00000004.00000800 .00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304711949.000000000 5F18000.00000004.00000800.00020000.00000 000.sdmp, ORDER (6256 OS)#391 PI.exe, 00 000000.00000003.304659358.0000000005F180 00.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .304523813.0000000005F18000.00000004.000 00800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3050 41614.0000000005F18000.00000004.00000800 .00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304757622.000000000 5F18000.00000004.00000800.00020000.00000 000.sdmp, ORDER (6256 OS)#391 PI.exe, 00 000000.00000003.305148691.0000000005F180 00.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .304920069.0000000005F18000.00000004.000 00800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3045 53639.0000000005F18000.00000004.00000800 .00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305302404.000000000 5F18000.00000004.00000800.00020000.00000 000.sdmp, ORDER (6256 OS)#391 PI.exe, 00 000000.00000003.305217303.0000000005F180 00.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .304474473.0000000005F18000.00000004.000 00800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3048 69319.0000000005F18000.00000004.00000800 .00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304627606.000000000 5F18000.00000004.00000800.00020000.00000 000.sdmp, ORDER (6256 OS)#391 PI.exe, 00 000000.00000003.304797825.0000000005F180 00.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .304682884.0000000005F18000.00000004.000 00800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3044 43149.0000000005F18000.00000004.00000800 .00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305176599.000000000 5F18000.00000004.00000800.00020000.00000 000.sdmp, ORDER (6256 OS)#391 PI.exe, 00 000000.00000003.305196320.0000000005F180 00.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	ORDER (6256 OS)#391 PI.exe, 00000000.000 00002.349859716.00000000070E2000.0000000 4.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .301689714.0000000005F13000.00000004.000 00800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com	ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304178747.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000002.349859716.00000000070E2000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304733777.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304498697.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305110962.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304711949.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304659358.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304523813.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305041614.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304757622.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305148691.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304920069.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304553639.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304203849.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304474473.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304869319.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304627606.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304797825.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304419984.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304682884.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304443149.0000000005F18000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.galapagosdesign.com/	ORDER (6256 OS)#391 PI.exe, 00000000.00000003.307525322.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.307540852.0000000005F18000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comK	ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306418196.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306179537.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305459409.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306112026.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305947057.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305334059.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305363596.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305872051.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306630165.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305405967.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305302404.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305688249.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305902033.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305793816.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306146868.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306356978.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306084469.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305838697.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306295180.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305649023.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306583635.0000000005F18000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/FL	ORDER (6256 OS)#391 PI.exe, 00000000.00000003.302546639.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.302387437.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.302630012.0000000005F18000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comF	ORDER (6256 OS)#391 PI.exe, 00000000.000 00003.306418196.0000000005F18000.0000000 4.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .306179537.0000000005F18000.00000004.000 00800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3054 59409.0000000005F18000.00000004.00000800 .00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306112026.000000000 5F18000.00000004.00000800.00020000.00000 000.sdmp, ORDER (6256 OS)#391 PI.exe, 00 000000.00000003.305947057.0000000005F180 00.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .305872051.0000000005F18000.00000004.000 00800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3066 30165.0000000005F18000.00000004.00000800 .00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305405967.000000000 5F18000.00000004.00000800.00020000.00000 000.sdmp, ORDER (6256 OS)#391 PI.exe, 00 000000.00000003.305688249.0000000005F180 00.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .305902033.0000000005F18000.00000004.000 00800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3057 93816.0000000005F18000.00000004.00000800 .00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306146868.000000000 5F18000.00000004.00000800.00020000.00000 000.sdmp, ORDER (6256 OS)#391 PI.exe, 00 000000.00000003.306356978.0000000005F180 00.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .306084469.0000000005F18000.00000004.000 00800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3058 38697.0000000005F18000.00000004.00000800 .00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306295180.000000000 5F18000.00000004.00000800.00020000.00000 000.sdmp, ORDER (6256 OS)#391 PI.exe, 00 000000.00000003.305649023.0000000005F180 00.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .306583635.0000000005F18000.00000004.000 00800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3055 17979.0000000005F18000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/T	ORDER (6256 OS)#391 PI.exe, 00000000.000 00003.302714801.0000000005F18000.0000000 4.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .302783202.0000000005F18000.00000004.000 00800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3028 14290.0000000005F18000.00000004.00000800 .00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.302586272.000000000 5F18000.00000004.00000800.00020000.00000 000.sdmp, ORDER (6256 OS)#391 PI.exe, 00 000000.00000003.302546639.0000000005F180 00.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .302630012.0000000005F18000.00000004.000 00800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.come.comQO	ORDER (6256 OS)#391 PI.exe, 00000000.000 00003.309947315.0000000005F18000.0000000 4.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .309780990.0000000005F18000.00000004.000 00800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3116 74086.0000000005F19000.00000004.00000800 .00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.313163883.000000000 5F18000.00000004.00000800.00020000.00000 000.sdmp, ORDER (6256 OS)#391 PI.exe, 00 000000.00000003.309806910.0000000005F180 00.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .312483314.0000000005F18000.00000004.000 00800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3136 47928.0000000005F18000.00000004.00000800 .00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.312816194.000000000 5F18000.00000004.00000800.00020000.00000 000.sdmp, ORDER (6256 OS)#391 PI.exe, 00 000000.00000003.314195867.0000000005F180 00.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .312692455.0000000005F18000.00000004.000 00800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3134 08101.0000000005F19000.00000004.00000800 .00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.312978255.000000000 5F19000.00000004.00000800.00020000.00000 000.sdmp, ORDER (6256 OS)#391 PI.exe, 00 000000.00000003.311643593.0000000005F180 00.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .314379195.0000000005F18000.00000004.000 00800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3103 04190.0000000005F18000.00000004.00000800 .00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.311583708.000000000 5F19000.00000004.00000800.00020000.00000 000.sdmp, ORDER (6256 OS)#391 PI.exe, 00 000000.00000003.312951679.0000000005F180 00.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/K	ORDER (6256 OS)#391 PI.exe, 00000000.000 00003.302319712.0000000005F18000.0000000 4.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .302714801.0000000005F18000.00000004.000 00800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3027 83202.0000000005F18000.00000004.00000800 .00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.302814290.000000000 5F18000.00000004.00000800.00020000.00000 000.sdmp, ORDER (6256 OS)#391 PI.exe, 00 000000.00000003.302586272.0000000005F180 00.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .302345072.0000000005F18000.00000004.000 00800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3025 46639.0000000005F18000.00000004.00000800 .00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.302387437.000000000 5F18000.00000004.00000800.00020000.00000 000.sdmp, ORDER (6256 OS)#391 PI.exe, 00 000000.00000003.302299146.0000000005F170 00.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .302439715.0000000005F18000.00000004.000 00800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3026 30012.0000000005F18000.00000004.00000800 .00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.303017257.000000000 5F18000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.telegram.org/bot5962712783:AAFVWYP7zptQlynX_9COtuxYcx3DI7EnfUQ/	ORDER (6256 OS)#391 PI.exe, 00000004.000 00002.565396808.0000000002BD1000.0000000 4.00000800.00020000.00000000.sdmp, WsdnBq.exe, 00000008.00000002.565696055.000000000327100 0.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comto	ORDER (6256 OS)#391 PI.exe, 00000000.000 00003.304733777.0000000005F18000.0000000 4.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .304498697.0000000005F18000.00000004.000 00800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3051 10962.0000000005F18000.00000004.00000800 .00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304711949.000000000 5F18000.00000004.00000800.00020000.00000 000.sdmp, ORDER (6256 OS)#391 PI.exe, 00 000000.00000003.304659358.0000000005F180 00.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .304523813.0000000005F18000.00000004.000 00800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3050 41614.0000000005F18000.00000004.00000800 .00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304757622.000000000 5F18000.00000004.00000800.00020000.00000 000.sdmp, ORDER (6256 OS)#391 PI.exe, 00 000000.00000003.305148691.0000000005F180 00.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .304920069.0000000005F18000.00000004.000 00800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3045 53639.0000000005F18000.00000004.00000800 .00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304474473.000000000 5F18000.00000004.00000800.00020000.00000 000.sdmp, ORDER (6256 OS)#391 PI.exe, 00 000000.00000003.304869319.0000000005F180 00.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .304627606.0000000005F18000.00000004.000 00800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3047 97825.0000000005F18000.00000004.00000800 .00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304682884.000000000 5F18000.00000004.00000800.00020000.00000 000.sdmp, ORDER (6256 OS)#391 PI.exe, 00 000000.00000003.304443149.0000000005F180 00.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .305176599.0000000005F18000.00000004.000 00800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3051 96320.0000000005F18000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	ORDER (6256 OS)#391 PI.exe, 00000000.000 00003.302630012.0000000005F18000.0000000 4.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .303017257.0000000005F18000.00000004.000 00800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3033 19313.0000000005F18000.00000004.00000800 .00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.303225948.000000000 5F18000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comd	ORDER (6256 OS)#391 PI.exe, 00000000.000 00003.305041614.0000000005F18000.0000000 4.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .304757622.0000000005F18000.00000004.000 00800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3049 20069.0000000005F18000.00000004.00000800 .00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304869319.000000000 5F18000.00000004.00000800.00020000.00000 000.sdmp, ORDER (6256 OS)#391 PI.exe, 00 000000.00000003.304797825.0000000005F180 00.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comonyT	ORDER (6256 OS)#391 PI.exe, 00000000.000 00003.306418196.0000000005F18000.0000000 4.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .306179537.0000000005F18000.00000004.000 00800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3054 59409.0000000005F18000.00000004.00000800 .00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306112026.000000000 5F18000.00000004.00000800.00020000.00000 000.sdmp, ORDER (6256 OS)#391 PI.exe, 00 000000.00000003.305947057.0000000005F180 00.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .305872051.0000000005F18000.00000004.000 00800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3056 88249.0000000005F18000.00000004.00000800 .00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305902033.000000000 5F18000.00000004.00000800.00020000.00000 000.sdmp, ORDER (6256 OS)#391 PI.exe, 00 000000.00000003.305793816.0000000005F180 00.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .306146868.0000000005F18000.00000004.000 00800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3063 56978.0000000005F18000.00000004.00000800 .00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306084469.000000000 5F18000.00000004.00000800.00020000.00000 000.sdmp, ORDER (6256 OS)#391 PI.exe, 00 000000.00000003.305838697.0000000005F180 00.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .306295180.0000000005F18000.00000004.000 00800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3056 49023.0000000005F18000.00000004.00000800 .00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305517979.000000000 5F18000.00000004.00000800.00020000.00000 000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	ORDER (6256 OS)#391 PI.exe, 00000000.000 00002.349859716.00000000070E2000.0000000 4.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	ORDER (6256 OS)#391 PI.exe, 00000000.000 00003.301420395.0000000005F0F000.0000000 4.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .301223897.0000000005F0F000.00000004.000 00800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3013 13763.0000000005F10000.00000004.00000800 .00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.301537024.000000000 5F10000.00000004.00000800.00020000.00000 000.sdmp, ORDER (6256 OS)#391 PI.exe, 00 000000.00000003.301391011.0000000005F090 00.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .301444783.0000000005F0F000.00000004.000 00800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3014 60866.0000000005F10000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	ORDER (6256 OS)#391 PI.exe, 00000000.000 00002.349859716.00000000070E2000.0000000 4.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn	ORDER (6256 OS)#391 PI.exe, 00000000.000 00002.349859716.00000000070E2000.0000000 4.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .300897558.0000000005F09000.00000004.000 00800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3009 40819.0000000005F0A000.00000004.00000800 .00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.301936890.000000000 5ED3000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown

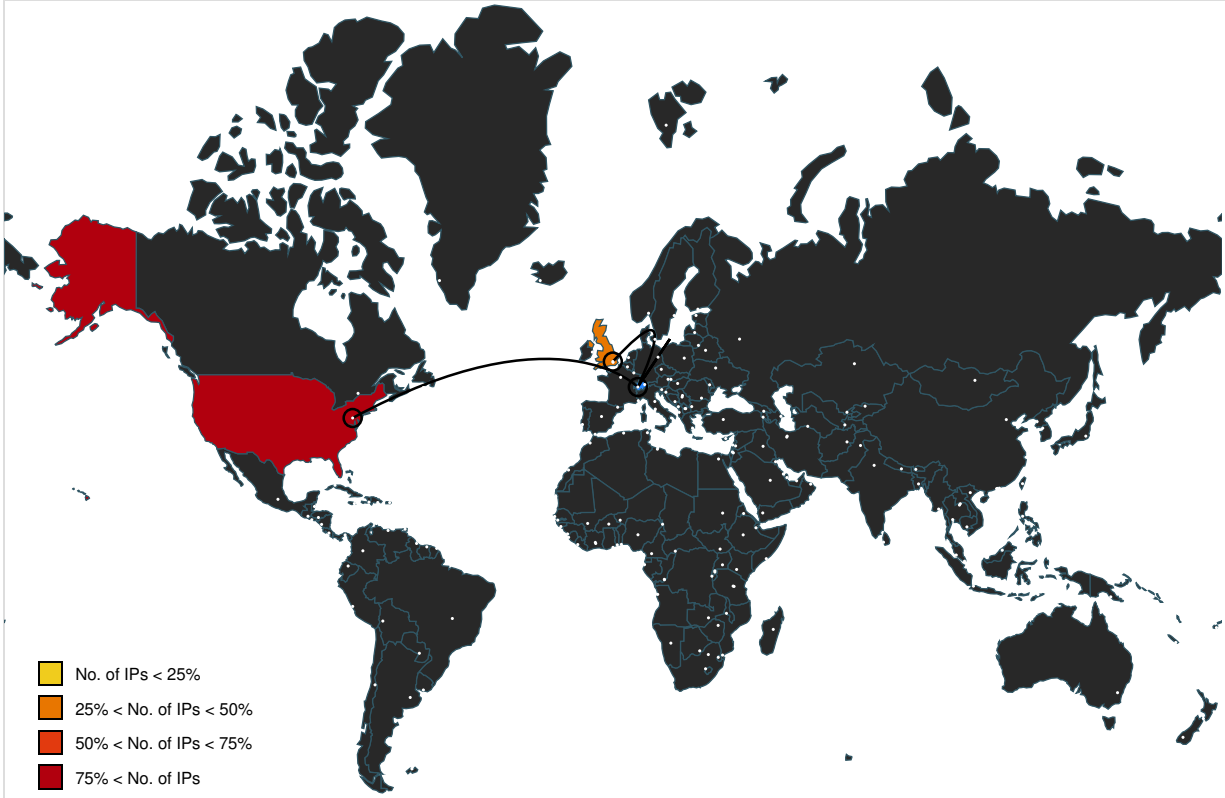
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/frere-user.html	ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304757622.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304887480.0000000005F1D000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304797825.0000000005F18000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/cabarga.html	ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305302404.0000000005F18000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comtalik	ORDER (6256 OS)#391 PI.exe, 00000000.00000003.30414920 1.0000000005F18000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comW.TTF0	ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304733777.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304498697.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304711949.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304659358.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304523813.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305041614.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304757622.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304920069.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304553639.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304474473.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304869319.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304627606.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304797825.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304682884.0000000005F18000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.commB	ORDER (6256 OS)#391 PI.exe, 00000000.000 00003.309947315.0000000005F18000.0000000 4.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .309780990.0000000005F18000.00000004.000 00800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3097 65831.0000000005F18000.00000004.00000800 .00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.311674086.000000000 5F19000.00000004.00000800.00020000.00000 000.sdmp, ORDER (6256 OS)#391 PI.exe, 00 000000.00000002.349633653.0000000005F180 00.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .313163883.0000000005F18000.00000004.000 00800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3098 06910.0000000005F18000.00000004.00000800 .00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.312483314.000000000 5F18000.00000004.00000800.00020000.00000 000.sdmp, ORDER (6256 OS)#391 PI.exe, 00 000000.00000003.313647928.0000000005F180 00.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .312816194.0000000005F18000.00000004.000 00800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3141 95867.0000000005F18000.00000004.00000800 .00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.312692455.000000000 5F18000.00000004.00000800.00020000.00000 000.sdmp, ORDER (6256 OS)#391 PI.exe, 00 000000.00000003.313408101.0000000005F190 00.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .312978255.0000000005F19000.00000004.000 00800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3116 43593.0000000005F18000.00000004.00000800 .00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.314379195.000000000 5F18000.00000004.00000800.00020000.00000 000.sdmp, ORDER (6256 OS)#391 PI.exe, 00 000000.00000003.310304190.0000000005F180 00.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .311583708.0000000005F19000.00000004.000 00800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3129 51679.0000000005F18000.00000004.00000800 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	ORDER (6256 OS)#391 PI.exe, 00000000.000 00003.303017257.0000000005F18000.0000000 4.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .303319313.0000000005F18000.00000004.000 00800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3032 25948.0000000005F18000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.como	ORDER (6256 OS)#391 PI.exe, 00000000.000 00003.309947315.0000000005F18000.0000000 4.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .309780990.0000000005F18000.00000004.000 00800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3116 74086.0000000005F19000.00000004.00000800 .00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.309806910.000000000 5F18000.00000004.00000800.00020000.00000 000.sdmp, ORDER (6256 OS)#391 PI.exe, 00 000000.00000003.304149201.0000000005F180 00.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003 .311643593.0000000005F18000.00000004.000 00800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.3103 04190.0000000005F18000.00000004.00000800 .00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.311583708.000000000 5F19000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers8	ORDER (6256 OS)#391 PI.exe, 00000000.00000002.349859716.00000000070E2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comals	ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306418196.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306179537.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306112026.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.305947057.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306630165.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306146868.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306356978.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306084469.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306295180.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.306583635.0000000005F18000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comtop/	ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304178747.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304498697.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304711949.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304659358.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304523813.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304553639.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304203849.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304474473.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304315545.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304286522.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304627606.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304419984.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304682884.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304443149.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304228747.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304257902.0000000005F18000.00000004.00000800.00020000.00000000.sdmp, ORDER (6256 OS)#391 PI.exe, 00000000.00000003.304393632.0000000005F18000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://VEVgTqSNHWikc.org	WsdnBq.exe, 00000008.00000002.566476117.00000000032DE000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://api.telegram.org	ORDER (6256 OS)#391 PI.exe, 00000004.00000002.567037453.0000000002CAF000.00000004.00000800.00020000.00000000.sdmp, WsdnBq.exe, 00000008.00000002.566476117.00000000032DE000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.ipify.orgMozilla/5.0	WsdnBq.exe, 00000008.00000002.565696055.0000000003271000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
149.154.167.220	api.telegram.org	United Kingdom		62041	TELEGRAMRU	false
54.91.59.199	unknown	United States		14618	AMAZON-AESUS	false
3.232.242.170	api.ipify.org.herokudns.com	United States		14618	AMAZON-AESUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	764027
Start date and time:	2022-12-09 10:18:09 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ORDER (6256 OS)#391 PI.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	14
Number of new started drivers analysed:	0
Number of existing processes analysed:	0

Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@14/5@6/4
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 95% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe
- 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
10:19:10	API Interceptor	674x Sleep call for process: ORDER (6256 OS)#391 PI.exe modified
10:19:17	Task Scheduler	Run new task: WsdnBq path: C:\Users\user\AppData\Roaming\WsdnBq.exe
10:19:40	API Interceptor	428x Sleep call for process: WsdnBq.exe modified

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\ORDER (6256 OS)#391 PI.exe.log

Process:	C:\Users\user\Desktop\ORDER (6256 OS)#391 PI.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, Ve rsion=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72 e6\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, Cultur e=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.Con figuration.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\WsdnBq.exe.log

Process:	C:\Users\user\AppData\Roaming\WsdnBq.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:	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, Ve rsion=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72 e6\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, Cultur e=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.Con figuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Temp\tmp645E.tmp

Process:	C:\Users\user\AppData\Roaming\WsdnBq.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1639
Entropy (8bit):	5.175860465839716
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGyYtn:cbhK79lNQR/rydbz9l3YODOLNdq3u
MD5:	0DBBF38DD1BB19DDB9D0C429955A1C4B
SHA1:	09B7CD25F4FBF6BD3EB74FF25BDA85A71B99C87E
SHA-256:	33B74500742DA6CCCF3FAB1A31DBD7953A5FB36C95EE25EF574839D96BB6D7C5
SHA-512:	6AE4FE4F7D63F604014A27AD1A59A8E8013D21A562B3025E656C2C1A5BB6C6FE1551F1B7F88B746A7D4BEBABDC023C2880377BD6B8DA13B5EB7EF74D34145F C1
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\tmpF47D.tmp

Process:	C:\Users\user\Desktop\ORDER (6256 OS)#391 PI.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1639
Entropy (8bit):	5.175860465839716
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGyYtn:cbhK79lNQR/rydbz9l3YODOLNdq3u
MD5:	0DBBF38DD1BB19DDB9D0C429955A1C4B
SHA1:	09B7CD25F4FBF6BD3EB74FF25BDA85A71B99C87E
SHA-256:	33B74500742DA6CCCF3FAB1A31DBD7953A5FB36C95EE25EF574839D96BB6D7C5
SHA-512:	6AE4FE4F7D63F604014A27AD1A59A8E8013D21A562B3025E656C2C1A5BB6C6FE1551F1B7F88B746A7D4BEBABDC023C2880377BD6B8DA13B5EB7EF74D34145FC1
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\WsdnBq.exe

Process:	C:\Users\user\Desktop\ORDER (6256 OS)#391 PI.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	873472
Entropy (8bit):	7.665798175957009
Encrypted:	false
SSDEEP:	24576:F2ibxF1RKDbH8emeHmXlO3Qe5/uwg5+RAj:/xFqXHXmeOlO3QW/2e
MD5:	19081EF2A08F678A3203B29124043C41
SHA1:	E86ACEA06A600F170402A0C1020C25AC2550FFA0
SHA-256:	2F356283C209400C6385A24450F266B59477E035E9389C8D1AF4843CD1AD2374
SHA-512:	AAD284AE800F26F6D27A12EC66CD42C781861DE7FBD907B8C5B3938DC8FA343286B35E21A56C3680CC92E36D1857FB8F1FD53796F3A82BE182245493855FFA3
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 31%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....J.c.....P..J.....h... .....@.. .....@.....\h..O.....+..T..... ....H.....text....H... ...J..... ..`.rsrc.....L.....@..@.reloc.....R.....@..B.....h.....H.....T...p.....(....*&..(.....*.s..... .....s!.....s".....s#.....*...0.....~....o$....+..*.0.....~....o%....+..*.0.....~....o&....+..*.0.....~....o'....+..*.0.....~....o(....+..*&..()....*...0..<.....~.....(*.....,!r...p.....(+...o,...s-.....~.....+..*.0.....~....+..*"....*.0.....(....r-..p~....o.....+..*...0..<.....~.....(*.....,!r=..p.....(+

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.665798175957009
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:	ORDER (6256 OS)#391 PI.exe
File size:	873472
MD5:	19081ef2a08f678a3203b29124043c41
SHA1:	e86acea06a600f170402a0c1020c25ac2550ffa0

SHA256:	2f356283c209400c6385a24450f266b59477e035e9389c8d1af4843cd1ad2374
SHA512:	aad284ae800f26f6d27a12ec66cd42c781861de7fbd907b8c5b3938dc8fa343286b35e21a56c3680cc92e36d1857fb8f1fd53796f3a82be182245493855ffa3f
SSDEEP:	24576:F2ibxF1RKDbH8emeHmXlO3Qe5/uwg5+RAj:/xFqXHXmeOlO3QW/2e
TLSH:	BC058BA773FB16E6C03492F4256063310EF1D62D89178731EF9458E89BA2A77C9E1732
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L....J.c..............P..J...........h... ....@.. ....@................................

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4d68ae
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:	0x63914A88 [Thu Dec 8 02:23:04 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

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
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	0xd685c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xd8000	0x5b4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xda000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xd2bd4	0x54	.text
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	0xd48b4	0xd4a00	False	0.8199416244121105	data	7.6706447927786225	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xd8000	0x5b4	0x600	False	0.421875	data	4.115880835857526	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xda000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xd8090	0x324	data		
RT_MANIFEST	0xd83c4	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Imports

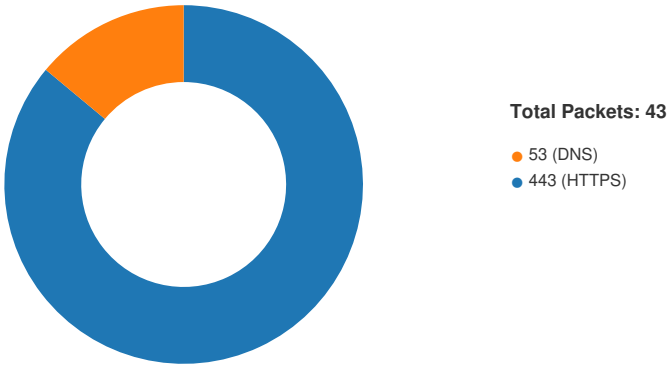
DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.4149.154.167.220496964432851779 12/09/22-10:19:40.984166	TCP	2851779	ETPRO TROJAN Agent Tesla Telegram Exfil	49696	443	192.168.2.4	149.154.167.220
192.168.2.4149.154.167.220496984432851779 12/09/22-10:20:17.013980	TCP	2851779	ETPRO TROJAN Agent Tesla Telegram Exfil	49698	443	192.168.2.4	149.154.167.220

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 9, 2022 10:19:22.698903084 CET	49695	443	192.168.2.4	3.232.242.170
Dec 9, 2022 10:19:22.698968887 CET	443	49695	3.232.242.170	192.168.2.4
Dec 9, 2022 10:19:22.699067116 CET	49695	443	192.168.2.4	3.232.242.170
Dec 9, 2022 10:19:22.772326946 CET	49695	443	192.168.2.4	3.232.242.170
Dec 9, 2022 10:19:22.772398949 CET	443	49695	3.232.242.170	192.168.2.4
Dec 9, 2022 10:19:23.034101963 CET	443	49695	3.232.242.170	192.168.2.4
Dec 9, 2022 10:19:23.034198046 CET	49695	443	192.168.2.4	3.232.242.170
Dec 9, 2022 10:19:23.039324045 CET	49695	443	192.168.2.4	3.232.242.170
Dec 9, 2022 10:19:23.039352894 CET	443	49695	3.232.242.170	192.168.2.4
Dec 9, 2022 10:19:23.039694071 CET	443	49695	3.232.242.170	192.168.2.4
Dec 9, 2022 10:19:23.219844103 CET	49695	443	192.168.2.4	3.232.242.170
Dec 9, 2022 10:19:24.152493000 CET	49695	443	192.168.2.4	3.232.242.170
Dec 9, 2022 10:19:24.152535915 CET	443	49695	3.232.242.170	192.168.2.4
Dec 9, 2022 10:19:24.271603107 CET	443	49695	3.232.242.170	192.168.2.4
Dec 9, 2022 10:19:24.271747112 CET	443	49695	3.232.242.170	192.168.2.4
Dec 9, 2022 10:19:24.271814108 CET	49695	443	192.168.2.4	3.232.242.170
Dec 9, 2022 10:19:24.275346994 CET	49695	443	192.168.2.4	3.232.242.170
Dec 9, 2022 10:19:40.860681057 CET	49696	443	192.168.2.4	149.154.167.220
Dec 9, 2022 10:19:40.860760927 CET	443	49696	149.154.167.220	192.168.2.4
Dec 9, 2022 10:19:40.860915899 CET	49696	443	192.168.2.4	149.154.167.220
Dec 9, 2022 10:19:40.861772060 CET	49696	443	192.168.2.4	149.154.167.220
Dec 9, 2022 10:19:40.861812115 CET	443	49696	149.154.167.220	192.168.2.4
Dec 9, 2022 10:19:40.937942982 CET	443	49696	149.154.167.220	192.168.2.4
Dec 9, 2022 10:19:40.938097954 CET	49696	443	192.168.2.4	149.154.167.220
Dec 9, 2022 10:19:40.942301035 CET	49696	443	192.168.2.4	149.154.167.220
Dec 9, 2022 10:19:40.942333937 CET	443	49696	149.154.167.220	192.168.2.4
Dec 9, 2022 10:19:40.942708969 CET	443	49696	149.154.167.220	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 9, 2022 10:19:40.944998980 CET	49696	443	192.168.2.4	149.154.167.220
Dec 9, 2022 10:19:40.945044041 CET	443	49696	149.154.167.220	192.168.2.4
Dec 9, 2022 10:19:40.980653048 CET	443	49696	149.154.167.220	192.168.2.4
Dec 9, 2022 10:19:40.983958960 CET	49696	443	192.168.2.4	149.154.167.220
Dec 9, 2022 10:19:40.984009981 CET	443	49696	149.154.167.220	192.168.2.4
Dec 9, 2022 10:19:41.150307894 CET	443	49696	149.154.167.220	192.168.2.4
Dec 9, 2022 10:19:41.150484085 CET	443	49696	149.154.167.220	192.168.2.4
Dec 9, 2022 10:19:41.150557995 CET	49696	443	192.168.2.4	149.154.167.220
Dec 9, 2022 10:19:41.150974035 CET	49696	443	192.168.2.4	149.154.167.220
Dec 9, 2022 10:19:53.055398941 CET	49697	443	192.168.2.4	54.91.59.199
Dec 9, 2022 10:19:53.055483103 CET	443	49697	54.91.59.199	192.168.2.4
Dec 9, 2022 10:19:53.055583954 CET	49697	443	192.168.2.4	54.91.59.199
Dec 9, 2022 10:19:53.072854996 CET	49697	443	192.168.2.4	54.91.59.199
Dec 9, 2022 10:19:53.072901011 CET	443	49697	54.91.59.199	192.168.2.4
Dec 9, 2022 10:19:53.324731112 CET	443	49697	54.91.59.199	192.168.2.4
Dec 9, 2022 10:19:53.324889898 CET	49697	443	192.168.2.4	54.91.59.199
Dec 9, 2022 10:19:53.327763081 CET	49697	443	192.168.2.4	54.91.59.199
Dec 9, 2022 10:19:53.327800989 CET	443	49697	54.91.59.199	192.168.2.4
Dec 9, 2022 10:19:53.328203917 CET	443	49697	54.91.59.199	192.168.2.4
Dec 9, 2022 10:19:53.534943104 CET	443	49697	54.91.59.199	192.168.2.4
Dec 9, 2022 10:19:53.535114050 CET	49697	443	192.168.2.4	54.91.59.199
Dec 9, 2022 10:19:53.805990934 CET	49697	443	192.168.2.4	54.91.59.199
Dec 9, 2022 10:19:53.806211948 CET	443	49697	54.91.59.199	192.168.2.4
Dec 9, 2022 10:19:53.927993059 CET	443	49697	54.91.59.199	192.168.2.4
Dec 9, 2022 10:19:53.928147078 CET	443	49697	54.91.59.199	192.168.2.4
Dec 9, 2022 10:19:53.928283930 CET	49697	443	192.168.2.4	54.91.59.199
Dec 9, 2022 10:19:53.929414034 CET	49697	443	192.168.2.4	54.91.59.199
Dec 9, 2022 10:20:16.890120983 CET	49698	443	192.168.2.4	149.154.167.220
Dec 9, 2022 10:20:16.890194893 CET	443	49698	149.154.167.220	192.168.2.4
Dec 9, 2022 10:20:16.890625954 CET	49698	443	192.168.2.4	149.154.167.220
Dec 9, 2022 10:20:16.891558886 CET	49698	443	192.168.2.4	149.154.167.220
Dec 9, 2022 10:20:16.891596079 CET	443	49698	149.154.167.220	192.168.2.4
Dec 9, 2022 10:20:16.961730957 CET	443	49698	149.154.167.220	192.168.2.4
Dec 9, 2022 10:20:16.962007999 CET	49698	443	192.168.2.4	149.154.167.220
Dec 9, 2022 10:20:16.966172934 CET	49698	443	192.168.2.4	149.154.167.220
Dec 9, 2022 10:20:16.966219902 CET	443	49698	149.154.167.220	192.168.2.4
Dec 9, 2022 10:20:16.966680050 CET	443	49698	149.154.167.220	192.168.2.4
Dec 9, 2022 10:20:16.969074011 CET	49698	443	192.168.2.4	149.154.167.220
Dec 9, 2022 10:20:16.969122887 CET	443	49698	149.154.167.220	192.168.2.4
Dec 9, 2022 10:20:17.013200998 CET	443	49698	149.154.167.220	192.168.2.4
Dec 9, 2022 10:20:17.013797998 CET	49698	443	192.168.2.4	149.154.167.220
Dec 9, 2022 10:20:17.013845921 CET	443	49698	149.154.167.220	192.168.2.4
Dec 9, 2022 10:20:17.194960117 CET	443	49698	149.154.167.220	192.168.2.4
Dec 9, 2022 10:20:17.195230007 CET	443	49698	149.154.167.220	192.168.2.4
Dec 9, 2022 10:20:17.195997000 CET	49698	443	192.168.2.4	149.154.167.220
Dec 9, 2022 10:20:17.196050882 CET	443	49698	149.154.167.220	192.168.2.4
Dec 9, 2022 10:20:17.196135044 CET	49698	443	192.168.2.4	149.154.167.220
Dec 9, 2022 10:20:17.196135044 CET	49698	443	192.168.2.4	149.154.167.220

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 9, 2022 10:19:22.594918013 CET	56572	53	192.168.2.4	8.8.8.8
Dec 9, 2022 10:19:22.613454103 CET	53	56572	8.8.8.8	192.168.2.4
Dec 9, 2022 10:19:22.628007889 CET	50911	53	192.168.2.4	8.8.8.8
Dec 9, 2022 10:19:22.646457911 CET	53	50911	8.8.8.8	192.168.2.4
Dec 9, 2022 10:19:40.828479052 CET	59683	53	192.168.2.4	8.8.8.8
Dec 9, 2022 10:19:40.847109079 CET	53	59683	8.8.8.8	192.168.2.4
Dec 9, 2022 10:19:52.963900089 CET	64167	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 9, 2022 10:19:52.980617046 CET	53	64167	8.8.8.8	192.168.2.4
Dec 9, 2022 10:19:53.015748024 CET	58565	53	192.168.2.4	8.8.8.8
Dec 9, 2022 10:19:53.034867048 CET	53	58565	8.8.8.8	192.168.2.4
Dec 9, 2022 10:20:16.871406078 CET	52239	53	192.168.2.4	8.8.8.8
Dec 9, 2022 10:20:16.888513088 CET	53	52239	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Dec 9, 2022 10:19:22.594918013 CET	192.168.2.4	8.8.8.8	0xcdbb	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:19:22.628007889 CET	192.168.2.4	8.8.8.8	0x39c2	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:19:40.828479052 CET	192.168.2.4	8.8.8.8	0xc143	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:19:52.963900089 CET	192.168.2.4	8.8.8.8	0xaabb	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:19:53.015748024 CET	192.168.2.4	8.8.8.8	0x1a60	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:20:16.871406078 CET	192.168.2.4	8.8.8.8	0x7df	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Dec 9, 2022 10:19:22.613454103 CET	8.8.8.8	192.168.2.4	0xcdbb	No error (0)	api.ipify.org	api.ipify.org.herokudns.com		CNAME (Canonical name)	IN (0x0001)	false
Dec 9, 2022 10:19:22.613454103 CET	8.8.8.8	192.168.2.4	0xcdbb	No error (0)	api.ipify.org.herokudns.com		3.232.242.170	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:19:22.613454103 CET	8.8.8.8	192.168.2.4	0xcdbb	No error (0)	api.ipify.org.herokudns.com		52.20.78.240	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:19:22.613454103 CET	8.8.8.8	192.168.2.4	0xcdbb	No error (0)	api.ipify.org.herokudns.com		3.220.57.224	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:19:22.613454103 CET	8.8.8.8	192.168.2.4	0xcdbb	No error (0)	api.ipify.org.herokudns.com		54.91.59.199	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:19:22.646457911 CET	8.8.8.8	192.168.2.4	0x39c2	No error (0)	api.ipify.org	api.ipify.org.herokudns.com		CNAME (Canonical name)	IN (0x0001)	false
Dec 9, 2022 10:19:22.646457911 CET	8.8.8.8	192.168.2.4	0x39c2	No error (0)	api.ipify.org.herokudns.com		52.20.78.240	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:19:22.646457911 CET	8.8.8.8	192.168.2.4	0x39c2	No error (0)	api.ipify.org.herokudns.com		3.232.242.170	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:19:22.646457911 CET	8.8.8.8	192.168.2.4	0x39c2	No error (0)	api.ipify.org.herokudns.com		3.220.57.224	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:19:22.646457911 CET	8.8.8.8	192.168.2.4	0x39c2	No error (0)	api.ipify.org.herokudns.com		54.91.59.199	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:19:40.847109079 CET	8.8.8.8	192.168.2.4	0xc143	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:19:52.980617046 CET	8.8.8.8	192.168.2.4	0xaabb	No error (0)	api.ipify.org	api.ipify.org.herokudns.com		CNAME (Canonical name)	IN (0x0001)	false
Dec 9, 2022 10:19:52.980617046 CET	8.8.8.8	192.168.2.4	0xaabb	No error (0)	api.ipify.org.herokudns.com		54.91.59.199	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:19:52.980617046 CET	8.8.8.8	192.168.2.4	0xaabb	No error (0)	api.ipify.org.herokudns.com		3.220.57.224	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:19:52.980617046 CET	8.8.8.8	192.168.2.4	0xaabb	No error (0)	api.ipify.org.herokudns.com		3.232.242.170	A (IP address)	IN (0x0001)	false

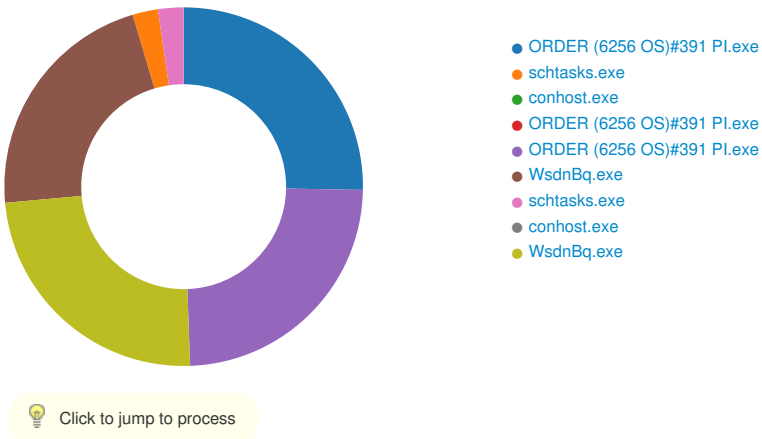
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Dec 9, 2022 10:19:52.980617046 CET	8.8.8.8	192.168.2.4	0xaabb	No error (0)	api.ipify.org.herokudns.com		52.20.78.240	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:19:53.034867048 CET	8.8.8.8	192.168.2.4	0x1a60	No error (0)	api.ipify.org	api.ipify.org.herokudns.com		CNAME (Canonical name)	IN (0x0001)	false
Dec 9, 2022 10:19:53.034867048 CET	8.8.8.8	192.168.2.4	0x1a60	No error (0)	api.ipify.org.herokudns.com		3.220.57.224	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:19:53.034867048 CET	8.8.8.8	192.168.2.4	0x1a60	No error (0)	api.ipify.org.herokudns.com		54.91.59.199	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:19:53.034867048 CET	8.8.8.8	192.168.2.4	0x1a60	No error (0)	api.ipify.org.herokudns.com		3.232.242.170	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:19:53.034867048 CET	8.8.8.8	192.168.2.4	0x1a60	No error (0)	api.ipify.org.herokudns.com		52.20.78.240	A (IP address)	IN (0x0001)	false
Dec 9, 2022 10:20:16.888513088 CET	8.8.8.8	192.168.2.4	0x7df	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- api.ipify.org
- api.telegram.org

Statistics

Behavior



System Behavior

Analysis Process: ORDER (6256 OS)#391 PI.exe PID: 1688, Parent PID: 3528

General

Target ID:	0
Start time:	10:18:58
Start date:	09/12/2022

Path:	C:\Users\user\Desktop\ORDER (6256 OS)#391 PI.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\ORDER (6256 OS)#391 PI.exe
Imagebase:	0xb20000
File size:	873472 bytes
MD5 hash:	19081EF2A08F678A3203B29124043C41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000000.00000002.343033622.0000000003FC9000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D62CF06	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	6D62CF06	unknown
C:\Users\user\AppData\Roaming\WsdnBq.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C471E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpF47D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C477038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ORDER (6256 OS)#391 PI.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D93C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpF47D.tmp	success or wait	1	6C476A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\WsdnBq.exe	0	873472	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 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 fd 4a fd 63 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 50 00 00 4a 0d 00 00 08 00 00 00 00 00 00 fd 68 0d 00 00 20 00 00 00 fd 0d 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 0d 00 00 02 00 00 00 00 00 00 02 00 40 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.$PELJcPJh @ @	success or wait	1	6C471B4F	WriteFile
C:\Users\user\AppData\Local\Temp\tmpF47D.tmp	0	1639	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?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> </RegistrationIn	success or wait	1	6C471B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ORDER (6256 OS)#391 PI.exe.log	0	1216	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 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 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 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6D93C907	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	6D605705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D605705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D60CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D5603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D605705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D605705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C471B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C471B4F	ReadFile
C:\Users\user\Desktop\ORDER (6256 OS)#391 PI.exe	unknown	873472	success or wait	1	6C471B4F	ReadFile

Analysis Process: schtasks.exe PID: **5964**, Parent PID: **1688**

General

Target ID:	1
Start time:	10:19:15
Start date:	09/12/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\WsdnBq" /XML "C:\Users\user\AppData\Local\Temp\tmpF47D.tmp
Imagebase:	0x10b0000
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\tmpF47D.tmp	unknown	2	success or wait	1	10BAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpF47D.tmp	unknown	1640	success or wait	1	10BABD9	ReadFile

Analysis Process: conhost.exe PID: **2236**, Parent PID: **5964**

General

Target ID:	2
Start time:	10:19:15
Start date:	09/12/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
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: ORDER (6256 OS)#391 PI.exe PID: **5052**, Parent PID: **1688**

General

Target ID:	3
Start time:	10:19:16
Start date:	09/12/2022
Path:	C:\Users\user\Desktop\ORDER (6256 OS)#391 PI.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x320000
File size:	873472 bytes
MD5 hash:	19081EF2A08F678A3203B29124043C41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: ORDER (6256 OS)#391 PI.exe PID: **1948**, Parent PID: **1688**

General

Target ID:	4
Start time:	10:19:16
Start date:	09/12/2022
Path:	C:\Users\user\Desktop\ORDER (6256 OS)#391 PI.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x860000
File size:	873472 bytes

MD5 hash:	19081EF2A08F678A3203B29124043C41
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: 00000004.00000002.565934222.0000000002C20000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000004.00000000.334155357.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D62CF06	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	6D62CF06	unknown
C:\Users\user\AppData\Local\Temp\tmp189D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C477038	GetTempFileNameW

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	6D605705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D605705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D60CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D5603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D605705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D605705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C471B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C471B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	49152	success or wait	1	6C471B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C471B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\ca8b3b75-86f2-4edb-b016-ef7ebe8beb9b	unknown	4096	success or wait	1	6C471B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C471B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C471B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C471B4F	ReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: WsdnBq.exe PID: **6004**, Parent PID: **1088**

General

Target ID:	5
Start time:	10:19:17
Start date:	09/12/2022
Path:	C:\Users\user\AppData\Roaming\WsdnBq.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\WsdnBq.exe
Imagebase:	0x8f0000
File size:	873472 bytes
MD5 hash:	19081EF2A08F678A3203B29124043C41
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 31%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D62CF06	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	6D62CF06	unknown
C:\Users\user\AppData\Local\Temp\tmp645E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C477038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\WsdnBq.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D93C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp645E.tmp	success or wait	1	6C476A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp645E.tmp	0	1639	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?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> </RegistrationIn	success or wait	1	6C471B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\WsdnBq.exe.log	0	1216	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 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 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 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6D93C907	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	6D605705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D605705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D60CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D5603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D605705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D605705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C471B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C471B4F	ReadFile

Analysis Process: schtasks.exe PID: **2224**, Parent PID: **6004**

General

Target ID:	6
Start time:	10:19:43
Start date:	09/12/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\WsdnBq" /XML "C:\Users\user\AppData\Local\Temp\tmp645E.tmp
Imagebase:	0x10b0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	false
Has administrator privileges:	false
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\tmp645E.tmp	unknown	2	success or wait	1	10BAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp645E.tmp	unknown	1640	success or wait	1	10BABD9	ReadFile

Analysis Process: conhost.exe PID: **1496**, Parent PID: **2224**

General

Target ID:	7
Start time:	10:19:43
Start date:	09/12/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
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: WsdnBq.exe PID: **1328**, Parent PID: **6004**

General

Target ID:	8
Start time:	10:19:44
Start date:	09/12/2022
Path:	C:\Users\user\AppData\Roaming\WsdnBq.exe
Wow64 process (32bit):	true

Commandline:	{path}
Imagebase:	0xeb0000
File size:	873472 bytes
MD5 hash:	19081EF2A08F678A3203B29124043C41
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000002.566251641.00000000032BF000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D62CF06	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	6D62CF06	unknown
C:\Users\user\AppData\Local\Temp\tmp93A6.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C477038	GetTempFileNameW

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	6D605705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D605705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D60CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D5603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D605705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D605705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C471B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C471B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	49152	success or wait	1	6C471B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C471B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\ca8b3b75-86f2-4edb-b016-ef7ebe8beb9b	unknown	4096	success or wait	1	6C471B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C471B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C471B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C471B4F	ReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly