

ID: 626340
Sample Name: NEW ORDER.exe
Cookbook: default.jbs
Time: 21:31:28
Date: 13/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report NEW ORDER.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Agenttesla 4
Yara Signatures 4
Memory Dumps 4
Unpacked PEs 5
Sigma Signatures 5
Snort Signatures 5
Joe Sandbox Signatures 6
AV Detection 6
Networking 6
System Summary 6
Boot Survival 6
Malware Analysis System Evasion 6
HIPS / PFW / Operating System Protection Evasion 6
Stealing of Sensitive Information 6
Remote Access Functionality 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 10
URLs 10
Domains and IPs 11
Contacted Domains 11
URLs from Memory and Binaries 11
World Map of Contacted IPs 15
Public IPs 15
General Information 15
Warnings 16
Simulations 16
Behavior and APIs 16
Joe Sandbox View / Context 16
IPs 16
Domains 16
ASNs 16
JA3 Fingerprints 16
Dropped Files 16
Created / dropped Files 16
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\NEW ORDER.exe.log 16
C:\Users\user\AppData\Local\Temp\tmp354B.tmp 17
C:\Users\user\AppData\Roaming\IrUpgWwdRBJK.exe 17
Static File Info 18
General 18
File Icon 18
Static PE Info 18
General 18
Entrypoint Preview 18
Data Directories 20
Sections 20
Resources 20
Imports 21
Version Infos 21
Network Behavior 21
Snort IDS Alerts 21
Network Port Distribution 21
TCP Packets 22
UDP Packets 22
DNS Queries 22
DNS Answers 22
SMTP Packets 22
Statistics 23
Behavior 23

Copyright Joe Security LLC 2022

System Behavior 23
Analysis Process: NEW ORDER.exePID: 7016, Parent PID: 5600 23
General 23
File Activities 24
File Created 24
File Deleted 24
File Written 24
File Read 25
Analysis Process: schtasks.exePID: 7120, Parent PID: 7016 26
General 26
File Activities 26
File Read 26
Analysis Process: conhost.exePID: 7128, Parent PID: 7120 26
General 26
Analysis Process: NEW ORDER.exePID: 3968, Parent PID: 7016 26
General 26
File Activities 27
File Created 27
File Read 27
Disassembly 28

Copyright Joe Security LLC 2022

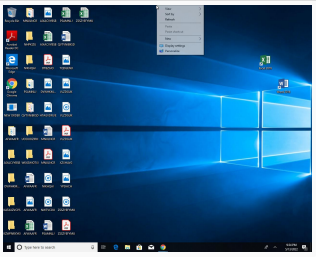
Windows Analysis Report

NEW ORDER.exe

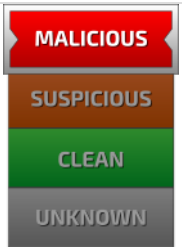
Overview

General Information

Sample Name:	NEW ORDER.exe
Analysis ID:	626340
MD5:	2ab185544e8686.
SHA1:	695efe1081e5b6..
SHA256:	ae376c158f4f8a1..
Tags:	exe
Infos:	



Detection



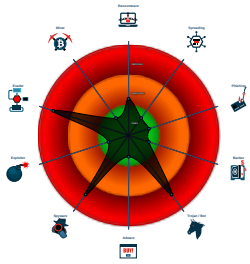
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Multi AV Scanner detection for drop…
- Snort IDS alert for network traffic
- Tries to steal Mail credentials (via fi…
- Initial sample is a PE file and has a…
- Tries to harvest and steal Putty / W…
- Tries to harvest and steal ftp login c…
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w10x64**
- NEW ORDER.exe (PID: 7016 cmdline: "C:\Users\user\Desktop\NEW ORDER.exe" MD5: 2AB185544E86862DAB6A5E7A4413C49F)
  - schtasks.exe (PID: 7120 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\IrUpgWwdRBJK" /XML "C:\Users\user\AppData\Local\Temp\tmp354B.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 7128 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - NEW ORDER.exe (PID: 3968 cmdline: {path} MD5: 2AB185544E86862DAB6A5E7A4413C49F)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "whford@focuzauto.com",
  "Password": "Gdn4ford@2016",
  "Host": "mail.focuzauto.com"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000000.486980862.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000000.486980862.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Copyright Joe Security LLC 2022

Source	Rule	Description	Author	Strings
00000000.00000002.505972636.000000000362F000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.505972636.000000000362F000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000003.00000002.698717283.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 13 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.NEW ORDER.exe.376bf08.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.NEW ORDER.exe.376bf08.4.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.NEW ORDER.exe.376bf08.4.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x30bd9:$s10: logins • 0x30646:$s11: credential • 0x2ccac:$g1: get_Clipboard • 0x2ccba:$g2: get_Keyboard • 0x2ccc7:$g3: get_Password • 0x2df77:$g4: get_CtrlKeyDown • 0x2df87:$g5: get_ShiftKeyDown • 0x2df98:$g6: get_AltKeyDown
3.0.NEW ORDER.exe.400000.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
3.0.NEW ORDER.exe.400000.4.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 20 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN AgentTesla Exfil Via SMTP - Source IP: 192.168.2.5 - Destination IP: 166.62.10.145

Timestamp:	192.168.2.5166.62.10.145497835872030171 05/13/22-21:33:25.240893
SID:	2030171
Source Port:	49783
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Win32/AgentTesla/OriginLogger Data Exfil via SMTP M2 - Source IP: 192.168.2.5 - Destination IP: 166.62.10.145

Timestamp:	192.168.2.5166.62.10.145497835872840032 05/13/22-21:33:25.240991
SID:	2840032
Source Port:	49783
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Win32/Agent Tesla SMTP Activity - Source IP: 192.168.2.5 - Destination IP: 166.62.10.145

Timestamp:	192.168.2.5166.62.10.145497835872839723 05/13/22-21:33:25.240893
SID:	2839723
Source Port:	49783
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

Copyright Joe Security LLC 2022

Joe Sandbox Signatures

AV Detection



Found malware configuration

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking



Snort IDS alert for network traffic

System Summary



Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

.NET source code contains very large array initializations

Boot Survival



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

Malware Analysis System Evasion



Yara detected AntiVM3

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

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

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

HIPS / PFW / Operating System Protection Evasion



Injects a PE file into a foreign processes

Stealing of Sensitive Information



Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

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

Remote Access Functionality

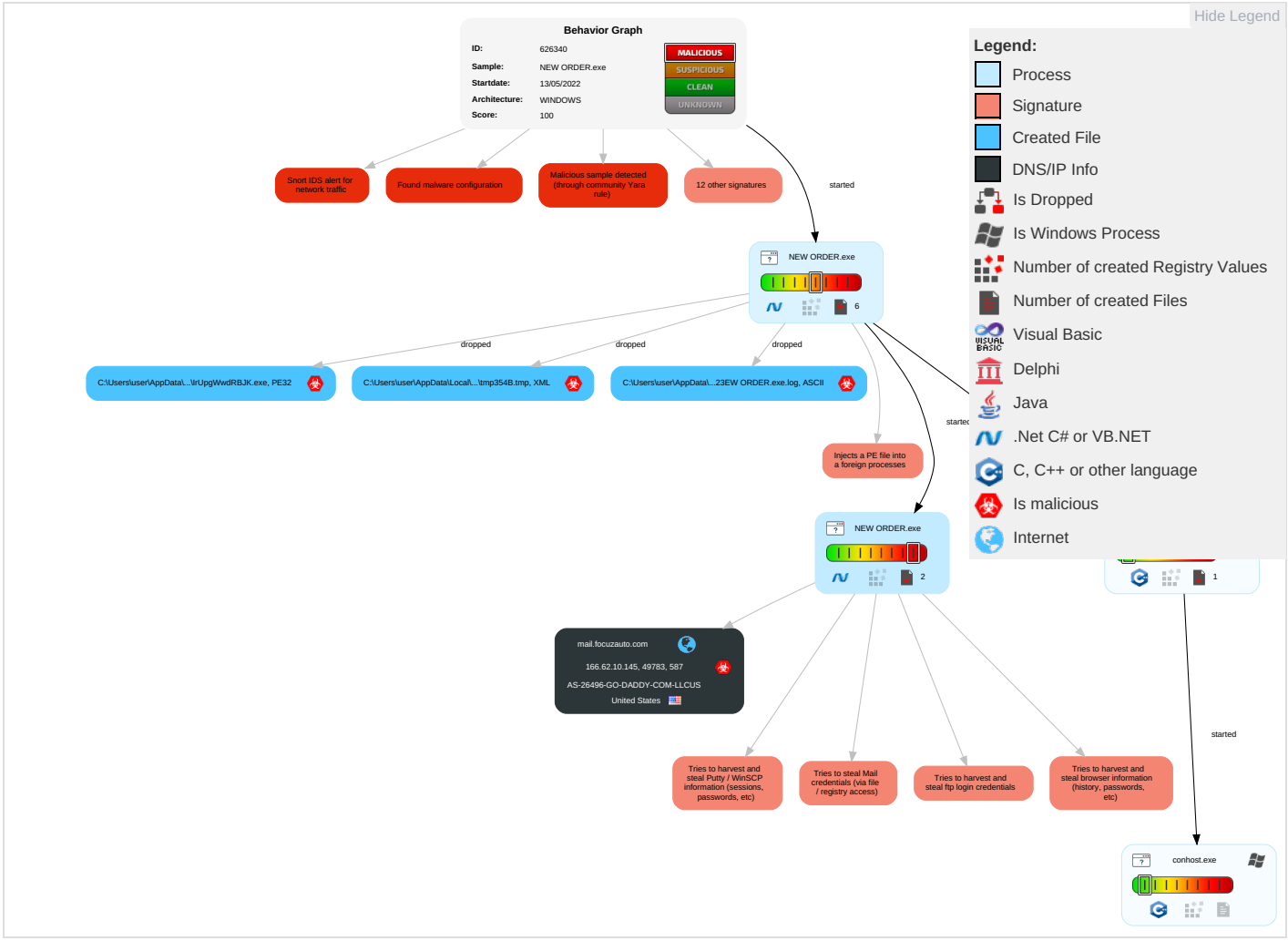


Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	1 Scheduled Task/Job	1 1 1 Process Injection	1 Masquerading	2 OS Credential Dumping	3 1 1 Security Software Discovery	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Scheduled Task/Job	1 Disable or Modify Tools	1 Credentials in Registry	1 Process Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 3 1 Virtualization/Sandbox Evasion	Security Account Manager	1 3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	2 Data from Local System	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 1 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Obfuscated Files or Information	Cached Domain Credentials	1 File and Directory 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	3 Software Packing	DCSync	1 1 4 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

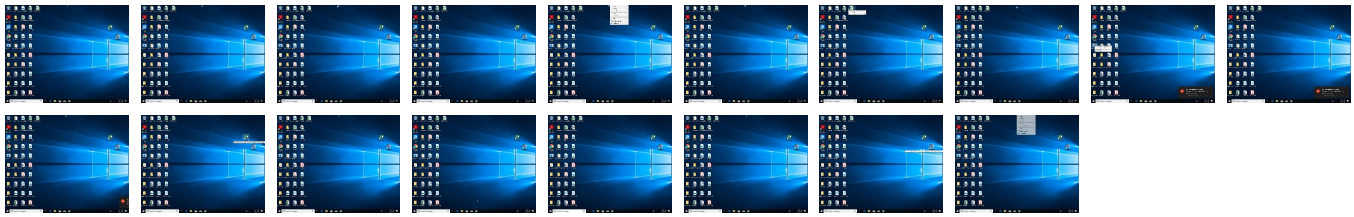
Behavior Graph



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	38%	Virustotal		Browse
NEW ORDER.exe	41%	ReversingLabs	Win32.Trojan.Injuke	
NEW ORDER.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\IrUpgWwdRBJK.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\IrUpgWwdRBJK.exe	41%	ReversingLabs	Win32.Trojan.Injuke	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.0.NEW ORDER.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.NEW ORDER.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.NEW ORDER.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.2.NEW ORDER.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.NEW ORDER.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.NEW ORDER.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File

Copyright Joe Security LLC 2022

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://mail.focuzauto.com	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.fontbureau.comessedm	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnt-bz	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.founder.c	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.sajatypeworks.comuctT/	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://www.fonts.comic	0%	URL Reputation	safe	
http://www.fontbureau.com%	0%	Avira URL Cloud	safe	
http://www.fontbureau.comcom	0%	URL Reputation	safe	
http://www.urwpp.de/	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	URL Reputation	safe	
http://www.fonts.comn	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://https://uLakVAQ46zx.org	0%	Avira URL Cloud	safe	
http://www.fontbureau.comrsiv	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.krF	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fonts.comc	0%	URL Reputation	safe	
http://nSfkEw.com	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.sandoll.co.krm	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kre	0%	URL Reputation	safe	
http://www.fontbureau.comtoo_	0%	Avira URL Cloud	safe	
http://www.tiro.comtn	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.fontbureau.comasva	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.fontbureau.comm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.sajatypeworks.coma-d	0%	URL Reputation	safe	
http://www.fontbureau.commA	0%	Avira URL Cloud	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.fontbureau.comFf	0%	Avira URL Cloud	safe	
http://www.fontbureau.comals	0%	URL Reputation	safe	
http://www.tiro.comc	0%	URL Reputation	safe	
http://www.founder.com.cn/cnu-e	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.focuzauto.com	166.62.10.145	true	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	NEW ORDER.exe, 00000003.00000002.705211244.0000000002A91000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	NEW ORDER.exe, 00000000.00000002.510314363.00000000067F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://mail.focuzauto.com	NEW ORDER.exe, 00000003.00000002.705613036.0000000002DDE000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	NEW ORDER.exe, 00000000.00000002.510314363.00000000067F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	NEW ORDER.exe, 00000000.00000002.510314363.00000000067F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comessedm	NEW ORDER.exe, 00000000.00000003.450299640.00000000055A9000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	NEW ORDER.exe, 00000000.00000002.510314363.00000000067F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cnt-bz	NEW ORDER.exe, 00000000.00000003.442016798.00000000055DD000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	NEW ORDER.exe, 00000000.00000002.510314363.00000000067F2000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.439415514.00000000055BB000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.439273001.00000000055BB000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.439377058.00000000055BB000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.439307136.00000000055BB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	NEW ORDER.exe, 00000000.00000002.510314363.00000000067F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.c	NEW ORDER.exe, 00000000.00000003.442354972.00000000055A4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.goodfont.co.kr	NEW ORDER.exe, 00000000.00000002.510314363.00000000067F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

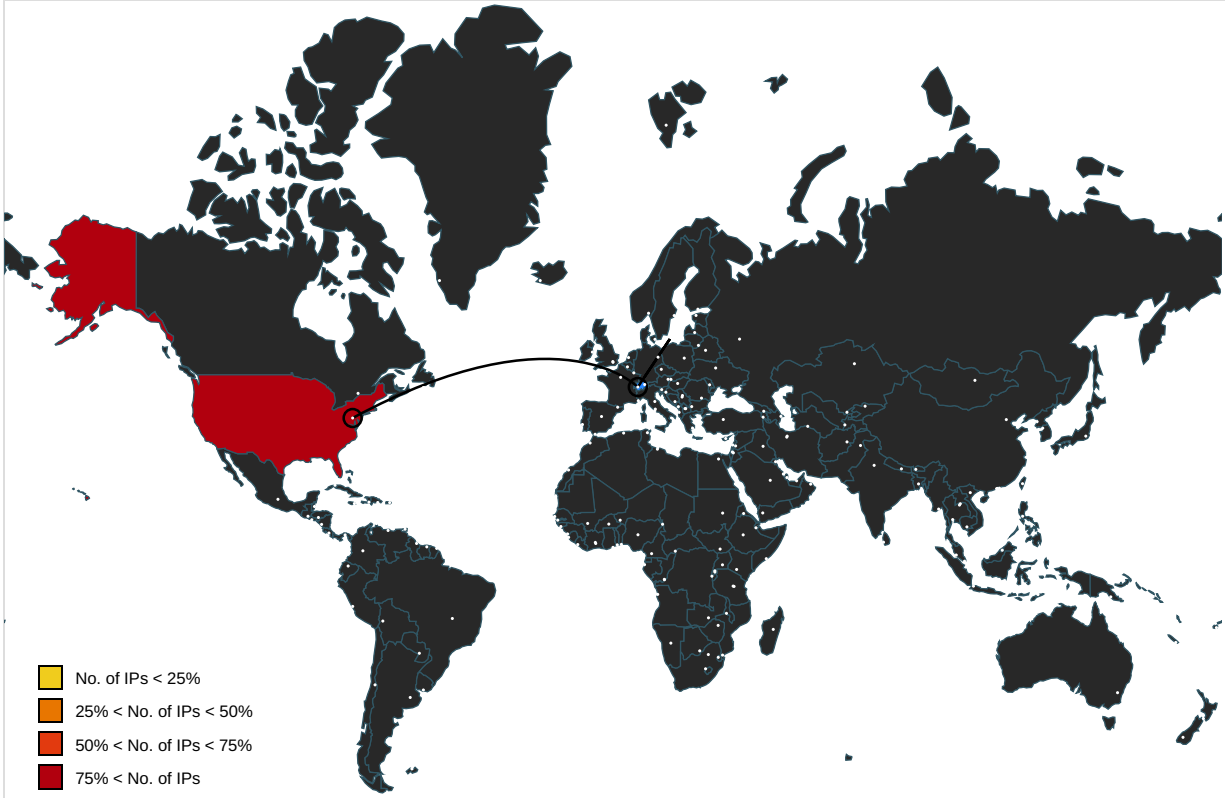
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.comuctT/	NEW ORDER.exe, 00000000.00000003.438584464.00000000055BB000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.438211868.00000000055BB000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.438422766.00000000055BB000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.438358460.00000000055BB000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.438304023.00000000055BB000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.438727968.00000000055BB000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.438654430.00000000055BB000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.438617797.00000000055BB000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.438259990.00000000055BB000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.438397273.00000000055BB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	NEW ORDER.exe, 00000000.00000003.438584464.00000000055BB000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000002.510314363.00000000067F2000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.438211868.00000000055BB000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.438422766.00000000055BB000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.438358460.00000000055BB000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.438304023.00000000055BB000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.438617797.00000000055BB000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.438259990.00000000055BB000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.438397273.00000000055BB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	NEW ORDER.exe, 00000000.00000002.510314363.00000000067F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	NEW ORDER.exe, 00000000.00000002.510314363.00000000067F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	NEW ORDER.exe, 00000000.00000002.510314363.00000000067F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	NEW ORDER.exe, 00000000.00000002.510314363.00000000067F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.comic	NEW ORDER.exe, 00000000.00000003.438584464.00000000055BB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com%	NEW ORDER.exe, 00000000.00000003.450299640.00000000055A9000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.comcom	NEW ORDER.exe, 00000000.00000003.450299640.00000000055A9000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.de/	NEW ORDER.exe, 00000000.00000003.450299640.00000000055A9000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	NEW ORDER.exe, 00000003.00000002.705211244.0000000002A91000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.comn	NEW ORDER.exe, 00000000.00000003.438617797.00000000055BB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	NEW ORDER.exe, 00000000.00000002.510314363.00000000067F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://uLakVAQ46zx.org	NEW ORDER.exe, 00000003.00000002.705598159.0000000002DD8000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comrsiv	NEW ORDER.exe, 00000000.00000003.450299640.00000000055A9000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	NEW ORDER.exe, 00000000.00000003.438617797.00000000055BB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	NEW ORDER.exe, 00000000.00000002.510314363.00000000067F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sandoll.co.krF	NEW ORDER.exe, 00000000.00000003.440601923.00000000055A6000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	NEW ORDER.exe, 00000000.00000002.510314363.00000000067F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.de	NEW ORDER.exe, 00000000.00000003.450299640.00000000055A9000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	NEW ORDER.exe, 00000000.00000002.510314363.00000000067F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	NEW ORDER.exe, 00000000.00000002.491114236.0000000002611000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	NEW ORDER.exe, 00000000.00000002.510314363.00000000067F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	NEW ORDER.exe, 00000000.00000002.510314363.00000000067F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	NEW ORDER.exe, 00000000.00000002.510314363.00000000067F2000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000002.509460420.00000000055A0000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.comc	NEW ORDER.exe, 00000000.00000003.438584464.00000000055BB000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.438817122.00000000055BB000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.438727968.00000000055BB000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.438654430.00000000055BB000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.438617797.00000000055BB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://nSfkEw.com	NEW ORDER.exe, 00000003.00000002.705211244.0000000002A91000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	NEW ORDER.exe, 00000003.00000002.705211244.0000000002A91000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sandoll.co.krm	NEW ORDER.exe, 00000000.00000003.440601923.00000000055A6000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.kre	NEW ORDER.exe, 00000000.00000003.440601923.00000000055A6000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comtoo_	NEW ORDER.exe, 00000000.00000003.449593906.00000000055AA000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.449121587.00000000055A9000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.tiro.comtn	NEW ORDER.exe, 00000000.00000003.439307136.00000000055BB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comd	NEW ORDER.exe, 00000000.00000003.449593906.00000000055AA000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.449121587.00000000055A9000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comasva	NEW ORDER.exe, 00000000.00000002.509460420.00000000055A0000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	NEW ORDER.exe, 00000000.00000002.510314363.00000000067F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	NEW ORDER.exe, 00000000.00000003.442354972.00000000055A4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	NEW ORDER.exe, 00000000.00000002.510314363.00000000067F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn	NEW ORDER.exe, 00000000.00000003.442035271.00000000055A4000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000002.510314363.00000000067F2000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.442016798.00000000055DD000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.442354972.00000000055A4000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.442490931.00000000055AB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	NEW ORDER.exe, 00000000.00000002.510314363.00000000067F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/cabarga.html	NEW ORDER.exe, 00000000.00000003.449795160.00000000055D5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comm	NEW ORDER.exe, 00000000.00000003.450299640.00000000055A9000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	NEW ORDER.exe, 00000000.00000002.510314363.00000000067F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.coma-d	NEW ORDER.exe, 00000000.00000003.438584464.00000000055BB000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.438211868.00000000055BB000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.438422766.00000000055BB000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.438358460.00000000055BB000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.438304023.00000000055BB000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.438617797.00000000055BB000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.438259990.00000000055BB000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.438397273.00000000055BB000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.438640795.00000000055C4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.commA	NEW ORDER.exe, 00000000.00000002.509460420.00000000055A0000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.como	NEW ORDER.exe, 00000000.00000003.449121587.00000000055A9000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	NEW ORDER.exe, 00000000.00000002.510314363.00000000067F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comFf	NEW ORDER.exe, 00000000.00000003.449593906.00000000055AA000.00000004.00000800.00020000.00000000.sdmp, NEW ORDER.exe, 00000000.00000003.449121587.00000000055A9000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comals	NEW ORDER.exe, 00000000.00000003.450299640.00000000055A9000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.comc	NEW ORDER.exe, 00000000.00000003.439377058.00000000055BB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cnu-e	NEW ORDER.exe, 00000000.00000003.442016798.00000000055DD000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
166.62.10.145	mail.focuzauto.com	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626340
Start date and time: 13/05/202221:31:28	2022-05-13 21:31:28 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 29s
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:	16
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

Copyright Joe Security LLC 2022

Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@6/3@1/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 98% • 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): audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 52.242.101.226
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, client.wns.windows.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, ctldl.windowsupdate.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com, glb.sls.prod.dcat.dsp.trafficmanager.net
- 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
21:32:56	API Interceptor	583x 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:\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:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F F8
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Temp\tmp354B.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):	1649
Entropy (8bit):	5.175352009521638
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/a7hTlNMFpH/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBBtn:cbhC7ZlNQF/rydbz9I3YODOLNdq3h
MD5:	27C0A47A8667AD260CA88339DC36059E
SHA1:	4539B9163F21FEE7DA3590850413B7B328F71358
SHA-256:	B031F195C17D439382C9FBA518948E3DAF59044D179D306ECF68A7A3FCA0F321
SHA-512:	82F6368DDA23B99CF5C0297B6248B1B51BFC78E9C1BBD70EEE0A959E4B92A04520F008545F422E045BEC0CB203F1AB9F1145E5D8A9FE8E50580384D802010651
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>t

C:\Users\user\AppData\Roaming\IrUpgWwdRBJK.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):	804864
Entropy (8bit):	7.841092667906191
Encrypted:	false
SSDEEP:	24576:Uk6jSIPaetDssX/qOWCSPr926SWzZJb9K:OjvPPbPixE6SwZN9
MD5:	2AB185544E86862DAB6A5E7A4413C49F
SHA1:	695EFE1081E5B65894132E870F882B587AD4DFCE
SHA-256:	AE376C158F4F8A123CA19B3FE6C96A158C8F7F88257CF07DE7987B33D376ACB2
SHA-512:	AD21A66E7CDE53A9F8E3DCB2951C1DF32ED7875F182FAE66F8E4123FE5A60A7B78CAD3B1CFCBE9F68D012EA22773691E882C5D57753A0D4F9AD373ACA61F44B7
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 41%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L..._I~b.....P..>.....\.. ...`....@.. ..... ..@.....4\..O....`..... ....H.....text....<... ...>..... ..`.rsrc.....`.....@.....@..@.rel oc.....F.....@..B.....h\.....H.....Y...Z.....`.....(....*&..(....*.s.....s .....s!.....s".....s#.....*...0.....~....o$....+..*.0..... .....~....o%....+..*.0.....~....o&....+..*.0.....~....o'....+..*.0.....~....o(...+..*.0..<.....~.....().....,!r...p....(*...o+...s,.....~.....+..*.0.....~.....+..*".....*.0..&.....(....r+..p~....o-...(.....t$....+..*Vs....(/...t.....*..(0...*.0.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.841092667906191
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:	804864
MD5:	2ab185544e86862dab6a5e7a4413c49f
SHA1:	695efe1081e5b65894132e870f882b587ad4dfce
SHA256:	ae376c158f4f8a123ca19b3fe6c96a158c8f7f88257cf07de7987b33d376acb2
SHA512:	ad21a66e7cde53a9f8e3dcb2951c1df32ed7875f182fae66f8e4123fe5a60a7b78cad3b1cfcbe9f68d012ea22773691e882c5d57753a0d4f9ad373aca61f44b7
SSDEEP:	24576:Uk6jSIPaetDssX/qOWCSPr926SWzZJb9K:OjvPPbPixE6SwZN9
TLSH:	550502153B6D7D12E6ABCB352255C1448AB0ECAF7C33E12B7E933C9F284DB5192A0971
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L..._I~b.....P..>.....\... ...`....@.. .....@.....

File Icon



Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4c5c86
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:	0x627E6C5F [Fri May 13 14:34:07 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
or al, byte ptr [eax+00h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [esi], cl
inc eax
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
adc byte ptr [eax+00h], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax+eax*2], cl
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
adc dword ptr [eax+00h], eax
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xc5c34	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc6000	0x5a4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xc8000	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	0xc3cb4	0xc3e00	False	0.897781888162	data	7.8467316034	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xc6000	0x5a4	0x600	False	0.419270833333	data	4.07653212502	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc8000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xc6090	0x314	data		
RT_MANIFEST	0xc63b4	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

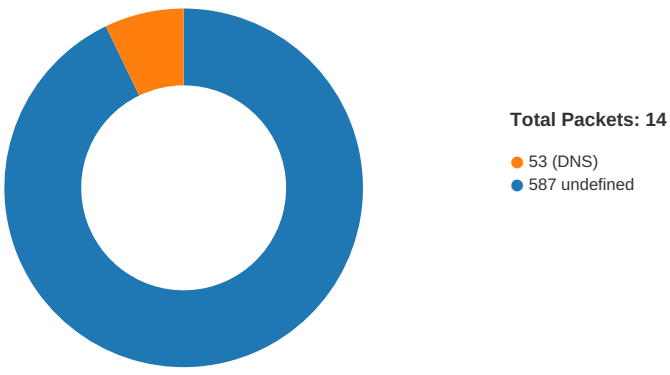
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2017
Assembly Version	1.0.0.0
InternalName	73tNI.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	Coffee Shop
ProductVersion	1.0.0.0
FileDescription	Coffee Shop
OriginalFilename	73tNI.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.5166.62.10.145 497835872030171 05/13/22- 21:33:25.240893	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49783	587	192.168.2.5	166.62.10.145
192.168.2.5166.62.10.145 497835872840032 05/13/22- 21:33:25.240991	TCP	2840032	ETPRO TROJAN Win32/AgentTesla/OriginLogger Data Exfil via SMTP M2	49783	587	192.168.2.5	166.62.10.145
192.168.2.5166.62.10.145 497835872839723 05/13/22- 21:33:25.240893	TCP	2839723	ETPRO TROJAN Win32/Agent Tesla SMTP Activity	49783	587	192.168.2.5	166.62.10.145

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2022 21:33:23.123352051 CEST	49783	587	192.168.2.5	166.62.10.145
May 13, 2022 21:33:23.375611067 CEST	587	49783	166.62.10.145	192.168.2.5
May 13, 2022 21:33:23.375829935 CEST	49783	587	192.168.2.5	166.62.10.145
May 13, 2022 21:33:23.641664028 CEST	587	49783	166.62.10.145	192.168.2.5
May 13, 2022 21:33:23.645809889 CEST	49783	587	192.168.2.5	166.62.10.145
May 13, 2022 21:33:23.898304939 CEST	587	49783	166.62.10.145	192.168.2.5
May 13, 2022 21:33:23.899597883 CEST	49783	587	192.168.2.5	166.62.10.145
May 13, 2022 21:33:24.152364969 CEST	587	49783	166.62.10.145	192.168.2.5
May 13, 2022 21:33:24.153141975 CEST	49783	587	192.168.2.5	166.62.10.145
May 13, 2022 21:33:24.419075966 CEST	587	49783	166.62.10.145	192.168.2.5
May 13, 2022 21:33:24.420389891 CEST	49783	587	192.168.2.5	166.62.10.145
May 13, 2022 21:33:24.672796011 CEST	587	49783	166.62.10.145	192.168.2.5
May 13, 2022 21:33:24.674534082 CEST	49783	587	192.168.2.5	166.62.10.145
May 13, 2022 21:33:24.967492104 CEST	587	49783	166.62.10.145	192.168.2.5
May 13, 2022 21:33:24.985084057 CEST	587	49783	166.62.10.145	192.168.2.5
May 13, 2022 21:33:24.985897064 CEST	49783	587	192.168.2.5	166.62.10.145
May 13, 2022 21:33:25.238105059 CEST	587	49783	166.62.10.145	192.168.2.5
May 13, 2022 21:33:25.238184929 CEST	587	49783	166.62.10.145	192.168.2.5
May 13, 2022 21:33:25.240892887 CEST	49783	587	192.168.2.5	166.62.10.145
May 13, 2022 21:33:25.240991116 CEST	49783	587	192.168.2.5	166.62.10.145
May 13, 2022 21:33:25.242198944 CEST	49783	587	192.168.2.5	166.62.10.145
May 13, 2022 21:33:25.242266893 CEST	49783	587	192.168.2.5	166.62.10.145
May 13, 2022 21:33:25.493294001 CEST	587	49783	166.62.10.145	192.168.2.5
May 13, 2022 21:33:25.494291067 CEST	587	49783	166.62.10.145	192.168.2.5
May 13, 2022 21:33:25.510797977 CEST	587	49783	166.62.10.145	192.168.2.5
May 13, 2022 21:33:25.659816980 CEST	49783	587	192.168.2.5	166.62.10.145

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2022 21:33:23.062099934 CEST	62466	53	192.168.2.5	8.8.8.8
May 13, 2022 21:33:23.092401028 CEST	53	62466	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 13, 2022 21:33:23.062099934 CEST	192.168.2.5	8.8.8.8	0x9a58	Standard query (0)	mail.focuz auto.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 13, 2022 21:33:23.092401028 CEST	8.8.8.8	192.168.2.5	0x9a58	No error (0)	mail.focuz auto.com		166.62.10.145	A (IP address)	IN (0x0001)

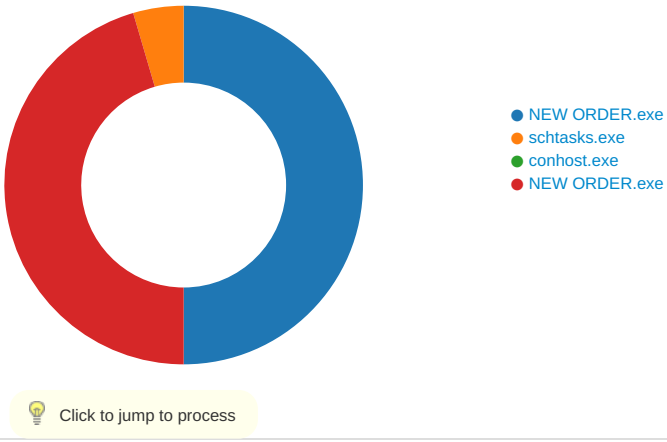
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 13, 2022 21:33:23.641664028 CEST	587	49783	166.62.10.145	192.168.2.5	220-sg2plcpnl0119.prod.sin2.secureserver.net ESMTP Exim 4.94.2 #2 Fri, 13 May 2022 12:33:23 -0700 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 13, 2022 21:33:23.645809889 CEST	49783	587	192.168.2.5	166.62.10.145	EHLO 701188
May 13, 2022 21:33:23.898304939 CEST	587	49783	166.62.10.145	192.168.2.5	250-sg2plcpnl0119.prod.sin2.secureserver.net Hello 701188 [84.17.52.36] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-CHUNKING 250-STARTTLS 250-SMTPUTF8 250 HELP

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 13, 2022 21:33:23.899597883 CEST	49783	587	192.168.2.5	166.62.10.145	AUTH login d2hmb3JkQGZvY3V6YXV0by5jb20=
May 13, 2022 21:33:24.152364969 CEST	587	49783	166.62.10.145	192.168.2.5	334 UGFzc3dvcmQ6
May 13, 2022 21:33:24.419075966 CEST	587	49783	166.62.10.145	192.168.2.5	235 Authentication succeeded
May 13, 2022 21:33:24.420389891 CEST	49783	587	192.168.2.5	166.62.10.145	MAIL FROM:<whford@focuzauto.com>
May 13, 2022 21:33:24.672796011 CEST	587	49783	166.62.10.145	192.168.2.5	250 OK
May 13, 2022 21:33:24.674534082 CEST	49783	587	192.168.2.5	166.62.10.145	RCPT TO:<obtxxxtf@gmail.com>
May 13, 2022 21:33:24.985084057 CEST	587	49783	166.62.10.145	192.168.2.5	250 Accepted
May 13, 2022 21:33:24.985897064 CEST	49783	587	192.168.2.5	166.62.10.145	DATA
May 13, 2022 21:33:25.238184929 CEST	587	49783	166.62.10.145	192.168.2.5	354 Enter message, ending with "." on a line by itself
May 13, 2022 21:33:25.242266893 CEST	49783	587	192.168.2.5	166.62.10.145	.
May 13, 2022 21:33:25.510797977 CEST	587	49783	166.62.10.145	192.168.2.5	250 OK id=1npb2T-007rzz-BE

Statistics

Behavior



System Behavior

Analysis Process: NEW ORDER.exe PID: **7016**, Parent PID: **5600**

General

Target ID:	0
Start time:	21:32:42
Start date:	13/05/2022
Path:	C:\Users\user\Desktop\NEW ORDER.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\NEW ORDER.exe"
Imagebase:	0x300000
File size:	804864 bytes
MD5 hash:	2AB185544E86862DAB6A5E7A4413C49F
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: 00000000.00000002.505972636.000000000362F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.505972636.000000000362F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E5CCF06	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	6E5CCF06	unknown
C:\Users\user\AppData\Roaming\IrUpgWwdRBJK.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CBE1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp354B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CBE7038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\NEW ORDER.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E8DC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp354B.tmp	success or wait	1	6CBE6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\IrUpgWwdRBJK.exe	0	804864	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp354B.tmp	0	1649	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 61 6c 66 6f 6e 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49	<?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> </RegistrationI	success or wait	1	6CBE1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\NEW ORDER.exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6E8DC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E5A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E5A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E5003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E5ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E5003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E5003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E5003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E5003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E5A5705	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E5A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CBE1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CBE1B4F	ReadFile
C:\Users\user\Desktop\NEW ORDER.exe	unknown	804864	success or wait	1	6CBE1B4F	ReadFile

Analysis Process: schtasks.exe PID: **7120**, Parent PID: **7016**

General

Target ID:	1
Start time:	21:33:04
Start date:	13/05/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\IrUpgWwdRBJK" /XML "C:\Users\user\AppData\Local\Temp\tmp354B.tmp
Imagebase:	0xff0000
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\tmp354B.tmp	unknown	2	success or wait	1	FFAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp354B.tmp	unknown	1650	success or wait	1	FFABD9	ReadFile

Analysis Process: conhost.exe PID: **7128**, Parent PID: **7120**

General

Target ID:	2
Start time:	21:33:05
Start date:	13/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
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: **3968**, Parent PID: **7016**

General

Target ID:	3
Start time:	21:33:06
Start date:	13/05/2022
Path:	C:\Users\user\Desktop\NEW ORDER.exe

Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x6f0000
File size:	804864 bytes
MD5 hash:	2AB185544E86862DAB6A5E7A4413C49F
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: 00000003.00000000.486980862.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000000.486980862.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.698717283.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000002.698717283.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000000.487669907.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000000.487669907.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000000.485892465.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000000.485892465.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000000.486525104.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000000.486525104.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.705211244.0000000002A91000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.705211244.0000000002A91000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E5CCF06	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	6E5CCF06	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	6E5A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E5A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E5003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E5ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E5003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E5003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E5003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E5003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E5A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E5A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CBE1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CBE1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6CBE1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\c3d0bcad-59c3-41fa-89dd-89b9005799af	unknown	4096	success or wait	1	6CBE1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6CBE1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CBE1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CBE1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CBE1B4F	ReadFile

Disassembly

No disassembly