ID: 383969
Sample Name: ORDER.exe
Cookbook: default.jbs
Time: 13:23:53
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

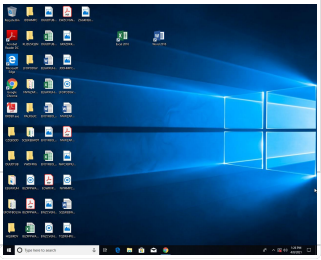
Analysis Report ORDER.exe

Overview

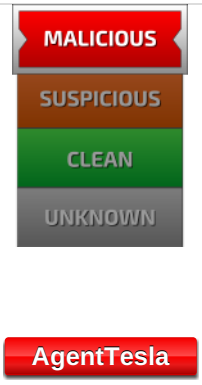
General Information

Sample Name:	ORDER.exe
Analysis ID:	383969
MD5:	351279e865038f0.
SHA1:	dd5ac844657d23..
SHA256:	dd7f52fd623b791..
Tags:	AgentTesla exe
Infos:	

Most interesting Screenshot:



Detection

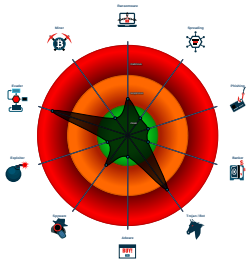


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Scheduled temp file…
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains method …
- .NET source code contains very larg…
- .NET source code references suspic…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Tries to detect sandboxes and other…

Classification



Startup

- **System is w10x64**
- ORDER.exe (PID: 5428 cmdline: 'C:\Users\user\Desktop\ORDER.exe' MD5: 351279E865038F0D4F1C34BE92C5FFCF)
  - schtasks.exe (PID: 240 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\uAtuTtfXv' /XML 'C:\Users\user\AppData\Local\Temp\tmp7391.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6072 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - ORDER.exe (PID: 6052 cmdline: {path} MD5: 351279E865038F0D4F1C34BE92C5FFCF)
    - dw20.exe (PID: 6088 cmdline: dw20.exe -x -s 756 MD5: 8D10DA8A3E11747E51F23C882C22BBC3)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "Telegram",
  "Chat id": "1422871978",
  "Chat URL": "https://api.telegram.org/bot1624300088:AAErstUTFyyeTcKqXZnnSnwnH27Dy-zCSTc/sendDocument"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.236134053.0000000003E01000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000006.00000002.249166242.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: ORDER.exe PID: 5428	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: ORDER.exe PID: 5428	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Source	Rule	Description	Author	Strings
Process Memory Space: ORDER.exe PID: 6052	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Unpacked PEs

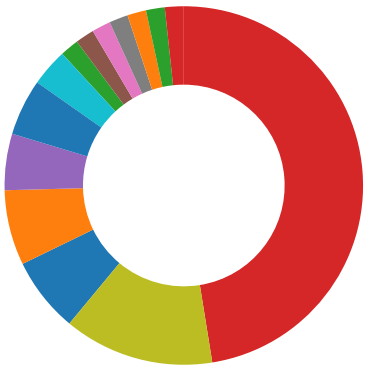
Source	Rule	Description	Author	Strings
1.2.ORDER.exe.4085d88.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
6.2.ORDER.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.ORDER.exe.40bbfa8.4.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.ORDER.exe.4085d88.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.ORDER.exe.3f9d948.3.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



- AV Detection
- Compliance
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

System Summary:

.NET source code contains very large array initializations

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

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

Boot Survival:

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

Malware Analysis System Evasion:

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion:

.NET source code references suspicious native API functions

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

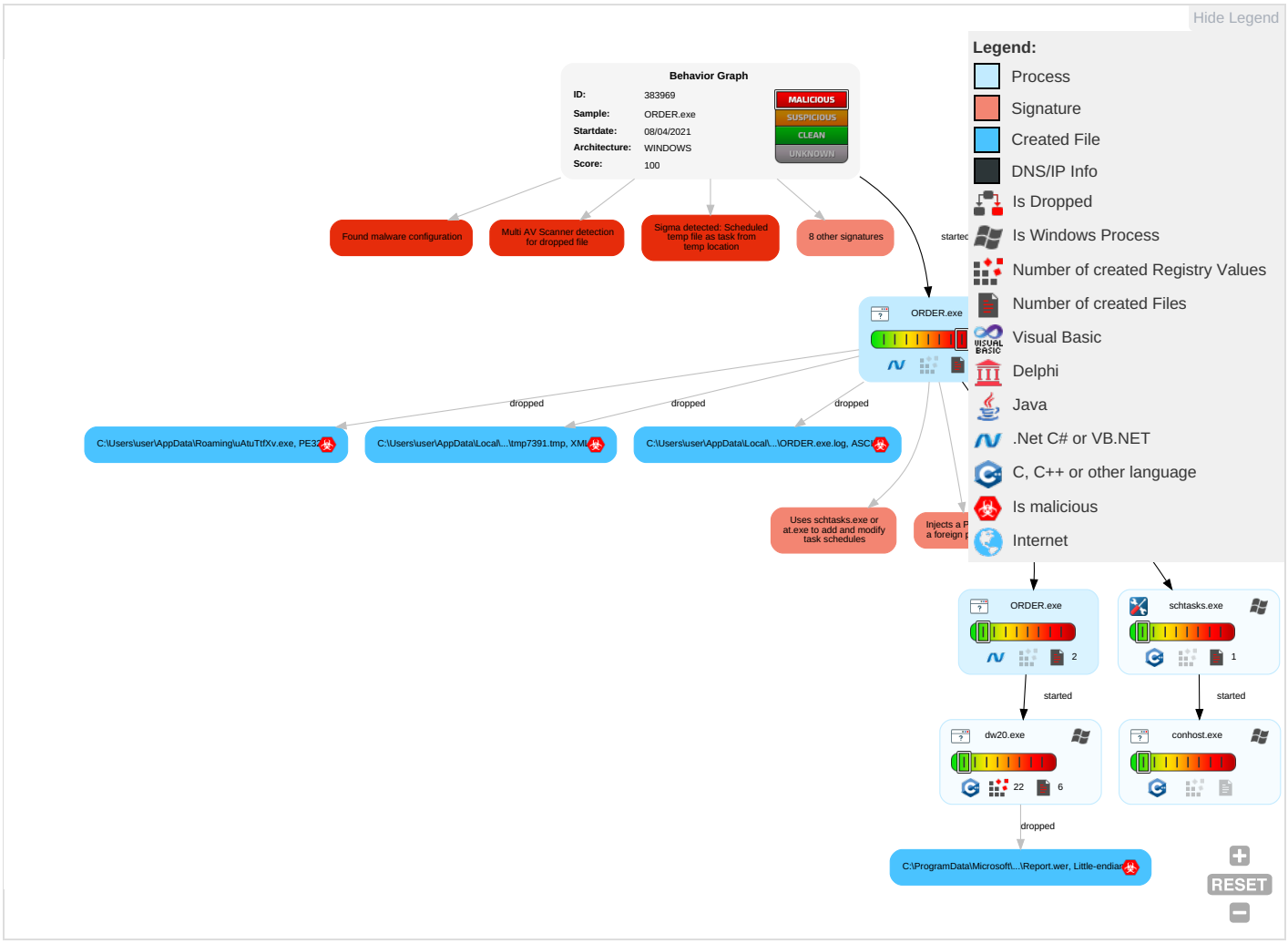
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 1 1 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 2 2 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop or Insecure Network Communicati
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Virtualization/Sandbox Evasion 4 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 t Redirect Pho Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 4 1	Security Account Manager	Remote System Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 t Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 1	NTDS	File and Directory Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	System Information Discovery 1 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicati
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Point

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.exe	39%	Virustotal		Browse
ORDER.exe	27%	ReversingLabs	Win32.Trojan.AgentTesla	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\uAtuTtfXv.exe	27%	ReversingLabs	Win32.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.2.ORDER.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cnJ	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.sajatypeworks.com4	0%	Avira URL Cloud	safe	
http://www.tiro.com3	0%	Avira URL Cloud	safe	
http://en.wDX	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/0	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.comF	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Verd	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnl-sw	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fonts.comic	0%	URL Reputation	safe	
http://www.fonts.comic	0%	URL Reputation	safe	
http://www.fonts.comic	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.founder.cl	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/W	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/W	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/W	0%	URL Reputation	safe	
http://www.sandoll.co.krtri	0%	Avira URL Cloud	safe	
http://www.fonts.comn%	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Gras	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/x	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/x	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/x	0%	URL Reputation	safe	
http://www.founder.com.cn/cn2	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/VerdJ	0%	Avira URL Cloud	safe	
http://www.fonts.com4	0%	Avira URL Cloud	safe	
http://www.fonts.com-u	0%	Avira URL Cloud	safe	
http://fontfabrik.com/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	ORDER.exe, 00000001.00000002.240280153.00000000065B2000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	ORDER.exe, 00000001.00000002.240280153.00000000065B2000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cnJ	ORDER.exe, 00000001.00000003.215719190.000000000535D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/bThe	ORDER.exe, 00000001.00000002.240280153.00000000065B2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com4	ORDER.exe, 00000001.00000003.213937928.000000000533B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com3	ORDER.exe, 00000001.00000003.214191426.000000000533B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://github.com/michel-pi/EasyBot.Net	ORDER.exe	false		high
http://www.fontbureau.com/designers?	ORDER.exe, 00000001.00000002.240280153.00000000065B2000.00000004.00000001.sdmp	false		high
http://en.wDX	ORDER.exe, 00000001.00000003.213511591.00000000012FD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/0	ORDER.exe, 00000001.00000003.217614683.0000000005324000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.tiro.com	ORDER.exe, 00000001.00000002.240280153.00000000065B2000.00000004.00000001.sdmp, ORDER.exe, 00000001.00000003.214219445.000000000533B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	ORDER.exe, 00000001.00000002.240280153.00000000065B2000.00000004.00000001.sdmp	false		high
http://www.tiro.comF	ORDER.exe, 00000001.00000003.214219445.000000000533B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	ORDER.exe, 00000001.00000002.240280153.00000000065B2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com	ORDER.exe, 00000001.00000003.216441928.0000000005330000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Verd	ORDER.exe, 00000001.00000003.217614683.0000000005324000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnl-sw	ORDER.exe, 00000001.00000003.215719190.000000000535D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersR	ORDER.exe, 00000001.00000003.220904273.0000000005329000.00000004.00000001.sdmp	false		high
http://www.sajatypeworks.com	ORDER.exe, 00000001.00000003.213978180.0000000005344000.00000004.00000001.sdmp, ORDER.exe, 00000001.00000002.240280153.0000000065B2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	ORDER.exe, 00000001.00000002.240280153.00000000065B2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	ORDER.exe, 00000001.00000002.240280153.00000000065B2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	ORDER.exe, 00000001.00000002.240280153.00000000065B2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	ORDER.exe, 00000001.00000002.240280153.00000000065B2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.comic	ORDER.exe, 00000001.00000003.213937928.000000000533B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	ORDER.exe, 00000001.00000002.240280153.00000000065B2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.com	ORDER.exe, 00000001.00000003.213937928.000000000533B000.00000004.00000001.sdmp	false		high
http://www.sandoll.co.kr	ORDER.exe, 00000001.00000002.240280153.00000000065B2000.00000004.00000001.sdmp, ORDER.exe, 00000001.00000003.215056921.0000000005329000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.cl	ORDER.exe, 00000001.00000003.215985763.0000000005324000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	ORDER.exe, 00000001.00000002.240280153.00000000065B2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	ORDER.exe, 00000001.00000002.240280153.00000000065B2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	ORDER.exe, 00000001.00000002.240280153.00000000065B2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	ORDER.exe, 00000001.00000002.236134053.0000000003E01000.00000004.00000001.sdmp, ORDER.exe, 00000006.00000002.249166242.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	ORDER.exe, 00000001.00000002.240280153.00000000065B2000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com	ORDER.exe, 00000001.00000002.240280153.00000000065B2000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/W	ORDER.exe, 00000001.00000003.217614683.0000000005324000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sandoll.co.krtri	ORDER.exe, 00000001.00000003.215056921.0000000005329000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.comn%	ORDER.exe, 00000001.00000003.213984328.000000000533B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.jiyu-kobo.co.jp/Gras	ORDER.exe, 00000001.00000003.217614683.0000000005324000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	ORDER.exe, 00000001.00000003.217614683.0000000005324000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.coma	ORDER.exe, 00000001.00000003.234693220.0000000005320000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	ORDER.exe, 00000001.00000002.240280153.00000000065B2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	ORDER.exe, 00000001.00000003.215985763.0000000005324000.00000004.00000001.sdmp, ORDER.exe, 00000001.00000003.215719190.000000000535D000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	ORDER.exe, 00000001.00000002.240280153.00000000065B2000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn	ORDER.exe, 00000001.00000003.216118395.000000000532B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/x	ORDER.exe, 00000001.00000003.217614683.0000000005324000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	ORDER.exe, 00000001.00000002.240280153.00000000065B2000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn2	ORDER.exe, 00000001.00000003.215719190.000000000535D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	ORDER.exe, 00000001.00000002.240280153.00000000065B2000.00000004.00000001.sdmp, ORDER.exe, 00000001.00000003.217614683.0000000005324000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	ORDER.exe, 00000001.00000002.240280153.00000000065B2000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/VerdJ	ORDER.exe, 00000001.00000003.217614683.0000000005324000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com4	ORDER.exe, 00000001.00000003.213937928.000000000533B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.telegram.org/bot1624300088:AAErstUTFyyeTcKqXZnnSnwnH27Dy-zCSTc/	ORDER.exe, 00000001.00000002.236134053.0000000003E01000.00000004.00000001.sdmp, ORDER.exe, 00000006.00000002.249166242.0000000000402000.00000040.00000001.sdmp	false		high
http://www.fonts.com-u	ORDER.exe, 00000001.00000003.213958029.000000000533B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://fontfabrik.com/	ORDER.exe, 00000001.00000003.214219445.000000000533B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383969
Start date:	08.04.2021
Start time:	13:23:53
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ORDER.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	31
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@8/6@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 23.54.113.53, 40.88.32.150, 104.42.151.234, 52.147.198.201, 13.88.21.125, 95.100.54.203, 20.82.210.154, 23.10.249.43, 23.10.249.26, 23.0.174.185, 23.0.174.200, 20.54.26.129, 104.43.193.48, 52.255.188.83, 13.64.90.137 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, skypedataprdcolwus15.cloudapp.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
13:24:51	API Interceptor	2x Sleep call for process: ORDER.exe modified
13:25:02	API Interceptor	1x Sleep call for process: dw20.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_ORDER.exe_a98c55928929b2832be98a97c3d2d245aa320_00000000_17f4f2e7\Report.wer	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	10352
Entropy (8bit):	3.7755754040059637
Encrypted:	false
SSDEEP:	96:45de7TM1r0zmVzxWs5h5pXI/+BHUHZopAnQ0DFH2EmSonj+wdOyWnEeVc1F9ZQbk:8de7Y1DDHPaPLk9MK/u7sBS274Itf
MD5:	116DA349623C4F9A9371F060A59BD64F
SHA1:	3A0775340DE08C0FCE8071BAA82EB7B326CA3022
SHA-256:	AF1F8B4EE10A591BB8D4F747CA6E1CD89BC1A168E3BB63D823254F5A90BCF7A4
SHA-512:	7EF096F0DFC7EF3AA6089688D90F5B7F9237CC3B5A2B2AF84EC3F69E39BE9463DA2B88ACFF3C7FE535468AB0598A8B747C0E4E195E95EE7619DDED572D5838EF
Malicious:	**true**
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.6.2.3.8.7.0.9.6.2.8.8.4.6.9.5.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.6.2.3.8.7.0.9.6.5.8.5.3.4.3.8.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.d.d.5.b.1.4.8.9.-.8.9.c.a.-.4.7.1.c.-.a.7.4.0.-.e.8.6.1.b.8.3.5.4.e.7.a.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.z.!.6.M...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.7.a.4.-.0.0.0.1.-.0.0.1.7.-.e.0.3.3.-.b.4.3.c.b.5.2.c.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.8.d.c.0.0.9.5.f.0.4.3.7.9.9.2.b.9.2.4.5.8.7.3.5.4.a.2.7.3.8.d.3.0.0.0.0.0.0.0.0.!.0.0.0.0.d.d.5.a.c.8.4.4.6.5.7.d.2.3.5.1.e.6.8.6.c.5.9.3.f.c.8.7.a.4.5.0.3.8.1.e.3.a.8.9.!.O.R.D.E.R...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.1././.0.4././.0.8.:.0.0.:.1.6.:.1.9.!.0.!.O.R.D.E.R...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.9.6.7.2.9.5.....T.a.r.g.e.t.A.s.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC42.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	7562
Entropy (8bit):	3.7059056723496213
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiGE6cP16YsB6tgmfo4T8SxSCp14nU1f5fIm:RrlsNiV6cP16YS6tgmfNYSx74n+f5l
MD5:	E848DB5E053961AD80EAACCC55EE5082
SHA1:	D68D6385562D9EBB81387D7FAF15EA6606F55B1A
SHA-256:	6DB4D2B3E08CB21DE99126C18DF4363CED175DC30F5FA31F2DA679F3928283B9
SHA-512:	40F8D02882C049E14ABAB06D5E7BC44A9B2A2879E2165F63C9C1E678A2CC26AF1429D4EC0406AF315D15A70138E245844B43D381DC934EAED1680D6C8D8F50(
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.0.5.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCE0.tmp.xml	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	XML 1.0 document, UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	4564
Entropy (8bit):	4.4884439745445075
Encrypted:	false
SSDEEP:	48:cvIwSD8zswJgtWI9YmWSC8Bc8fm8M4JFKffsJoFN+q8LJsDJCquud:uITf2fnSN7JFKXEsAJmJCquud
MD5:	4650AED76587B321F6B29D3D0355B0CA
SHA1:	F7F1369DCC1AA686097C0893C3C9A19E66687070
SHA-256:	11E3EF95D68B1E1441D982BB3FC6148E75D83458B904F4F4294A03925E1E8B3F
SHA-512:	4D891BA3A90458ED36C1FD162579AB641DA0C19BBD0760D469079CD8DED10BD76815C51098C4F9C7A1C461D3976F2C9FEB335B3283E4B88269FF144EDECDC11

C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCE0.tmp.xml	
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="937775" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\ORDER.exe.log	
Process:	C:\Users\user\Desktop\ORDER.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Temp\tmp7391.tmp	
Process:	C:\Users\user\Desktop\ORDER.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1642
Entropy (8bit):	5.185842204775607
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBKtn:cbh47TlNQ//rydbz9l3YODOLNdq3C
MD5:	C30B598C6019BB98F01CD42F85E8E8D9
SHA1:	3BF8BEDC801D372BAF2278B9F148A80882D50D6E
SHA-256:	0D3DDFCC3AD50DDFCA495CC209EC58A1C4AC43CB2AA28DAC786F15F4D0517706
SHA-512:	EC98195FACD8B18DB899FDF69A2BDE59B211DF150F60DA6CC2FC707D69936B5F0F835960AD48B720B389FF2C495C638D53E8DB81CB839929029801D32C58461
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\uAtuTtfXv.exe	
Process:	C:\Users\user\Desktop\ORDER.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	945152
Entropy (8bit):	7.733393625247205
Encrypted:	false
SSDEEP:	12288:FKXy1c0w2iNJn+oHxDZ3jKV/JyZ3LNFyzGx+5BXdfwkiJ2eb9B5eSiyyjK:cP1r+Sxd3jgYZ3RczOYZ1wfUwId8
MD5:	351279E865038F0D4F1C34BE92C5FFCF
SHA1:	DD5AC844657D2351E686C593FC87A450381E3A89
SHA-256:	DD7F52FD623B7913C7494ECEBAE45A9B4DD843B5A363652E3AB92DA9CDB3A691
SHA-512:	04771F68BB7901FC9B56C0813BA11AC247208B1A0FBECAFCA175E3416CF4290B5254062479A94D14B939FE62539917ED4F7DD3D78AA4E9BEC80480239764A010
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 27%
Reputation:	low

C:\Users\user\AppData\Roaming\uAtuTtfXv.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...SKn`.....0..v..... .....@.. ..... ..@.....O..... ..... ..H.....text....u... ...v..... ..`.rsrc.....x.....@..@.reloc..... .....j.....@..B.....H.....Y...:.....^..}.....(.....(....*..*..0..+.....,..{.....+.....,..{....o.....(....*..0.....(....s.....s....}.....s.... }.....s....}.....s....}.....s....}.....s....}.....s ...}.....s!...}.....{....o".....{....o#.....("....{.....o$.....{....o%....".Bs&...o'..&.{....o%....".Bs&...o'...&.{....o(....{.....o).....{....o(....{.....o).....{....o(....{.....o).....{....o(....{.....o).....{....o

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.733393625247205
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.exe
File size:	945152
MD5:	351279e865038f0d4f1c34be92c5ffcf
SHA1:	dd5ac844657d2351e686c593fc87a450381e3a89
SHA256:	dd7f52fd623b7913c7494ecebae45a9b4dd843b5a363652e3ab92da9cdb3a691
SHA512:	04771f68bb7901fc9b56c0813ba11ac247208b1a0fbecafca175e3416cf4290b5254062479a94d14b939fe62539917ed4f7dd3d78aa4e9bec80480239764a010
SSDEEP:	12288:FKXy1c0w2iNJn+oHxDZ3jKV/JyZ3LNFyzGx+5BXdfwkiJ2eb9B5eSiyyjK:cP1r+Sxd3jgYZ3RczOYZ1wfUwId8
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...SKn`.....0..v..... .....@.. .....@.....

File Icon

Icon Hash:	929296929e9e8eb2

Static PE Info

General

Entrypoint:	0x4b94fa
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x606E4B53 [Thu Apr 8 00:16:19 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
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]
mov dword ptr [eax+4Eh], edx
inc edi
or eax, 000A1A0Ah
add byte ptr [eax], al
add byte ptr [ecx+45h], cl
dec esi
inc esp
scasb
inc edx
pushad
add byte ptr [eax], 00000000h
add 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
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xb94a8	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xba000	0x2f0ac	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xea000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xb7518	0xb7600	False	0.907054149625	data	7.89896443713	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xba000	0x2f0ac	0x2f200	False	0.362421253316	data	6.2421551019	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xea000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xba2b0	0x709e	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0xc1350	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 318767104, next used block 117440512		
RT_ICON	0xd1b78	0x94a8	data		
RT_ICON	0xdb020	0x5488	data		
RT_ICON	0xe04a8	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 224, next used block 117440512		
RT_ICON	0xe46d0	0x25a8	data		
RT_ICON	0xe6c78	0x10a8	data		
RT_ICON	0xe7d20	0x988	data		
RT_ICON	0xe86a8	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xe8b10	0x84	data		
RT_VERSION	0xe8b94	0x32c	data		
RT_MANIFEST	0xe8ec0	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2018 - 2021
Assembly Version	3.1.0.5
InternalName	zM.exe
FileVersion	3.1.0.5
CompanyName	
LegalTrademarks	
Comments	
ProductName	Image Manager
ProductVersion	3.1.0.5
FileDescription	Image Manager
OriginalFilename	zM.exe

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 13:24:40.569474936 CEST	50200	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:24:40.588349104 CEST	53	50200	8.8.8.8	192.168.2.3
Apr 8, 2021 13:24:42.784682989 CEST	51281	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:24:42.797214031 CEST	53	51281	8.8.8.8	192.168.2.3
Apr 8, 2021 13:24:43.706543922 CEST	49199	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:24:43.718858004 CEST	53	49199	8.8.8.8	192.168.2.3
Apr 8, 2021 13:24:45.143517017 CEST	50620	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:24:45.156260014 CEST	53	50620	8.8.8.8	192.168.2.3
Apr 8, 2021 13:24:46.883788109 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:24:46.896325111 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 8, 2021 13:24:48.457182884 CEST	60152	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:24:48.469640017 CEST	53	60152	8.8.8.8	192.168.2.3
Apr 8, 2021 13:24:49.472404957 CEST	57544	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:24:49.488020897 CEST	53	57544	8.8.8.8	192.168.2.3
Apr 8, 2021 13:24:50.534167051 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:24:50.550154924 CEST	53	55984	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 13:24:51.457585096 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:24:51.471801996 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 8, 2021 13:24:57.920488119 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:24:57.933506966 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 8, 2021 13:25:03.651426077 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:25:03.664046049 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 8, 2021 13:25:04.704349995 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:25:04.719369888 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 8, 2021 13:25:05.349138021 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:25:05.362237930 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 8, 2021 13:25:10.124577999 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:25:10.173801899 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 8, 2021 13:25:12.177082062 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:25:12.189585924 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 8, 2021 13:25:13.210030079 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:25:13.222681999 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 8, 2021 13:25:16.184787035 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:25:16.196759939 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 8, 2021 13:25:27.971662998 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:25:27.990072966 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 8, 2021 13:25:34.350477934 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:25:34.369616032 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 8, 2021 13:25:43.725986004 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:25:43.751817942 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 8, 2021 13:25:45.549663067 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:25:45.561527014 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 8, 2021 13:25:46.346766949 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:25:46.359770060 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 8, 2021 13:25:47.424964905 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:25:47.436907053 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 8, 2021 13:25:48.470308065 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:25:48.482166052 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 8, 2021 13:25:51.655776978 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:25:51.668162107 CEST	53	54366	8.8.8.8	192.168.2.3
Apr 8, 2021 13:25:55.663841963 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:25:55.681936979 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 8, 2021 13:26:26.452462912 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:26:26.471427917 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 8, 2021 13:26:28.661109924 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:26:28.687755108 CEST	53	55435	8.8.8.8	192.168.2.3

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: ORDER.exe PID: 5428 Parent PID: 5696

General

Start time:	13:24:44
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\ORDER.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\ORDER.exe'
Imagebase:	0x760000
File size:	945152 bytes
MD5 hash:	351279E865038F0D4F1C34BE92C5FFCF
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: 00000001.00000002.236134053.0000000003E01000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	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	72FB60AC	unknown
C:\Users\user\AppData\Roaming\uAtuTtfXv.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	725080F	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp7391.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	12DB5B8	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\ORDER.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72FA34A7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp7391.tmp	success or wait	1	725149A	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\uAtuTtfXv.exe	unknown	945152	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 53 4b 6e 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 76 0b 00 00 f4 02 00 00 00 00 00 fa 94 0b 00 00 20 00 00 00 a0 0b 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 c0 0e 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...SKn`.......... ....0..v............... ....@.. ....@................	success or wait	1	7250B43	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp7391.tmp	unknown	1642	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 68 61 72 64 7a 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	7250B43	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\ORDER.exe.log	unknown	525	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 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 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 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 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 5c 35 34 64 39 34 34 62 33 63 61 30 65 61 31 31 38 38 64 37 30 30 66 62 64 38 30 38 39 37 32 36 62 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"	success or wait	1	7328A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Users\user\Desktop\ORDER.exe	unknown	945152	success or wait	1	7250B43	ReadFile

Analysis Process: schtasks.exe PID: 240 Parent PID: 5428

General

Start time:	13:24:54
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\uAtuTtfXv' /XML 'C:\Users\user\AppData\Local\Temp\tmp7391.tmp'
Imagebase:	0x8f0000
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\tmp7391.tmp	unknown	2	success or wait	1	8FAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp7391.tmp	unknown	1643	success or wait	1	8FABD9	ReadFile

Analysis Process: conhost.exe PID: 6072 Parent PID: 240

General

Start time:	13:24:54
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: ORDER.exe PID: 6052 Parent PID: 5428

General

Start time:	13:24:55
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\ORDER.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x510000
File size:	945152 bytes
MD5 hash:	351279E865038F0D4F1C34BE92C5FFCF

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000002.249166242.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	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	72FB60AC	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown

Analysis Process: dw20.exe PID: 6088 Parent PID: 6052

General

Start time:	13:24:55
Start date:	08/04/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
Wow64 process (32bit):	true
Commandline:	dw20.exe -x -s 756
Imagebase:	0x10000000
File size:	33936 bytes
MD5 hash:	8D10DA8A3E11747E51F23C882C22BBC3
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 Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis