ID: 404158
Sample Name: New Order Request_0232147.exe
Cookbook: default.jbs
Time: 19:00:41
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

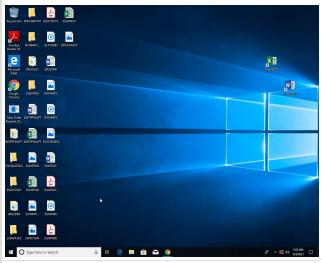
Analysis Report New Order Request_0232147.exe

Overview

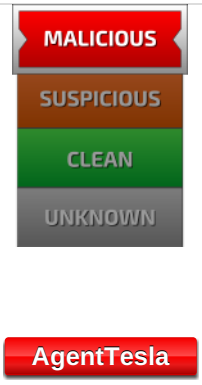
General Information

Sample Name:	New Order Request_0232147.exe
Analysis ID:	404158
MD5:	5133cbc9db4989..
SHA1:	72052feec6f9f94…
SHA256:	fbdc2f9c6e970ae..
Tags:	AgentTesla exe
Infos:	

Most interesting Screenshot:



Detection



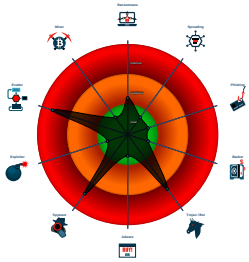
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains very larg…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to detect sandboxes and other…
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal browser in…
- Tries to harvest and steal ftp login c…
- Tries to steal Mail credentials (via fil…

Classification



Startup

- **System is w10x64**
- New Order Request_0232147.exe (PID: 6368 cmdline: 'C:\Users\user\Desktop\New Order Request_0232147.exe' MD5: 5133CBC9DB4989D6FBB350E0829911C8)
  - New Order Request_0232147.exe (PID: 6596 cmdline: {path} MD5: 5133CBC9DB4989D6FBB350E0829911C8)
  - New Order Request_0232147.exe (PID: 6604 cmdline: {path} MD5: 5133CBC9DB4989D6FBB350E0829911C8)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "calidad1@iruberritechnologies.comVpx7s4QHfJx7mail.iruberritechnologies.comrichardjortega@yandex.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.263302597.000000000454 8000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000002.495432203.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000002.500811322.0000000002C5 1000.00000004.00000001.sdmp	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	
Process Memory Space: New Order Request_0232147.exe PID: 6368	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: New Order Request_0232147.exe PID: 6368	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Source	Rule	Description	Author	Strings
Click to see the 2 entries				

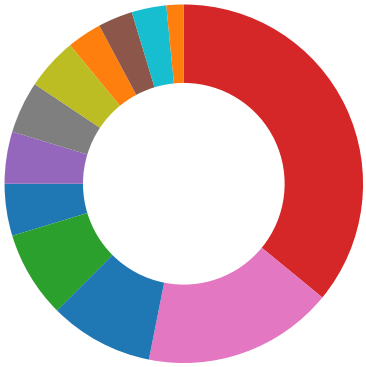
Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.New Order Request_0232147.exe.45ee328.3.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
5.2.New Order Request_0232147.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.New Order Request_0232147.exe.45ee328.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

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

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

System Summary:

.NET source code contains very large array initializations

Initial sample is a PE file and has a suspicious name

Malware Analysis System Evasion:

Yara detected AntiVM3

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

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

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

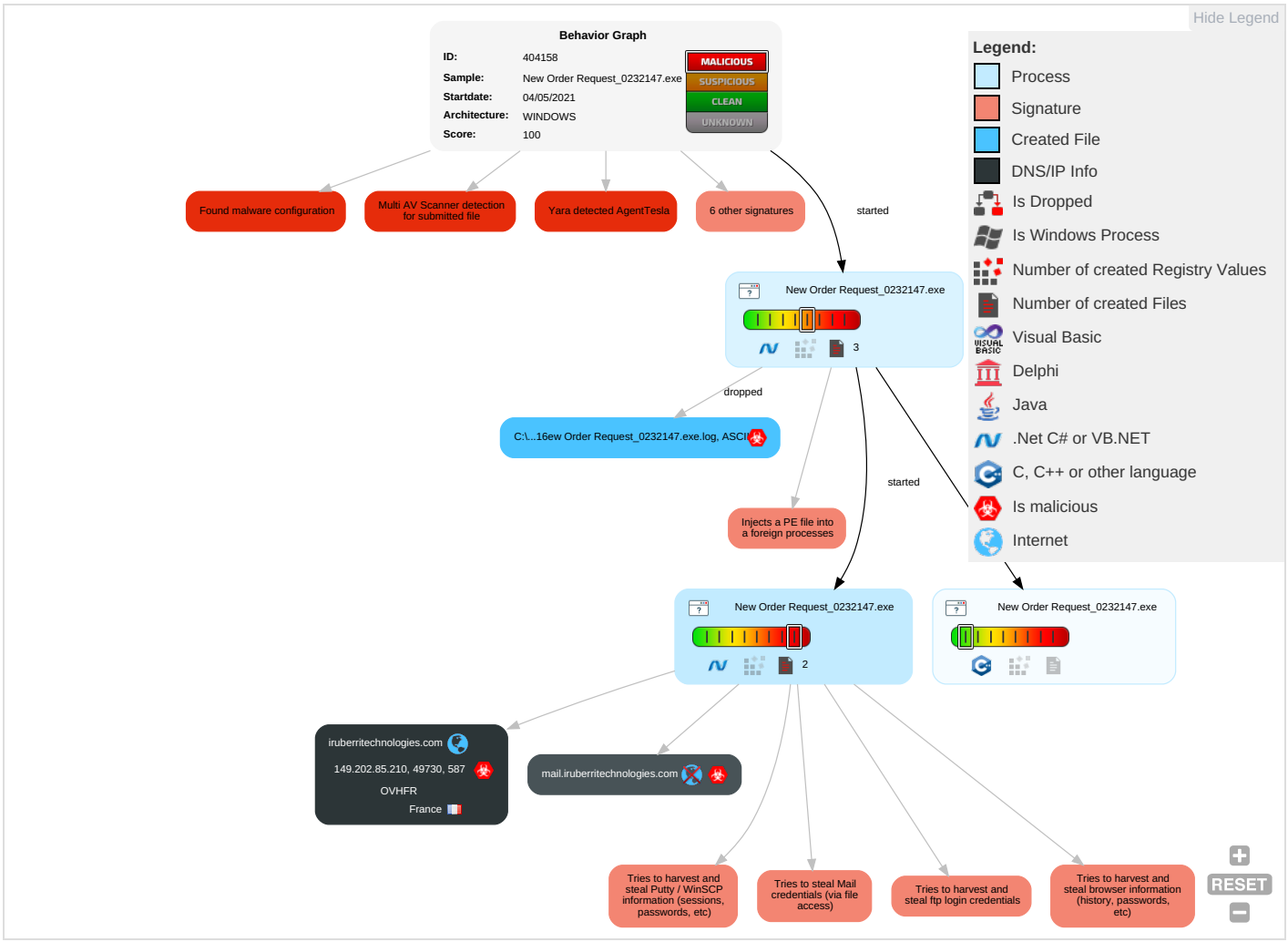
Remote Access Functionality:

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
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1 1 2	Masquerading 1	OS Credential Dumping 2	Query Registry 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Command and Scripting Interpreter 2	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	Credentials in Registry 1	Security Software Discovery 2 1 1	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1 3 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Local System 2	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Virtualization/Sandbox Evasion 1 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicati
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 2	DCSync	System Information Discovery 1 1 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Timestomp 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocc

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 Request_0232147.exe	15%	Virustotal		Browse
New Order Request_0232147.exe	17%	ReversingLabs	ByteCode-MSIL.Trojan.Wacatac	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.New Order Request_0232147.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
iruberritechnologies.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comiv	0%	URL Reputation	safe	
http://www.sajatypeworks.comiv	0%	URL Reputation	safe	
http://www.sajatypeworks.comiv	0%	URL Reputation	safe	
http://www.tiro.com7	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.carterandcone.comTCZ	0%	Avira URL Cloud	safe	
http://r3.i.lencr.org/0?	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://iruberritechnologies.com	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.sajatypeworks.comt	0%	URL Reputation	safe	
http://www.sajatypeworks.comt	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.sajatypeworks.comt	0%	URL Reputation	safe	
http://www.sajatypeworks.comTF	0%	Avira URL Cloud	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://LPzxab.com	0%	Avira URL Cloud	safe	
http://https://9TuO2oVE4tm8Yg0qRsK.org	0%	Avira URL Cloud	safe	
http://www.fontbureau.comion	0%	URL Reputation	safe	
http://www.fontbureau.comion	0%	URL Reputation	safe	
http://www.fontbureau.comion	0%	URL Reputation	safe	
http://www.founder.com.cn/cnFYT/	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://mail.iruberritechnologies.com	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.fontbureau.comh	0%	Avira URL Cloud	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn(	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
iruberritechnologies.com	149.202.85.210	true	true	• 0%, Virustotal, Browse	unknown
mail.iruberritechnologies.com	unknown	unknown	true		unknown

URLs from Memory and Binaries

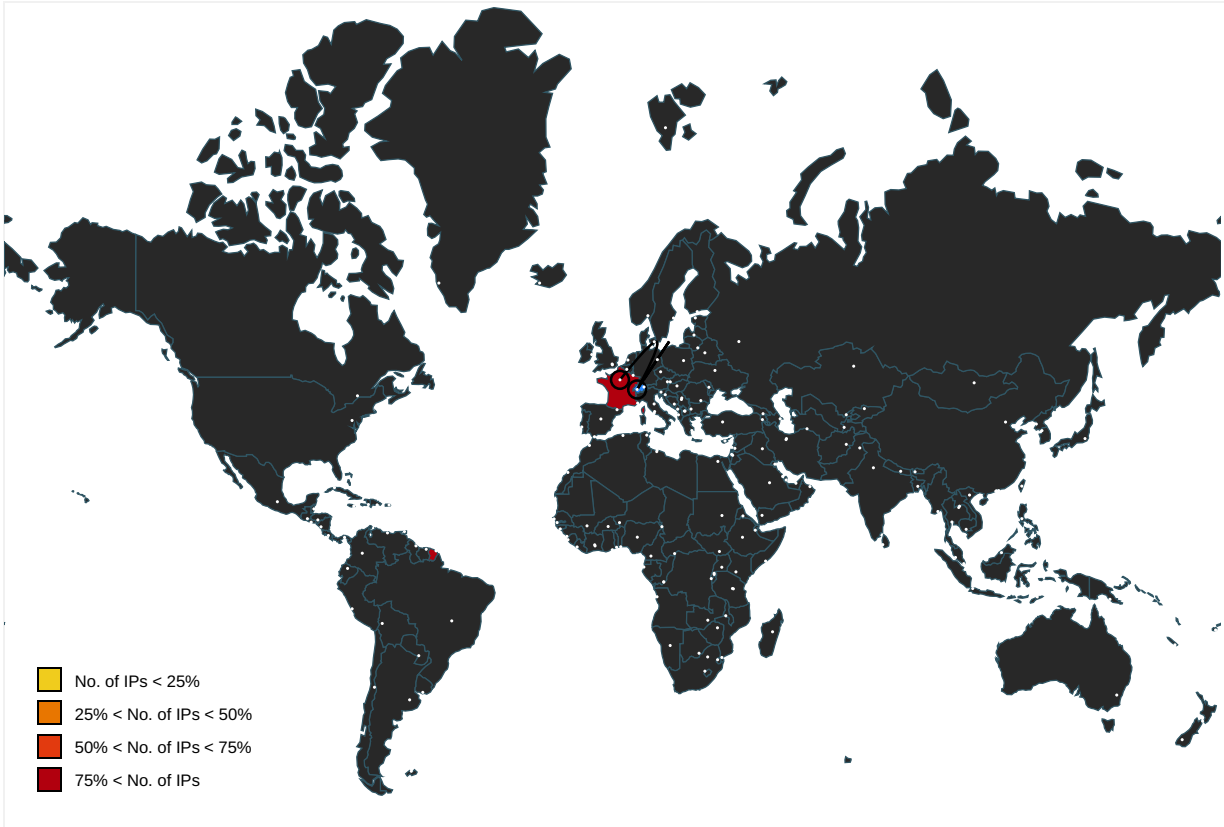
Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	New Order Request_0232147.exe, 00000005.00000002.500811322.000000002C51000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	New Order Request_0232147.exe, 00000000.00000002.268539867.000000006370000.00000002.00000001.sdmp	false		high
http://www.sajatypeworks.comiv	New Order Request_0232147.exe, 00000000.00000003.233482785.00000000629B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tiro.com7	New Order Request_0232147.exe, 00000000.00000003.235097752.000000006288000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	New Order Request_0232147.exe, 00000000.00000002.268539867.000000006370000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/bThe	New Order Request_0232147.exe, 00000000.00000002.268539867.000000006370000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	New Order Request_0232147.exe, 00000000.00000002.268539867.000000006370000.00000002.00000001.sdmp	false		high
http://www.carterandcone.comTCZ	New Order Request_0232147.exe, 00000000.00000003.237770203.00000000628E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://r3.i.lencr.org/0?	New Order Request_0232147.exe, 00000005.00000002.503206058.000000002F00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	New Order Request_0232147.exe, 00000000.00000002.268539867.000000006370000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	New Order Request_0232147.exe, 00000000.00000003.243298062.000000006285000.00000004.00000001.sdmp	false		high
http://www.goodfont.co.kr	New Order Request_0232147.exe, 00000000.00000002.268539867.000000006370000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com	New Order Request_0232147.exe, 00000000.00000003.237770203.00000000628E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://iruberritechnologies.com	New Order Request_0232147.exe, 00000005.00000002.503177096.000000002EFA000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	New Order Request_0232147.exe, 00000000.00000002.268539867.000000006370000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	New Order Request_0232147.exe, 00000000.00000002.268539867.000000006370000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	New Order Request_0232147.exe, 00000000.00000002.268539867.000000006370000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	New Order Request_0232147.exe, 00000000.00000003.242633271.000000006285000.00000004.00000001.sdmp, New Order Request_0232147.exe, 00000000.00000002.268539867.0000000006370000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	New Order Request_0232147.exe, 00000000.00000002.268539867.000000006370000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://r3.o.lencr.org0	New Order Request_0232147.exe, 00000005.00000002.503206058.000000002F00000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	New Order Request_0232147.exe, 00000000.00000002.268539867.000000006370000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.com	New Order Request_0232147.exe, 00000000.00000002.268539867.000000006370000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	New Order Request_0232147.exe, 00000000.00000002.268539867.000000006370000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	New Order Request_0232147.exe, 00000000.00000002.268539867.000000006370000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.zhongyicts.com.cn	New Order Request_0232147.exe, 00000000.00000002.268539867.000000006370000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	New Order Request_0232147.exe, 00000000.00000003.237365971.000000006286000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	New Order Request_0232147.exe, 00000000.00000002.263302597.000000004548000.00000004.00000001.sdmp, New Order Request_0232147.exe, 00000005.00000002.495432203.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cps.root-x1.letsencrypt.org0	New Order Request_0232147.exe, 00000005.00000002.503206058.000000002F00000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	New Order Request_0232147.exe, 00000000.00000002.268539867.000000006370000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	New Order Request_0232147.exe, 00000000.00000002.268539867.000000006370000.00000002.00000001.sdmp	false		high
http://DynDns.comDynDNS	New Order Request_0232147.exe, 00000005.00000002.500811322.000000002C51000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.comt	New Order Request_0232147.exe, 00000000.00000003.233482785.00000000629B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.comTF	New Order Request_0232147.exe, 00000000.00000003.233482785.00000000629B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://cps.letsencrypt.org0	New Order Request_0232147.exe, 00000005.00000002.503206058.000000002F00000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	New Order Request_0232147.exe, 00000005.00000002.500811322.000000002C51000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comTC	New Order Request_0232147.exe, 00000000.00000003.237770203.00000000628E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://LPzxab.com	New Order Request_0232147.exe, 00000005.00000002.500811322.000000002C51000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://9TuO2oVE4tm8Yg0qRsK.org	New Order Request_0232147.exe, 00000005.00000002.500811322.000000002C51000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comion	New Order Request_0232147.exe, 00000000.00000002.259475460.00000000019A7000.00000004.00000040.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnFYT/	New Order Request_0232147.exe, 00000000.00000003.234986480.000000006288000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	New Order Request_0232147.exe, 00000000.00000002.268539867.000000006370000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://mail.iruberritechnologies.com	New Order Request_0232147.exe, 00000005.00000002.503177096.000000002EFA000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	New Order Request_0232147.exe, 00000000.00000002.268539867.000000006370000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn	New Order Request_0232147.exe, 00000000.00000002.268539867.000000006370000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	New Order Request_0232147.exe, 00000000.00000002.268539867.000000006370000.00000002.00000001.sdmp	false		high
http://www.fontbureau.comh	New Order Request_0232147.exe, 00000000.00000002.259475460.00000000019A7000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.monotype.	New Order Request_0232147.exe, 00000000.00000003.241640533.00000000628B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	New Order Request_0232147.exe, 00000000.00000002.268539867.000000006370000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	New Order Request_0232147.exe, 00000000.00000002.268539867.000000006370000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn(	New Order Request_0232147.exe, 00000000.00000003.234986480.000000006288000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
149.202.85.210	iruberritechnologies.com	France		16276	OVHFR	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond

Analysis ID:	404158
Start date:	04.05.2021
Start time:	19:00:41
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	New Order Request_0232147.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:	24
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@5/1@6/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Excluded IPs from analysis (whitelisted): 93.184.220.29, 204.79.197.200, 13.107.21.200, 20.82.210.154, 13.88.21.125, 52.147.198.201, 92.122.145.220, 52.255.188.83, 104.43.139.144, 23.57.80.111, 2.20.142.210, 2.20.142.209, 92.122.213.194, 92.122.213.247, 20.54.26.129 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, cs9.wac.phicdn.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e12564.dspb.akamaiedge.net, ocsp.digicert.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, fs.microsoft.com, dual-a-0001.a-msedge.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
19:01:41	API Interceptor	706x Sleep call for process: New Order Request_0232147.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
149.202.85.210	Zwi#U0119ksz-2873037.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
OVHFR	Transcation03232016646pdf.exe	Get hash	malicious	Browse	• 79.137.109.121
	5e60c283_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 51.77.73.218
	MZyeln5mSFOjxMx.exe	Get hash	malicious	Browse	• 66.70.204.222
	5e60c283_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 51.77.73.218
	51086cc4_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	8aa43191_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	5e60c283_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 51.77.73.218
	51086cc4_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	8aa43191_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	840e7dfd_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	840e7dfd_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	94765446_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	d192feb6_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	7bc33f1c_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	94765446_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	448b5d7d_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	7bc33f1c_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	feb26e28_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	cfba18f5_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	ae394500_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\New Order Request_0232147.exe.log

Process:	C:\Users\user\Desktop\New Order Request_0232147.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\New Order Request_0232147.exe.log	
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
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..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=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.16370494238722
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 Request_0232147.exe
File size:	1045504
MD5:	5133cbc9db4989d6fbb350e0829911c8
SHA1:	72052feec6f9f94fe0831a77bdf8c3493d268e37
SHA256:	fbdc2f9c6e970ae88ff30847c4d63472a0f0aa9b8e008e5b5c37f62ac526a963
SHA512:	8f13f01160e182cb9169ebaffc97e48f1f84661c613370cf9c9c77dc39b4e8c1686a74cd4e438530e27970a0fe9c0465043434aad000f66b4469f9009c0807e1
SSDEEP:	24576:Zv0t4KctioLA/9NjMjEjqRUj+hRZJr+F/:Zv0t4KEyYoOWaJr+F
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...d.....0..... ... .@.. .....`.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x5007e2
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

General

Time Stamp:	0xF0C0A264 [Sun Dec 29 11:52:04 2097 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
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add 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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x100790	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x102000	0x604	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x104000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x100774	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
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	0xfe7e8	0xfe800	False	0.625946824349	data	7.17013687848	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x102000	0x604	0x800	False	0.330078125	data	3.44053524231	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x104000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x102090	0x374	data		
RT_MANIFEST	0x102414	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

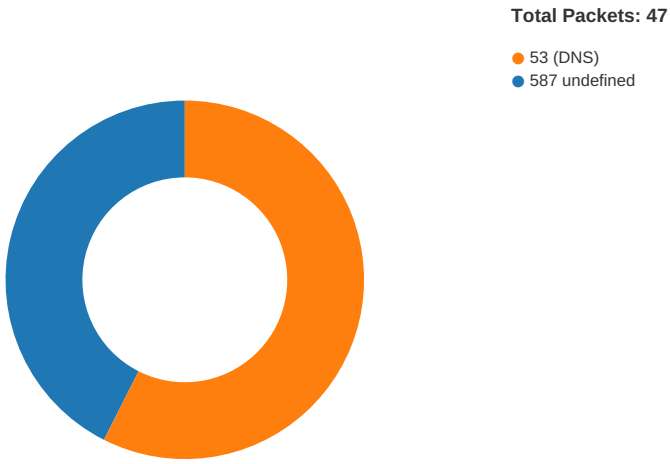
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2019
Assembly Version	1.0.0.0
InternalName	qGOldQU8bPo4VOD.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	HospitalManagementSystem
ProductVersion	1.0.0.0
FileDescription	HospitalManagementSystem
OriginalFilename	qGOldQU8bPo4VOD.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/04/21-19:03:34.149691	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.5	8.8.8.8
05/04/21-19:03:35.147063	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.5	8.8.8.8
05/04/21-19:03:38.608596	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.5	8.8.8.8

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 19:03:35.674813986 CEST	49730	587	192.168.2.5	149.202.85.210
May 4, 2021 19:03:35.724775076 CEST	587	49730	149.202.85.210	192.168.2.5
May 4, 2021 19:03:35.724873066 CEST	49730	587	192.168.2.5	149.202.85.210
May 4, 2021 19:03:35.874888897 CEST	587	49730	149.202.85.210	192.168.2.5
May 4, 2021 19:03:35.875323057 CEST	49730	587	192.168.2.5	149.202.85.210
May 4, 2021 19:03:35.925534010 CEST	587	49730	149.202.85.210	192.168.2.5
May 4, 2021 19:03:35.925946951 CEST	49730	587	192.168.2.5	149.202.85.210
May 4, 2021 19:03:35.978585005 CEST	587	49730	149.202.85.210	192.168.2.5
May 4, 2021 19:03:36.029336929 CEST	49730	587	192.168.2.5	149.202.85.210
May 4, 2021 19:03:36.059819937 CEST	49730	587	192.168.2.5	149.202.85.210
May 4, 2021 19:03:36.131764889 CEST	587	49730	149.202.85.210	192.168.2.5
May 4, 2021 19:03:36.131798983 CEST	587	49730	149.202.85.210	192.168.2.5
May 4, 2021 19:03:36.131819963 CEST	587	49730	149.202.85.210	192.168.2.5
May 4, 2021 19:03:36.131889105 CEST	49730	587	192.168.2.5	149.202.85.210
May 4, 2021 19:03:36.139411926 CEST	49730	587	192.168.2.5	149.202.85.210
May 4, 2021 19:03:36.189862013 CEST	587	49730	149.202.85.210	192.168.2.5
May 4, 2021 19:03:36.232606888 CEST	49730	587	192.168.2.5	149.202.85.210
May 4, 2021 19:03:36.524369955 CEST	49730	587	192.168.2.5	149.202.85.210
May 4, 2021 19:03:36.574446917 CEST	587	49730	149.202.85.210	192.168.2.5
May 4, 2021 19:03:36.576993942 CEST	49730	587	192.168.2.5	149.202.85.210
May 4, 2021 19:03:36.627314091 CEST	587	49730	149.202.85.210	192.168.2.5
May 4, 2021 19:03:36.628407001 CEST	49730	587	192.168.2.5	149.202.85.210
May 4, 2021 19:03:36.717538118 CEST	587	49730	149.202.85.210	192.168.2.5
May 4, 2021 19:03:36.732202053 CEST	587	49730	149.202.85.210	192.168.2.5
May 4, 2021 19:03:36.733273029 CEST	49730	587	192.168.2.5	149.202.85.210
May 4, 2021 19:03:36.783344030 CEST	587	49730	149.202.85.210	192.168.2.5
May 4, 2021 19:03:36.784981966 CEST	49730	587	192.168.2.5	149.202.85.210
May 4, 2021 19:03:36.848463058 CEST	587	49730	149.202.85.210	192.168.2.5
May 4, 2021 19:03:36.849080086 CEST	49730	587	192.168.2.5	149.202.85.210
May 4, 2021 19:03:36.899036884 CEST	587	49730	149.202.85.210	192.168.2.5
May 4, 2021 19:03:36.903260946 CEST	49730	587	192.168.2.5	149.202.85.210
May 4, 2021 19:03:36.903429031 CEST	49730	587	192.168.2.5	149.202.85.210
May 4, 2021 19:03:36.903563023 CEST	49730	587	192.168.2.5	149.202.85.210
May 4, 2021 19:03:36.903666019 CEST	49730	587	192.168.2.5	149.202.85.210
May 4, 2021 19:03:36.953233957 CEST	587	49730	149.202.85.210	192.168.2.5
May 4, 2021 19:03:36.953267097 CEST	587	49730	149.202.85.210	192.168.2.5
May 4, 2021 19:03:36.953285933 CEST	587	49730	149.202.85.210	192.168.2.5
May 4, 2021 19:03:36.953876019 CEST	587	49730	149.202.85.210	192.168.2.5
May 4, 2021 19:03:37.489578962 CEST	587	49730	149.202.85.210	192.168.2.5
May 4, 2021 19:03:37.529539108 CEST	49730	587	192.168.2.5	149.202.85.210

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 19:01:25.592560053 CEST	53	64344	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 19:01:26.003287077 CEST	62060	53	192.168.2.5	8.8.8.8
May 4, 2021 19:01:26.060152054 CEST	53	62060	8.8.8.8	192.168.2.5
May 4, 2021 19:01:26.093084097 CEST	61805	53	192.168.2.5	8.8.8.8
May 4, 2021 19:01:26.144553900 CEST	53	61805	8.8.8.8	192.168.2.5
May 4, 2021 19:01:26.345740080 CEST	54795	53	192.168.2.5	8.8.8.8
May 4, 2021 19:01:26.395255089 CEST	53	54795	8.8.8.8	192.168.2.5
May 4, 2021 19:01:27.437642097 CEST	49557	53	192.168.2.5	8.8.8.8
May 4, 2021 19:01:27.486398935 CEST	53	49557	8.8.8.8	192.168.2.5
May 4, 2021 19:01:28.266197920 CEST	61733	53	192.168.2.5	8.8.8.8
May 4, 2021 19:01:28.317600965 CEST	53	61733	8.8.8.8	192.168.2.5
May 4, 2021 19:01:29.049745083 CEST	65447	53	192.168.2.5	8.8.8.8
May 4, 2021 19:01:29.109853029 CEST	53	65447	8.8.8.8	192.168.2.5
May 4, 2021 19:01:29.161185026 CEST	52441	53	192.168.2.5	8.8.8.8
May 4, 2021 19:01:29.221350908 CEST	53	52441	8.8.8.8	192.168.2.5
May 4, 2021 19:01:30.116239071 CEST	62176	53	192.168.2.5	8.8.8.8
May 4, 2021 19:01:30.167891026 CEST	53	62176	8.8.8.8	192.168.2.5
May 4, 2021 19:01:30.920952082 CEST	59596	53	192.168.2.5	8.8.8.8
May 4, 2021 19:01:30.969603062 CEST	53	59596	8.8.8.8	192.168.2.5
May 4, 2021 19:01:31.944355965 CEST	65296	53	192.168.2.5	8.8.8.8
May 4, 2021 19:01:31.995897055 CEST	53	65296	8.8.8.8	192.168.2.5
May 4, 2021 19:01:32.728172064 CEST	63183	53	192.168.2.5	8.8.8.8
May 4, 2021 19:01:32.776891947 CEST	53	63183	8.8.8.8	192.168.2.5
May 4, 2021 19:01:34.211884022 CEST	60151	53	192.168.2.5	8.8.8.8
May 4, 2021 19:01:34.270097017 CEST	53	60151	8.8.8.8	192.168.2.5
May 4, 2021 19:01:35.463999987 CEST	56969	53	192.168.2.5	8.8.8.8
May 4, 2021 19:01:35.515537024 CEST	53	56969	8.8.8.8	192.168.2.5
May 4, 2021 19:01:50.874479055 CEST	55161	53	192.168.2.5	8.8.8.8
May 4, 2021 19:01:50.938227892 CEST	53	55161	8.8.8.8	192.168.2.5
May 4, 2021 19:02:02.922646046 CEST	54757	53	192.168.2.5	8.8.8.8
May 4, 2021 19:02:02.974347115 CEST	53	54757	8.8.8.8	192.168.2.5
May 4, 2021 19:02:21.236640930 CEST	49992	53	192.168.2.5	8.8.8.8
May 4, 2021 19:02:21.294007063 CEST	53	49992	8.8.8.8	192.168.2.5
May 4, 2021 19:02:45.338238955 CEST	60075	53	192.168.2.5	8.8.8.8
May 4, 2021 19:02:45.389822006 CEST	53	60075	8.8.8.8	192.168.2.5
May 4, 2021 19:02:55.162802935 CEST	55016	53	192.168.2.5	8.8.8.8
May 4, 2021 19:02:55.221085072 CEST	53	55016	8.8.8.8	192.168.2.5
May 4, 2021 19:03:10.427627087 CEST	64345	53	192.168.2.5	8.8.8.8
May 4, 2021 19:03:10.493542910 CEST	53	64345	8.8.8.8	192.168.2.5
May 4, 2021 19:03:30.029875040 CEST	57128	53	192.168.2.5	8.8.8.8
May 4, 2021 19:03:31.029841900 CEST	57128	53	192.168.2.5	8.8.8.8
May 4, 2021 19:03:32.045248032 CEST	57128	53	192.168.2.5	8.8.8.8
May 4, 2021 19:03:32.948568106 CEST	54791	53	192.168.2.5	8.8.8.8
May 4, 2021 19:03:32.997354031 CEST	53	54791	8.8.8.8	192.168.2.5
May 4, 2021 19:03:34.092262030 CEST	57128	53	192.168.2.5	8.8.8.8
May 4, 2021 19:03:34.134357929 CEST	53	57128	8.8.8.8	192.168.2.5
May 4, 2021 19:03:34.134438038 CEST	53	57128	8.8.8.8	192.168.2.5
May 4, 2021 19:03:34.149570942 CEST	53	57128	8.8.8.8	192.168.2.5
May 4, 2021 19:03:34.505417109 CEST	50463	53	192.168.2.5	8.8.8.8
May 4, 2021 19:03:35.146867037 CEST	53	57128	8.8.8.8	192.168.2.5
May 4, 2021 19:03:35.435235977 CEST	50394	53	192.168.2.5	8.8.8.8
May 4, 2021 19:03:35.492245913 CEST	53	50394	8.8.8.8	192.168.2.5
May 4, 2021 19:03:35.498763084 CEST	50463	53	192.168.2.5	8.8.8.8
May 4, 2021 19:03:35.558713913 CEST	53	50463	8.8.8.8	192.168.2.5
May 4, 2021 19:03:38.608398914 CEST	53	50463	8.8.8.8	192.168.2.5

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
May 4, 2021 19:03:34.149691105 CEST	192.168.2.5	8.8.8.8	d020	(Port unreachable)	Destination Unreachable
May 4, 2021 19:03:35.147063017 CEST	192.168.2.5	8.8.8.8	d020	(Port unreachable)	Destination Unreachable
May 4, 2021 19:03:38.608596087 CEST	192.168.2.5	8.8.8.8	d020	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 19:03:30.029875040 CEST	192.168.2.5	8.8.8.8	0x9dbd	Standard query (0)	mail.iruberritechnologies.com	A (IP address)	IN (0x0001)
May 4, 2021 19:03:31.029841900 CEST	192.168.2.5	8.8.8.8	0x9dbd	Standard query (0)	mail.iruberritechnologies.com	A (IP address)	IN (0x0001)
May 4, 2021 19:03:32.045248032 CEST	192.168.2.5	8.8.8.8	0x9dbd	Standard query (0)	mail.iruberritechnologies.com	A (IP address)	IN (0x0001)
May 4, 2021 19:03:34.092262030 CEST	192.168.2.5	8.8.8.8	0x9dbd	Standard query (0)	mail.iruberritechnologies.com	A (IP address)	IN (0x0001)
May 4, 2021 19:03:34.505417109 CEST	192.168.2.5	8.8.8.8	0xf0aa	Standard query (0)	mail.iruberritechnologies.com	A (IP address)	IN (0x0001)
May 4, 2021 19:03:35.498763084 CEST	192.168.2.5	8.8.8.8	0xf0aa	Standard query (0)	mail.iruberritechnologies.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 19:03:34.134357929 CEST	8.8.8.8	192.168.2.5	0x9dbd	No error (0)	mail.iruberritechnologies.com	iruberritechnologies.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 19:03:34.134357929 CEST	8.8.8.8	192.168.2.5	0x9dbd	No error (0)	iruberritechnologies.com		149.202.85.210	A (IP address)	IN (0x0001)
May 4, 2021 19:03:34.134438038 CEST	8.8.8.8	192.168.2.5	0x9dbd	No error (0)	mail.iruberritechnologies.com	iruberritechnologies.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 19:03:34.134438038 CEST	8.8.8.8	192.168.2.5	0x9dbd	No error (0)	iruberritechnologies.com		149.202.85.210	A (IP address)	IN (0x0001)
May 4, 2021 19:03:34.149570942 CEST	8.8.8.8	192.168.2.5	0x9dbd	No error (0)	mail.iruberritechnologies.com	iruberritechnologies.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 19:03:34.149570942 CEST	8.8.8.8	192.168.2.5	0x9dbd	No error (0)	iruberritechnologies.com		149.202.85.210	A (IP address)	IN (0x0001)
May 4, 2021 19:03:35.146867037 CEST	8.8.8.8	192.168.2.5	0x9dbd	No error (0)	mail.iruberritechnologies.com	iruberritechnologies.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 19:03:35.146867037 CEST	8.8.8.8	192.168.2.5	0x9dbd	No error (0)	iruberritechnologies.com		149.202.85.210	A (IP address)	IN (0x0001)
May 4, 2021 19:03:35.558713913 CEST	8.8.8.8	192.168.2.5	0xf0aa	No error (0)	mail.iruberritechnologies.com	iruberritechnologies.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 19:03:35.558713913 CEST	8.8.8.8	192.168.2.5	0xf0aa	No error (0)	iruberritechnologies.com		149.202.85.210	A (IP address)	IN (0x0001)
May 4, 2021 19:03:38.608398914 CEST	8.8.8.8	192.168.2.5	0xf0aa	No error (0)	mail.iruberritechnologies.com	iruberritechnologies.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 19:03:38.608398914 CEST	8.8.8.8	192.168.2.5	0xf0aa	No error (0)	iruberritechnologies.com		149.202.85.210	A (IP address)	IN (0x0001)

SMTP Packets

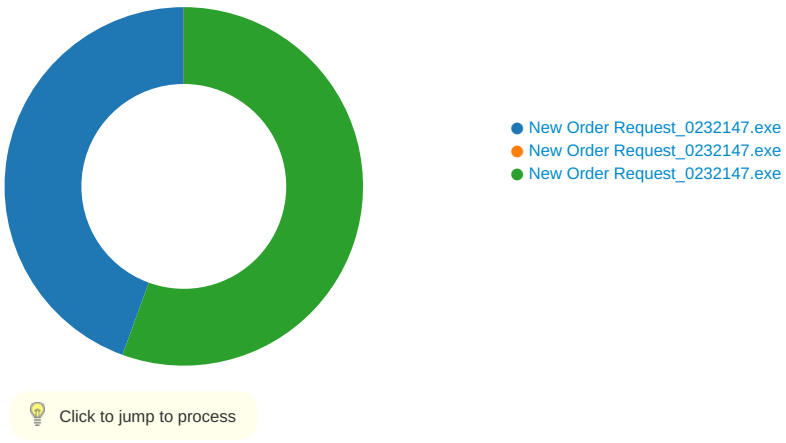
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 4, 2021 19:03:35.874888897 CEST	587	49730	149.202.85.210	192.168.2.5	220-ns3020561.ip-149-202-85.eu ESMTP Exim 4.94 #2 Tue, 04 May 2021 19:03:34 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 4, 2021 19:03:35.875323057 CEST	49730	587	192.168.2.5	149.202.85.210	EHLO 688098

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 4, 2021 19:03:35.925534010 CEST	587	49730	149.202.85.210	192.168.2.5	250-ns3020561.ip-149-202-85.eu Hello 688098 [84.17.52.3] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-X_PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 4, 2021 19:03:35.925946951 CEST	49730	587	192.168.2.5	149.202.85.210	STARTTLS
May 4, 2021 19:03:35.978585005 CEST	587	49730	149.202.85.210	192.168.2.5	220 TLS go ahead

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: New Order Request_0232147.exe PID: 6368 Parent PID: 5668

General

Start time:	19:01:32
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\New Order Request_0232147.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\New Order Request_0232147.exe'
Imagebase:	0xf00000
File size:	1045504 bytes
MD5 hash:	5133CBC9DB4989D6FBB350E0829911C8
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: 00000000.00000002.263302597.0000000004548000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DB3CF06	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	6DB3CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\New Order Request_0232147.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DE4C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\New Order Request_0232147.exe.log	unknown	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",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_v4.0.3	success or wait	1	6DE4C907	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	6DB15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DB15705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DA703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB1CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DA703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DA703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DA703DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DA703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DB15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C831B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C831B4F	ReadFile

Analysis Process: New Order Request_0232147.exe PID: 6596 Parent PID: 6368

General

Start time:	19:01:43
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\New Order Request_0232147.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x1e0000
File size:	1045504 bytes
MD5 hash:	5133CBC9DB4989D6FBB350E0829911C8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: New Order Request_0232147.exe PID: 6604 Parent PID: 6368

General

Start time:	19:01:44
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\New Order Request_0232147.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x860000
File size:	1045504 bytes
MD5 hash:	5133CBC9DB4989D6FBB350E0829911C8
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: 00000005.00000002.495432203.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.500811322.0000000002C51000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DB3CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6DB3CF06	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	6DB15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DB15705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DA703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB1CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DA703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DA703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DA703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DA703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DB15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DB15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C831B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C831B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	10960	success or wait	1	6C831B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\6c58c849-6de7-4340-ac1b-f2c5948b06ac	unknown	4096	success or wait	1	6C831B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	10960	success or wait	1	6C831B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C831B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C831B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C831B4F	ReadFile

Disassembly

Code Analysis