ID: 411847
Sample Name: NEW ORDER SOR 10531220.exe
Cookbook: default.jbs
Time: 07:43:24
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

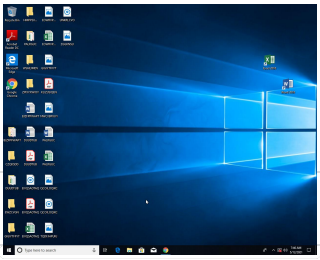
Analysis Report NEW ORDER SOR 10531220.exe

Overview

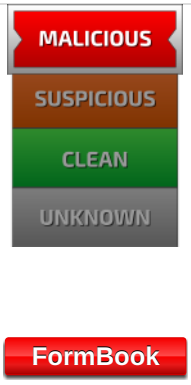
General Information

Sample Name:	NEW ORDER SOR 10531220.exe
Analysis ID:	411847
MD5:	2e2de2014ccb06..
SHA1:	b571217f8771069.
SHA256:	f8ca257b6bbb8a0.
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection

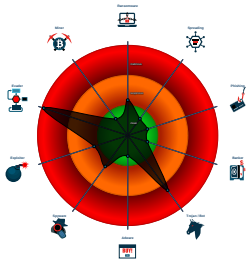


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e….
- System process connects to networ…
- Yara detected AntiVM3
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Initial sample is a PE file and has a …
- Machine Learning detection for samp…

Classification



Startup

- **System is w10x64**
- NEW ORDER SOR 10531220.exe (PID: 3756 cmdline: 'C:\Users\user\Desktop\NEW ORDER SOR 10531220.exe' MD5: 2E2DE2014CCB06FEA1B50414F5E301E6)
  - NEW ORDER SOR 10531220.exe (PID: 6164 cmdline: C:\Users\user\Desktop\NEW ORDER SOR 10531220.exe MD5: 2E2DE2014CCB06FEA1B50414F5E301E6)
  - NEW ORDER SOR 10531220.exe (PID: 6176 cmdline: C:\Users\user\Desktop\NEW ORDER SOR 10531220.exe MD5: 2E2DE2014CCB06FEA1B50414F5E301E6)
    - explorer.exe (PID: 3472 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - netsh.exe (PID: 7088 cmdline: C:\Windows\SysWOW64\netsh.exe MD5: A0AA3322BB46BBFC36AB9DC1DBBBB807)
        - cmd.exe (PID: 3552 cmdline: /c del 'C:\Users\user\Desktop\NEW ORDER SOR 10531220.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5808 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.magnumopuspro.com/nyr/"
  ],
  "decoy": [
    "anemone-vintage.com",
    "ironcitytools.com",
    "joshandmatthew.com",
    "breathtakingscenery.photos",
    "karabakh-terror.com",
    "micahelgall.com",
    "entretiendesterrasses.com",
    "mhgholdings.com",
    "blewm.com",
    "sidewalknotary.com",
    "ytrs-elec.com",
    "danhpham.com",
    "ma21cle2henz.xyz",
    "lotusforlease.com",
    "shipleyphotoandfilm.com",
    "bulktool.xyz",
    "ouedzmala.com",
    "yichengvpr.com",
    "connectmygames.com",
    "chjcsc.com",
    "dope-chocolate.com",
    "tacowench.com",
    "projectsbay.com",
    "xn--pgboc92d.com",
    "royaldropofoil.com",
    "ranguanglian.club",
    "mobilne-kucice.com",
    "buytsycon.com",
    "goiasbets.net",
    "blpetroleum.com",
    "starrealms.net",
    "exclusiveflooringcollection.com",
    "kudalive.com",
    "tienda-sky.com",
    "drillinginsider.info",
    "theglasshousenyc.com",
    "vietnammoi.xyz",
    "walterbenicio.com",
    "zoomtvliveshows.xyz",
    "boujiehoodbaby.com",
    "yzyangyu.com",
    "exploreecetera.com",
    "sycord.com",
    "waykifood.com",
    "shadingconsultancy.com",
    "precedentai.net",
    "linhanhkitchen.com",
    "expekt24.com",
    "socialdating24.com",
    "lubvim.com",
    "floryi.com",
    "alerist.com",
    "maluss.com",
    "hitbbq.com",
    "alerrandrotattoo.com",
    "algoplayer.com",
    "idahooutsiders.com",
    "qygmuakhk.club",
    "neverpossible.com",
    "winparadigm.com",
    "toughdecorative.com",
    "yourbuildmedia.com",
    "summercrowd.com",
    "josemvazquez.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.305618158.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000003.00000002.305618158.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000003.00000002.305618158.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$sqlite3step: 68 34 1C 7B E1 • 0x1851c:$sqlite3step: 68 34 1C 7B E1 • 0x18438:$sqlite3text: 68 38 2A 90 C5 • 0x1855d:$sqlite3text: 68 38 2A 90 C5 • 0x1844b:$sqlite3blob: 68 53 D8 7F 8C • 0x18573:$sqlite3blob: 68 53 D8 7F 8C
0000000F.00000002.502736423.0000000000980000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000F.00000002.502736423.0000000000980000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 18 entries				

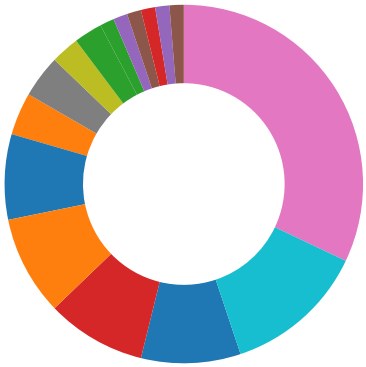
Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.NEW ORDER SOR 10531220.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.2.NEW ORDER SOR 10531220.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x977a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa473:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a527:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b52a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
3.2.NEW ORDER SOR 10531220.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17609:$sqlite3step: 68 34 1C 7B E1 • 0x1771c:$sqlite3step: 68 34 1C 7B E1 • 0x17638:$sqlite3text: 68 38 2A 90 C5 • 0x1775d:$sqlite3text: 68 38 2A 90 C5 • 0x1764b:$sqlite3blob: 68 53 D8 7F 8C • 0x17773:$sqlite3blob: 68 53 D8 7F 8C
3.2.NEW ORDER SOR 10531220.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.2.NEW ORDER SOR 10531220.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- 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
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Hooking and other Techniques for Hiding and Protection:

Modifies the prolog of user mode functions (user mode inline hooks)

Malware Analysis System Evasion:

Yara detected AntiVM3

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

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

System process connects to network (likely due to code injection or exploit)

Maps a DLL or memory area into another process

Modifies the context of a thread in another process (thread injection)

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Lowering of HIPS / PFW / Operating System Security Settings:

Uses netsh to modify the Windows network and firewall settings

Stealing of Sensitive Information:

Yara detected FormBook

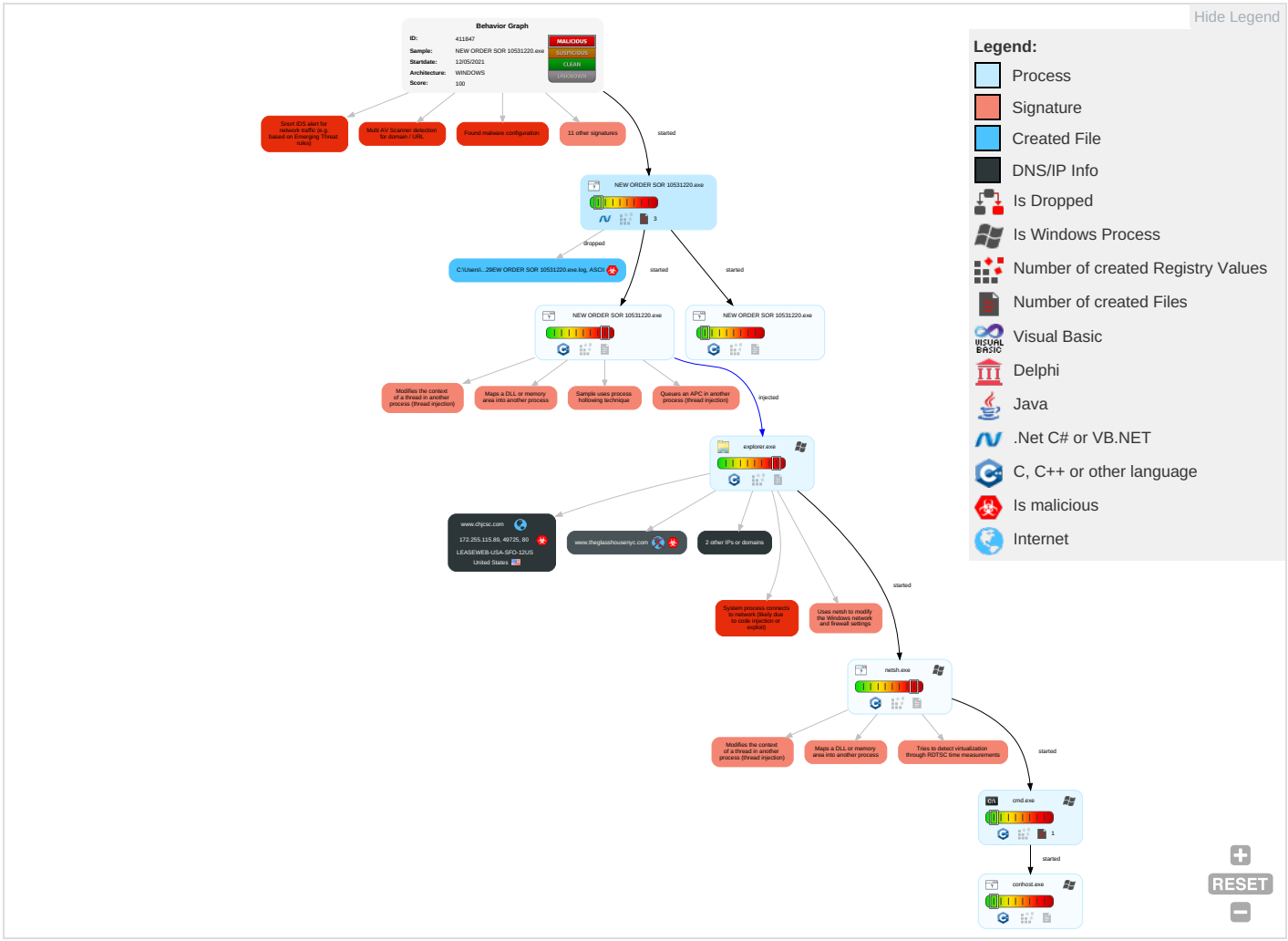
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Command and Scripting Interpreter 2	Path Interception	Process Injection 5 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 2 2 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communi
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Masquerading 1	Input Capture 1	Process Discovery 2	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS Redirect F Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Archive Collected Data 1	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS Track Dev Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 3 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 5 1 2	LSA Secrets	System Information Discovery 1 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulat Device Communi
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 4	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi Access Po
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrad Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Timestomp 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Ce Base Stati

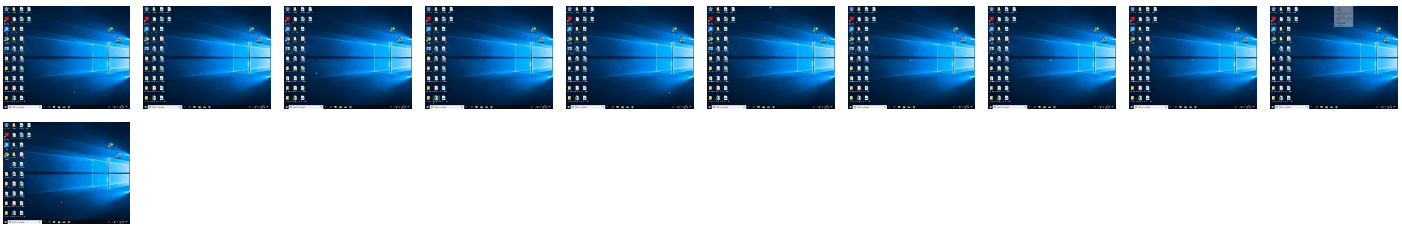
Behavior Graph



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 SOR 10531220.exe	61%	Virustotal		Browse
NEW ORDER SOR 10531220.exe	24%	Metadefender		Browse
NEW ORDER SOR 10531220.exe	52%	ReversingLabs	ByteCode-MSIL.Spyware.Noon	
NEW ORDER SOR 10531220.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.NEW ORDER SOR 10531220.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
theglasshousenyc.com	0%	Virustotal		Browse
www.theglasshousenyc.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.theglasshousenyc.com/nyr/?VBZDH=6l68xBo0LhJD2lv&hRXX=17hAXKnq4LEoTdb/hcwwVfWjS4IYRgMdOmXX52SprwB/nueYqi9a5dgIoxBN3QmuetP3	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.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.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	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.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.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.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://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://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	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.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.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
www.magnumopuspro.com/nyr/	6%	Virustotal		Browse
www.magnumopuspro.com/nyr/	100%	Avira URL Cloud	malware	
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.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.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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://www.sakkal.com	0%	URL Reputation	safe	
http://www.chjcsc.com/nyr/?hRXX=pvzb7SsULo7Y2vRo6lGAqy8tja7/7li767PDw0lqJEj7KBKEBSl8rkLevIquA9l06aH5&VBZDH=6l68xBo0LhJD2lv	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.chjcsc.com	172.255.115.89	true	true		unknown
theglasshousenyc.com	34.102.136.180	true	false	• 0%, Virustotal, Browse	unknown
www.socialdating24.com	unknown	unknown	true		unknown
www.theglasshousenyc.com	unknown	unknown	true	• 0%, Virustotal, Browse	unknown

Contacted URLs

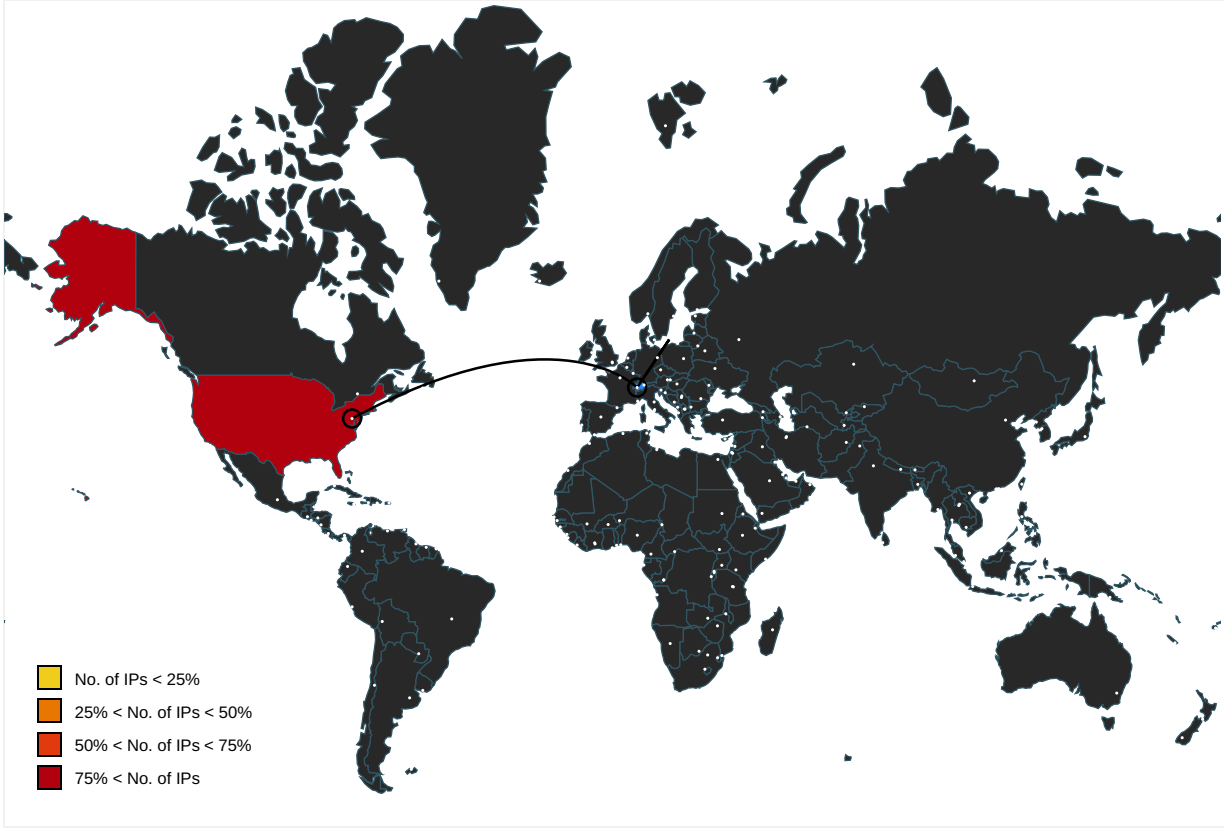
Name	Malicious	Antivirus Detection	Reputation
http://www.theglasshousenyc.com/nyr/?VBZDH=6l68xBo0LhJD2lv&hRXX=17hAXKnq4LEoTdb/hcwwVfWjS4IYRgMdOmXX52SprwB/nueYqi9a5dgIoxBN3QmuetP3	false	• Avira URL Cloud: safe	unknown
www.magnumopuspro.com/nyr/	true	• 6%, Virustotal, Browse • Avira URL Cloud: malware	low
http://www.chjcsc.com/nyr/?hRXX=pvzb7SsULo7Y2vRo6lGAqy8tja7/7li767PDw0lqJEj7KBKEBSl8rkLevIquA9l06aH5&VBZDH=6l68xBo0LhJD2lv	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000005.00000000.274441918.000000000BC36000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000005.00000000.274441918.000000000BC36000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000005.00000000.274441918.000000000BC36000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000005.00000000.274441918.000000000BC36000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000005.00000000.274441918.000000000BC36000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000005.00000000.274441918.000000000BC36000.00000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000005.00000000.274441918.000000000BC36000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000005.00000000.274441918.000000000BC36000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000005.00000000.274441918.000000000BC36000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	NEW ORDER SOR 10531220.exe, 00000000.00000002.244540222.00000000002F26000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.coml	explorer.exe, 00000005.0000000 0.274441918.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000005.0000000 0.274441918.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000005.0000000 0.274441918.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000005.0000000 0.274441918.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000005.0000000 0.274441918.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000005.0000000 0.274441918.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000005.0000000 0.274441918.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000005.0000000 0.274441918.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 00000005.0000000 0.274441918.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000005.0000000 0.274441918.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000005.0000000 0.274441918.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000005.0000000 0.274441918.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.fonts.com	explorer.exe, 00000005.0000000 0.274441918.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000005.0000000 0.274441918.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000005.0000000 0.274441918.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000005.0000000 0.274441918.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	NEW ORDER SOR 10531220.exe, 00 000000.00000002.244487250.0000 000002EE1000.00000004.00000001 .sdmp	false		high
http://www.sakkal.com	explorer.exe, 00000005.0000000 0.274441918.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.255.115.89	www.chjcsc.com	United States		7203	LEASEWEB-USA-SFO-12US	true
34.102.136.180	theglasshousenyc.com	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	411847
Start date:	12.05.2021
Start time:	07:43:24
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 7s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	NEW ORDER SOR 10531220.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:	29
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@9/1@3/2

EGA Information:	Failed
HDC Information:	• Successful, ratio: 38.3% (good quality ratio 35.1%) • Quality average: 75.8% • Quality standard deviation: 30.3%
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

Simulations

Behavior and APIs

Time	Type	Description
07:44:19	API Interceptor	1x Sleep call for process: NEW ORDER SOR 10531220.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
LEASEWEB-USA-SFO-12US	BANK-ACCOUNT. NUMBER.PDF.exe	Get hash	malicious	Browse	• 172.255.115.119
	126-21-11HAR.exe	Get hash	malicious	Browse	• 172.255.208.73
	PO#10244.exe	Get hash	malicious	Browse	• 23.82.175.79
	PI34567890987.exe	Get hash	malicious	Browse	• 23.82.175.79
	RDAx9iDSEL.exe	Get hash	malicious	Browse	• 147.255.162.204
	5PthEm83NG.exe	Get hash	malicious	Browse	• 147.255.162.204
	k7AgZOwF4S.exe	Get hash	malicious	Browse	• 147.255.162.204
	lFfDzzZYTl.exe	Get hash	malicious	Browse	• 147.255.162.204
	o52k2obPCG.exe	Get hash	malicious	Browse	• 147.255.162.204
	q3uHPdoxWP.exe	Get hash	malicious	Browse	• 147.255.162.204
	NMpDBwHJP8.exe	Get hash	malicious	Browse	• 23.82.57.32
	pCkqlKXv05.exe	Get hash	malicious	Browse	• 23.82.57.32
	PO-2021-UTITECH-.exe.exe	Get hash	malicious	Browse	• 23.106.92.110
	u87sEvt9v3.exe	Get hash	malicious	Browse	• 23.82.57.32
	Processed APR12.xlsx	Get hash	malicious	Browse	• 23.82.57.32
	36ne6xnkop.exe	Get hash	malicious	Browse	• 23.82.57.32
	Customer-100912288113.xlsx	Get hash	malicious	Browse	• 23.82.57.32
	KL9fcbfrMB.exe	Get hash	malicious	Browse	• 147.255.162.204
	rErRI1Ktbf.exe	Get hash	malicious	Browse	• 23.108.117.12
	Gt8AN6GiOD.exe	Get hash	malicious	Browse	• 23.82.57.32

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\NEW ORDER SOR 10531220.exe.log	
Process:	C:\Users\user\Desktop\NEW ORDER SOR 10531220.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..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=b77a

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.8695867721304396
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 SOR 10531220.exe
File size:	929792
MD5:	2e2de2014ccb06fea1b50414f5e301e6
SHA1:	b571217f877106966f056526c0fdb0068ebfcbff
SHA256:	f8ca257b6bbb8a0b617611a8ddb0068f056f3dc38eb525495978632b03964380
SHA512:	06359a6730f19363432e72f1fe4d85e8a12d5df2ee2ff00cd153da94bdb80086728f4ba3cd42966e61ba227cf844893ae7bc4cbb216e7668b8c7ac0c722e742
SSDEEP:	24576:zIIJQXHDDlVMhFhuEMCfWYwINNmBC/eXz2f:zIDZGhPzMCeKiUeXzi
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....P..&.....rD... ..`....@.. .....@.....

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4e4472
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:	0x9FBA10BA [Tue Dec 1 20:55:22 2054 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

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
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	0xe4420	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xe6000	0x5bc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xe8000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xe4404	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	
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	0xe2478	0xe2600	False	0.910225272639	data	7.87523328982	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xe6000	0x5bc	0x600	False	0.424479166667	data	4.11315545531	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xe8000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xe6090	0x32c	data		
RT_MANIFEST	0xe63cc	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

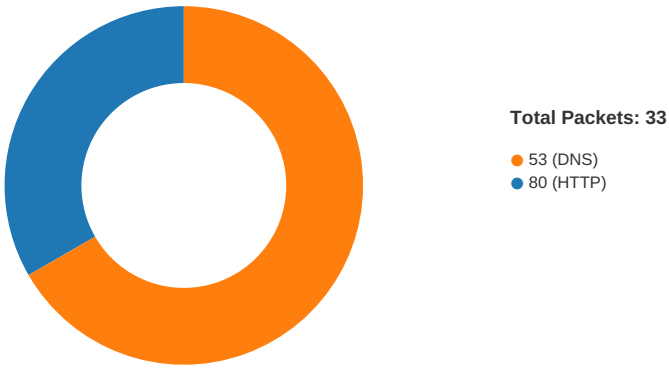
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2019
Assembly Version	1.0.0.0
InternalName	ValueTuple.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	WinFormBlur
ProductVersion	1.0.0.0
FileDescription	WinFormBlur
OriginalFilename	ValueTuple.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/12/21-07:45:57.680250	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49725	80	192.168.2.5	172.255.115.89
05/12/21-07:45:57.680250	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49725	80	192.168.2.5	172.255.115.89
05/12/21-07:45:57.680250	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49725	80	192.168.2.5	172.255.115.89
05/12/21-07:46:16.189912	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49727	80	192.168.2.5	34.102.136.180
05/12/21-07:46:16.189912	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49727	80	192.168.2.5	34.102.136.180
05/12/21-07:46:16.189912	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49727	80	192.168.2.5	34.102.136.180
05/12/21-07:46:16.327475	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49727	34.102.136.180	192.168.2.5

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 07:45:57.476780891 CEST	49725	80	192.168.2.5	172.255.115.89
May 12, 2021 07:45:57.679785013 CEST	80	49725	172.255.115.89	192.168.2.5
May 12, 2021 07:45:57.679990053 CEST	49725	80	192.168.2.5	172.255.115.89
May 12, 2021 07:45:57.680249929 CEST	49725	80	192.168.2.5	172.255.115.89
May 12, 2021 07:45:57.883593082 CEST	80	49725	172.255.115.89	192.168.2.5
May 12, 2021 07:45:57.883640051 CEST	80	49725	172.255.115.89	192.168.2.5
May 12, 2021 07:45:57.883668900 CEST	80	49725	172.255.115.89	192.168.2.5
May 12, 2021 07:45:57.883948088 CEST	49725	80	192.168.2.5	172.255.115.89
May 12, 2021 07:45:57.884073973 CEST	49725	80	192.168.2.5	172.255.115.89
May 12, 2021 07:45:57.884253025 CEST	49725	80	192.168.2.5	172.255.115.89
May 12, 2021 07:46:16.148560047 CEST	49727	80	192.168.2.5	34.102.136.180
May 12, 2021 07:46:16.189594030 CEST	80	49727	34.102.136.180	192.168.2.5
May 12, 2021 07:46:16.189714909 CEST	49727	80	192.168.2.5	34.102.136.180
May 12, 2021 07:46:16.189912081 CEST	49727	80	192.168.2.5	34.102.136.180
May 12, 2021 07:46:16.230925083 CEST	80	49727	34.102.136.180	192.168.2.5
May 12, 2021 07:46:16.327475071 CEST	80	49727	34.102.136.180	192.168.2.5
May 12, 2021 07:46:16.327513933 CEST	80	49727	34.102.136.180	192.168.2.5
May 12, 2021 07:46:16.327816010 CEST	49727	80	192.168.2.5	34.102.136.180
May 12, 2021 07:46:16.328022957 CEST	49727	80	192.168.2.5	34.102.136.180
May 12, 2021 07:46:16.369128942 CEST	80	49727	34.102.136.180	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 07:44:10.055042982 CEST	62060	53	192.168.2.5	8.8.8.8
May 12, 2021 07:44:10.113535881 CEST	53	62060	8.8.8.8	192.168.2.5
May 12, 2021 07:44:10.301431894 CEST	61805	53	192.168.2.5	8.8.8.8
May 12, 2021 07:44:10.366353035 CEST	53	61805	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 07:44:10.609643936 CEST	54795	53	192.168.2.5	8.8.8.8
May 12, 2021 07:44:10.658327103 CEST	53	54795	8.8.8.8	192.168.2.5
May 12, 2021 07:44:12.193048954 CEST	49557	53	192.168.2.5	8.8.8.8
May 12, 2021 07:44:12.241750956 CEST	53	49557	8.8.8.8	192.168.2.5
May 12, 2021 07:44:13.292526960 CEST	61733	53	192.168.2.5	8.8.8.8
May 12, 2021 07:44:13.342951059 CEST	53	61733	8.8.8.8	192.168.2.5
May 12, 2021 07:44:14.318603992 CEST	65447	53	192.168.2.5	8.8.8.8
May 12, 2021 07:44:14.367415905 CEST	53	65447	8.8.8.8	192.168.2.5
May 12, 2021 07:44:15.541054010 CEST	52441	53	192.168.2.5	8.8.8.8
May 12, 2021 07:44:15.589855909 CEST	53	52441	8.8.8.8	192.168.2.5
May 12, 2021 07:44:16.566256046 CEST	62176	53	192.168.2.5	8.8.8.8
May 12, 2021 07:44:16.614901066 CEST	53	62176	8.8.8.8	192.168.2.5
May 12, 2021 07:44:17.615890980 CEST	59596	53	192.168.2.5	8.8.8.8
May 12, 2021 07:44:17.664671898 CEST	53	59596	8.8.8.8	192.168.2.5
May 12, 2021 07:44:18.526763916 CEST	65296	53	192.168.2.5	8.8.8.8
May 12, 2021 07:44:18.587477922 CEST	53	65296	8.8.8.8	192.168.2.5
May 12, 2021 07:44:20.414697886 CEST	63183	53	192.168.2.5	8.8.8.8
May 12, 2021 07:44:20.463496923 CEST	53	63183	8.8.8.8	192.168.2.5
May 12, 2021 07:44:32.558574915 CEST	60151	53	192.168.2.5	8.8.8.8
May 12, 2021 07:44:32.620421886 CEST	53	60151	8.8.8.8	192.168.2.5
May 12, 2021 07:44:43.997464895 CEST	56969	53	192.168.2.5	8.8.8.8
May 12, 2021 07:44:44.054786921 CEST	53	56969	8.8.8.8	192.168.2.5
May 12, 2021 07:44:56.688585997 CEST	55161	53	192.168.2.5	8.8.8.8
May 12, 2021 07:44:56.760118008 CEST	53	55161	8.8.8.8	192.168.2.5
May 12, 2021 07:45:05.509707928 CEST	54757	53	192.168.2.5	8.8.8.8
May 12, 2021 07:45:05.567146063 CEST	53	54757	8.8.8.8	192.168.2.5
May 12, 2021 07:45:25.449173927 CEST	49992	53	192.168.2.5	8.8.8.8
May 12, 2021 07:45:25.517127991 CEST	53	49992	8.8.8.8	192.168.2.5
May 12, 2021 07:45:28.383513927 CEST	60075	53	192.168.2.5	8.8.8.8
May 12, 2021 07:45:28.444931984 CEST	53	60075	8.8.8.8	192.168.2.5
May 12, 2021 07:45:34.655599117 CEST	55016	53	192.168.2.5	8.8.8.8
May 12, 2021 07:45:34.866652966 CEST	53	55016	8.8.8.8	192.168.2.5
May 12, 2021 07:45:46.591283083 CEST	64345	53	192.168.2.5	8.8.8.8
May 12, 2021 07:45:46.653258085 CEST	53	64345	8.8.8.8	192.168.2.5
May 12, 2021 07:45:57.098051071 CEST	57128	53	192.168.2.5	8.8.8.8
May 12, 2021 07:45:57.469284058 CEST	53	57128	8.8.8.8	192.168.2.5
May 12, 2021 07:46:05.829041004 CEST	54791	53	192.168.2.5	8.8.8.8
May 12, 2021 07:46:05.901702881 CEST	53	54791	8.8.8.8	192.168.2.5
May 12, 2021 07:46:16.082046986 CEST	50463	53	192.168.2.5	8.8.8.8
May 12, 2021 07:46:16.146555901 CEST	53	50463	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 07:45:34.655599117 CEST	192.168.2.5	8.8.8.8	0xae22	Standard query (0)	www.social dating24.com	A (IP address)	IN (0x0001)
May 12, 2021 07:45:57.098051071 CEST	192.168.2.5	8.8.8.8	0x73fe	Standard query (0)	www.chjcsc.com	A (IP address)	IN (0x0001)
May 12, 2021 07:46:16.082046986 CEST	192.168.2.5	8.8.8.8	0xe6cc	Standard query (0)	www.thegla sshousenyc.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 07:45:34.866652966 CEST	8.8.8.8	192.168.2.5	0xae22	Name error (3)	www.social dating24.com	none	none	A (IP address)	IN (0x0001)
May 12, 2021 07:45:57.469284058 CEST	8.8.8.8	192.168.2.5	0x73fe	No error (0)	www.chjcsc.com		172.255.115.89	A (IP address)	IN (0x0001)
May 12, 2021 07:46:16.146555901 CEST	8.8.8.8	192.168.2.5	0xe6cc	No error (0)	www.thegla sshousenyc.com	theglasshousenyc.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 07:46:16.146555901 CEST	8.8.8.8	192.168.2.5	0xe6cc	No error (0)	theglassho usenyc.com		34.102.136.180	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.chjcsc.com
- www.theglasshousenyc.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49725	172.255.115.89	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 07:45:57.680249929 CEST	4608	OUT	GET /nyr/?hRXX=pvzb7SsULo7Y2vRo6lGAqy8tja7/7li767PDw0lqJEj7KBKEBSl8rkLevIquA9l06aH5&VBZDH=6l68xBo0LhJD2lv HTTP/1.1 Host: www.chjcsc.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 07:45:57.883593082 CEST	4608	IN	HTTP/1.1 200 OK Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Server: Nginx Microsoft-HTTPAPI/2.0 X-Powered-By: Nginx Date: Wed, 12 May 2021 05:46:06 GMT Connection: close Data Raw: 33 0d 0a ef bb bf 0d 0a Data Ascii: 3

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49727	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 07:46:16.189912081 CEST	4618	OUT	GET /nyr/?VBZDH=6l68xBo0LhJD2lv&hRXX=17hAXKnq4LEoTdb/hcwwVfWjS4IYRgMdOmXX52SprwB/nueYqi9a5dgIoxBN3QmuetP3 HTTP/1.1 Host: www.theglasshousenyc.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 07:46:16.327475071 CEST	4619	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 12 May 2021 05:46:16 GMT Content-Type: text/html Content-Length: 275 ETag: "609953da-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
PeekMessageA	INLINE	explorer.exe

Function Name	Hook Type	Active in Processes
PeekMessageW	INLINE	explorer.exe
GetMessageW	INLINE	explorer.exe
GetMessageA	INLINE	explorer.exe

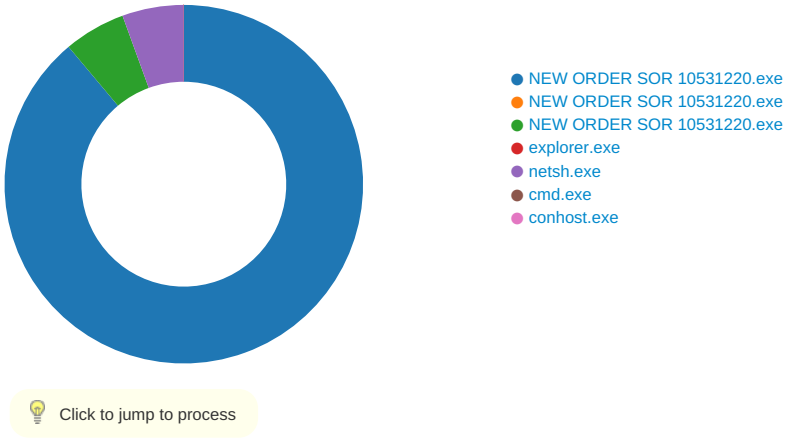
Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x8A 0xAE 0xE0
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x82 0x2E 0xE0
GetMessageW	INLINE	0x48 0x8B 0xB8 0x82 0x2E 0xE0
GetMessageA	INLINE	0x48 0x8B 0xB8 0x8A 0xAE 0xE0

Statistics

Behavior



System Behavior

Analysis Process: NEW ORDER SOR 10531220.exe PID: 3756 Parent PID: 5796

General

Start time:	07:44:17
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\NEW ORDER SOR 10531220.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\NEW ORDER SOR 10531220.exe'
Imagebase:	0xa70000
File size:	929792 bytes
MD5 hash:	2E2DE2014CCB06FEA1B50414F5E301E6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.245056631.0000000003EE9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.245056631.0000000003EE9000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.245056631.0000000003EE9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.244540222.0000000002F26000.00000004.00000001.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	6DAECF06	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	6DAECF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\NEW ORDER SOR 10531220.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDFC78D	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 SOR 10531220.exe.log	unknown	1314	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 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 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 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 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	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6DDFC907	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	6DAC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DAC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DA203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DACCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DA203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DA203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DA203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DA203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DAC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DAC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C931B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C931B4F	ReadFile

Analysis Process: NEW ORDER SOR 10531220.exe PID: 6164 Parent PID: 3756

General

Start time:	07:44:21
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\NEW ORDER SOR 10531220.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\NEW ORDER SOR 10531220.exe
Imagebase:	0x10000
File size:	929792 bytes
MD5 hash:	2E2DE2014CCB06FEA1B50414F5E301E6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: NEW ORDER SOR 10531220.exe PID: 6176 Parent PID: 3756

General

Start time:	07:44:21
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\NEW ORDER SOR 10531220.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\NEW ORDER SOR 10531220.exe
Imagebase:	0x5d0000
File size:	929792 bytes
MD5 hash:	2E2DE2014CCB06FEA1B50414F5E301E6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.305618158.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.305618158.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.305618158.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.305837682.0000000000B70000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.305837682.0000000000B70000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.305837682.0000000000B70000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.305819661.0000000000B40000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.305819661.0000000000B40000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.305819661.0000000000B40000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	419E57	NtReadFile

Analysis Process: explorer.exe PID: 3472 Parent PID: 6176

General

Start time:	07:44:26
Start date:	12/05/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff693d90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: netsh.exe PID: 7088 Parent PID: 3472

General

Start time:	07:44:48
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\netsh.exe

Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\netsh.exe
Imagebase:	0x1280000
File size:	82944 bytes
MD5 hash:	A0AA3322BB46BBFC36AB9DC1DBBBB807
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000002.502736423.0000000000980000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.502736423.0000000000980000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.502736423.0000000000980000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000002.504085150.0000000000BD0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.504085150.0000000000BD0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.504085150.0000000000BD0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000002.501752912.0000000000170000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.501752912.0000000000170000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.501752912.0000000000170000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	189E57	NtReadFile

Analysis Process: cmd.exe PID: 3552 Parent PID: 7088

General

Start time:	07:44:53
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\NEW ORDER SOR 10531220.exe'
Imagebase:	0xf30000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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

Analysis Process: conhost.exe PID: 5808 Parent PID: 3552

General

Start time:	07:44:54
Start date:	12/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis