**ID:** 502245
**Sample Name:** CNEW ORDER17.exe
**Cookbook:** default.jbs
**Time:** 18:34:34
**Date:** 13/10/2021
**Version:** 33.0.0 White Diamond

# Table of Contents

Table of Contents 2
Windows Analysis Report CNEW ORDER17.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: FormBook 4
Yara Overview 5
Memory Dumps 5
Unpacked PEs 6
Sigma Overview 6
Jbx Signature Overview 7
AV Detection: 7
Networking: 7
E-Banking Fraud: 7
System Summary: 7
Hooking and other Techniques for Hiding and Protection: 7
Malware Analysis System Evasion: 7
HIPS / PFW / Operating System Protection Evasion: 7
Stealing of Sensitive Information: 7
Remote Access Functionality: 7
Mitre Att&ck Matrix 8
Behavior Graph 8
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 10
Domains 10
URLs 11
Domains and IPs 11
Contacted Domains 11
Contacted URLs 11
Contacted IPs 11
General Information 11
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 12
IPs 12
Domains 12
ASN 12
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 12
Static File Info 13
General 13
File Icon 13
Static PE Info 14
General 14
Entrypoint Preview 14
Data Directories 14
Sections 14
Resources 14
Imports 14
Version Infos 14
Network Behavior 14
Code Manipulations 14
User Modules 14
Hook Summary 14
Processes 15
Statistics 15
Behavior 15
System Behavior 15
Analysis Process: CNEW ORDER17.exe PID: 4344 Parent PID: 3088 15
General 15
File Activities 15
File Created 15
File Written 15
File Read 15
Analysis Process: CNEW ORDER17.exe PID: 5680 Parent PID: 4344 15
General 16

File Activities 16
File Read 16
Analysis Process: explorer.exe PID: 3352 Parent PID: 5680 16
General 16
Analysis Process: raserver.exe PID: 4632 Parent PID: 5680 17
General 17
File Activities 17
File Read 17
Analysis Process: cmd.exe PID: 4476 Parent PID: 4632 18
General 18
File Activities 18
Analysis Process: conhost.exe PID: 6628 Parent PID: 4476 18
General 18
Disassembly 18
Code Analysis 18

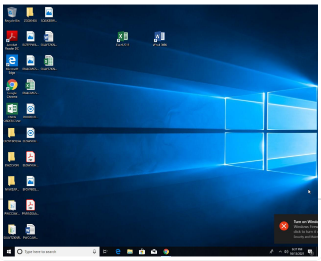
# Windows Analysis Report CNEW ORDER17.exe

## Overview

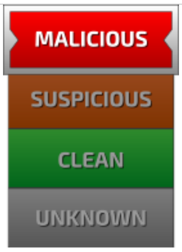
### General Information

| | |
|---|---|
| Sample Name: | CNEW ORDER17.exe |
| Analysis ID: | 502245 |
| MD5: | c54edc9ef9d72fe.. |
| SHA1: | 11dce70f33e490e. |
| SHA256: | 43fcb442b80665d. |
| Tags: | exe formbook |
| Infos: | |

Most interesting Screenshot:



### Detection



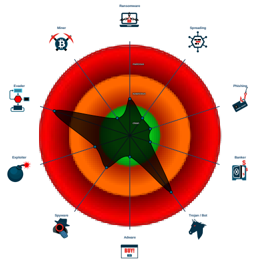
FormBook

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

### Signatures

- Found malware configuration
- Yara detected FormBook
- Malicious sample detected (through …
- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- 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 samp…
- Modifies the prolog of user mode fun…
- Self deletion via cmd delete
- Queues an APC in another process …

### Classification



## Process Tree

- **System is w10x64**
- CNEW ORDER17.exe (PID: 4344 cmdline: 'C:\Users\user\Desktop\CNEW ORDER17.exe'  MD5: C54EDC9EF9D72FE0FE048E8AC884626B)
  - CNEW ORDER17.exe (PID: 5680 cmdline: C:\Users\user\AppData\Local\Temp\CNEW ORDER17.exe MD5: C54EDC9EF9D72FE0FE048E8AC884626B)
    - explorer.exe (PID: 3352 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - raserver.exe (PID: 4632 cmdline: C:\Windows\SysWOW64\raserver.exe MD5: 2AADF65E395BFBD0D9B71D7279C8B5EC)
      - cmd.exe (PID: 4476 cmdline: /c del 'C:\Users\user\AppData\Local\Temp\CNEW ORDER17.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 6628 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

## Malware Configuration

### Threatname: FormBook

```
{
  "C2 list": [
    "www.cursoukulelegospel.com/h0c4/"
  ],
  "decoy": [
    "looknewly.com",
    "icha2016.com",
    "datnenhoalachn.xyz",
    "fark.ltd",
    "zjlj.site",
    "carpinteriacansino.com",
    "atozmp33.com",
    "oficialacesso.com",
    "tuningfrance.com",
    "rmm-mx96r.net",
    "outsidestyleshop.com",
    "eufundas.com",
    "a91furniture.com",
    "sfme.net",
    "englisch.coach",
    "wallacechen.info",
    "nyayeo.com",
    "jintongstore.com",
    "vanwerknaarwerk.info",
    "thekimlab.net",
    "morvirtualassistant.com",
    "ichatbengal.com",
    "doctors-technology.com",
    "mississippisms.com",
    "koopa.codes",
    "sproutheads.com",
    "gardenkitchenspa.com",
    "hoom.life",
    "wiselogistic.com",
    "appadaptor.com",
    "jumtix.xyz",
    "academiavirtualjjb.com",
    "pcmrmf.com",
    "hlsx069.com",
    "sunielkapoor.com",
    "truetaster.com",
    "rylautosales.com",
    "cgmobile.net",
    "www-inloggen-nl.info",
    "businesswebstrategy.net",
    "fetch-a-sg-hair-transplant.fyi",
    "paintingservicespune.com",
    "cakeeyes.net",
    "tandebrokers.com",
    "navigantcapitalpartners.com",
    "hubska.com",
    "foillaws.com",
    "battletraining.com",
    "bitcoin-recovery.com",
    "yourbuildvideos.com",
    "naturalsumaq.com",
    "prasikapsychotherapy.com",
    "jphousecleaningservices.com",
    "fetch-hepatitis-c.zone",
    "easypay-agent.com",
    "ronaldcraig.com",
    "highonloveshop.com",
    "bayharborislandhouse2.com",
    "aventuramaker.com",
    "han-chill.com",
    "wrapmeupbkk.com",
    "videomarketing.tips",
    "ishouldntbthareasonugohard.com",
    "psychotherapie-wermuth.com"
  ]
}
```

# Yara Overview

## Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000010.00000000.455090898.00000000079B 2000.00000040.00020000.sdmp | JoeSecurity_FormBook | Yara detected FormBook | Joe Security | |

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000010.00000000.455090898.00000000079B2000.00000040.00020000.sdmp | Formbook_1 | autogenerated rule brought to you by yara-signator | Felix Bilstein - yara-signator at cocacoding dot com | • 0x2685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94<br>• 0x2171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91<br>• 0x2787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F<br>• 0x28ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07<br>• 0x13ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8<br>• 0x84f7:$sequence_8: 3C 54 74 04 3C 74 75 F4<br>• 0x94fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00 |
| 00000010.00000000.455090898.00000000079B2000.00000040.00020000.sdmp | Formbook | detect Formbook in memory | JPCERT/CC Incident Response Group | • 0x5419:$sqlite3step: 68 34 1C 7B E1<br>• 0x552c:$sqlite3step: 68 34 1C 7B E1<br>• 0x5448:$sqlite3text: 68 38 2A 90 C5<br>• 0x556d:$sqlite3text: 68 38 2A 90 C5<br>• 0x545b:$sqlite3blob: 68 53 D8 7F 8C<br>• 0x5583:$sqlite3blob: 68 53 D8 7F 8C |
| 00000012.00000002.569532126.0000000000350000.00000004.00000001.sdmp | JoeSecurity_FormBook | Yara detected FormBook | Joe Security | |
| 00000012.00000002.569532126.0000000000350000.00000004.00000001.sdmp | Formbook_1 | autogenerated rule brought to you by yara-signator | Felix Bilstein - yara-signator at cocacoding dot com | • 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94<br>• 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91<br>• 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F<br>• 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07<br>• 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06<br>• 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8<br>• 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D<br>• 0x1b4f7:$sequence_8: 3C 54 74 04 3C 74 75 F4<br>• 0x1c4fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00 |

Click to see the 25 entries

## Unpacked PEs

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 15.2.CNEW ORDER17.exe.400000.0.unpack | JoeSecurity_FormBook | Yara detected FormBook | Joe Security | |
| 15.2.CNEW ORDER17.exe.400000.0.unpack | Formbook_1 | autogenerated rule brought to you by yara-signator | Felix Bilstein - yara-signator at cocacoding dot com | • 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0x8d62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0x14885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94<br>• 0x14371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91<br>• 0x14987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F<br>• 0x14aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07<br>• 0x977a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06<br>• 0x135ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8<br>• 0xa473:$sequence_7: 66 89 0C 02 5B 8B E5 5D<br>• 0x1a6f7:$sequence_8: 3C 54 74 04 3C 74 75 F4<br>• 0x1b6fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00 |
| 15.2.CNEW ORDER17.exe.400000.0.unpack | Formbook | detect Formbook in memory | JPCERT/CC Incident Response Group | • 0x17619:$sqlite3step: 68 34 1C 7B E1<br>• 0x1772c:$sqlite3step: 68 34 1C 7B E1<br>• 0x17648:$sqlite3text: 68 38 2A 90 C5<br>• 0x1776d:$sqlite3text: 68 38 2A 90 C5<br>• 0x1765b:$sqlite3blob: 68 53 D8 7F 8C<br>• 0x17783:$sqlite3blob: 68 53 D8 7F 8C |
| 15.2.CNEW ORDER17.exe.400000.0.raw.unpack | JoeSecurity_FormBook | Yara detected FormBook | Joe Security | |
| 15.2.CNEW ORDER17.exe.400000.0.raw.unpack | Formbook_1 | autogenerated rule brought to you by yara-signator | Felix Bilstein - yara-signator at cocacoding dot com | • 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94<br>• 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91<br>• 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F<br>• 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07<br>• 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06<br>• 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8<br>• 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D<br>• 0x1b4f7:$sequence_8: 3C 54 74 04 3C 74 75 F4<br>• 0x1c4fa:$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

## Jbx Signature Overview

Click to jump to signature section

### AV Detection:

- Found malware configuration
- Yara detected FormBook
- Antivirus / Scanner detection for submitted sample
- Antivirus detection for dropped file
- Machine Learning detection for sample
- Machine Learning detection for dropped file

### Networking:

- 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:

- Tries to detect virtualization through RDTSC time measurements

### HIPS / PFW / Operating System Protection Evasion:

- Sample uses process hollowing technique
- Maps a DLL or memory area into another process
- 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

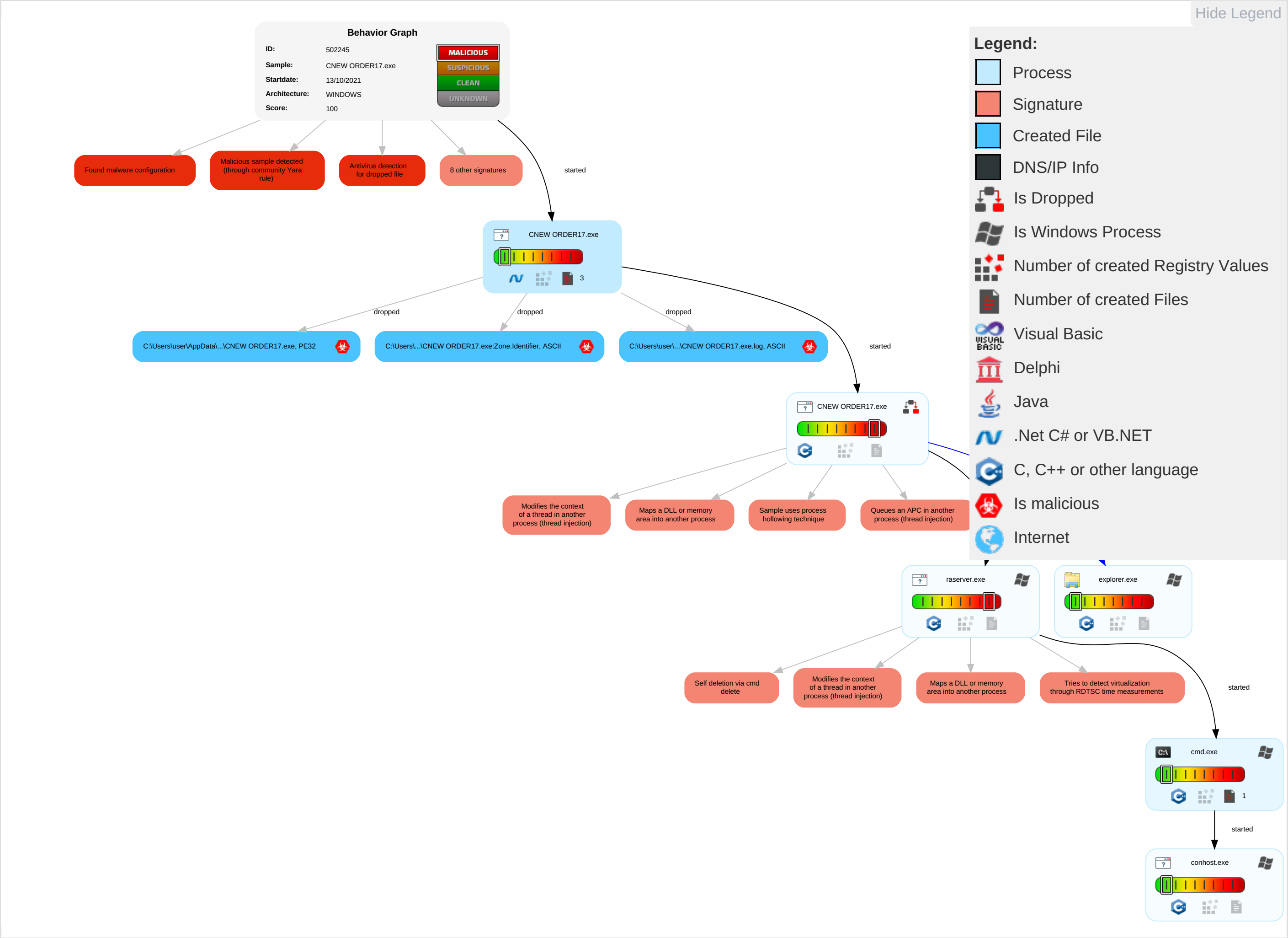
### Remote Access Functionality:

- 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Valid Accounts | Shared Modules 1 | Path Interception | Process Injection 4 1 2 | Rootkit 1 | Credential API Hooking 1 | Security Software Discovery 1 2 1 | Remote Services | Credential API Hooking 1 | Exfiltration Over Other Network Medium | Encrypted Channel 1 | Eavesdrop Insecure Network Communica |
| Default Accounts | Scheduled Task/Job | 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 | Application Layer Protocol 1 | Exploit SS7 Redirect Ph Calls/SMS |
| Domain Accounts | At (Linux) | Logon Script (Windows) | Logon Script (Windows) | Disable or Modify Tools 1 | Security Account Manager | Virtualization/Sandbox Evasion 3 1 | SMB/Windows Admin Shares | Archive Collected Data 1 | Automated Exfiltration | Steganography | Exploit SS7 Track Devic Location |
| Local Accounts | At (Windows) | Logon Script (Mac) | Logon Script (Mac) | Virtualization/Sandbox Evasion 3 1 | NTDS | Application Window Discovery 1 | Distributed Component Object Model | Input Capture | Scheduled Transfer | Protocol Impersonation | SIM Card Swap |
| Cloud Accounts | Cron | Network Logon Script | Network Logon Script | Process Injection 4 1 2 | LSA Secrets | System Information Discovery 1 1 2 | SSH | Keylogging | Data Transfer Size Limits | Fallback Channels | Manipulate Device Communica |
| Replication Through Removable Media | Launchd | Rc.common | Rc.common | Obfuscated Files or Information 3 | Cached Domain Credentials | System Owner/User Discovery | VNC | GUI Input Capture | Exfiltration Over C2 Channel | Multiband Communication | Jamming or Denial of Service |
| External Remote Services | Scheduled Task | Startup Items | Startup Items | Software Packing 3 | DCSync | Network Sniffing | Windows Remote Management | Web Portal Capture | Exfiltration Over Alternative Protocol | Commonly Used Port | Rogue Wi-F Access Poir |
| Drive-by Compromise | Command and Scripting Interpreter | Scheduled Task/Job | Scheduled Task/Job | Timestomp 1 | Proc Filesystem | Network Service Scanning | Shared Webroot | Credential API Hooking | Exfiltration Over Symmetric Encrypted Non-C2 Protocol | Application Layer Protocol | Downgrade Insecure Protocols |
| Exploit Public-Facing Application | PowerShell | At (Linux) | At (Linux) | File Deletion 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 Cellu Base Statioi |

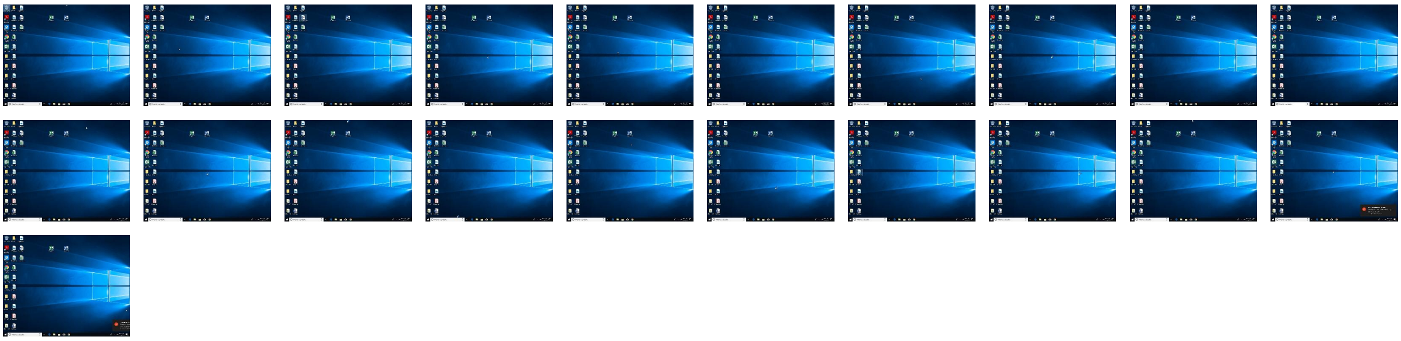
## Behavior Graph

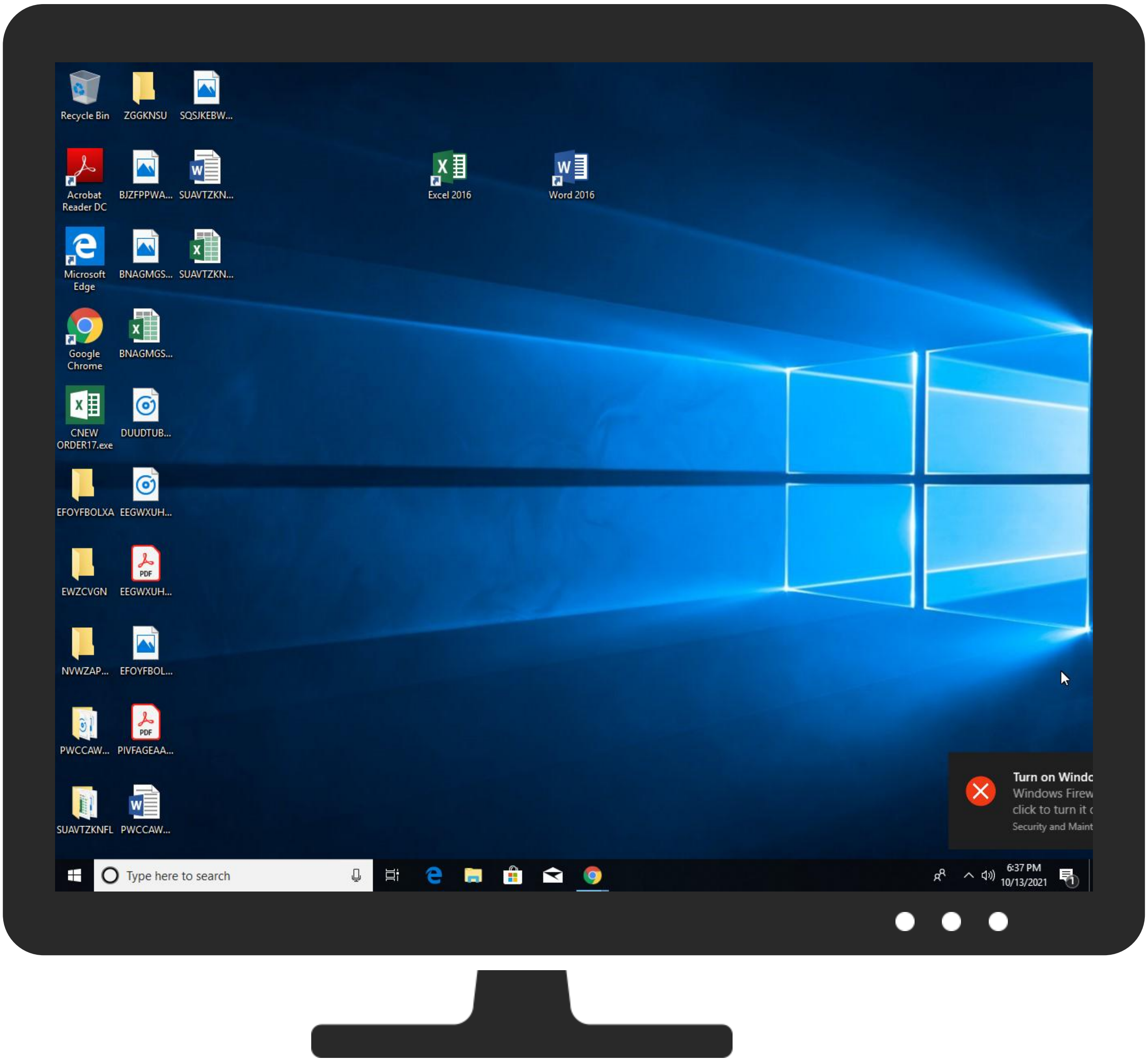

Hide Legend
Behavior Graph
ID: 502245
Sample: CNEW ORDER17.exe
Startdate: 13/10/2021
Architecture: WINDOWS
Score: 100
MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN
Found malware configuration
Malicious sample detected (through community Yara rule)
Antivirus detection for dropped file
8 other signatures
started
CNEW ORDER17.exe
3
dropped
dropped
dropped
C:\Users\user\AppData\...\CNEW ORDER17.exe, PE32
C:\Users\...\CNEW ORDER17.exe:Zone.Identifier, ASCII
C:\Users\user\...\CNEW ORDER17.exe.log, ASCII
started
CNEW ORDER17.exe
Modifies the context of a thread in another process (thread injection)
Maps a DLL or memory area into another process
Sample uses process hollowing technique
Queues an APC in another process (thread injection)
raserver.exe
explorer.exe
Self deletion via cmd delete
Modifies the context of a thread in another process (thread injection)
Maps a DLL or memory area into another process
Tries to detect virtualization through RDTSC time measurements
started
cmd.exe
1
started
conhost.exe
Legend:
Process
Signature
Created File
DNS/IP Info
Is Dropped
Is Windows Process
Number of created Registry Values
Number of created Files
Visual Basic
Delphi
Java
.Net C# or VB.NET
C, C++ or other language
Is malicious
Internet

## Screenshots

### Thumbnails

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





Turn on Windo
Windows Firew
click to turn it
Security and Maint

# Antivirus, Machine Learning and Genetic Malware Detection

## Initial Sample

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| CNEW ORDER17.exe | 100% | Avira | HEUR/AGEN.1142543 | |
| CNEW ORDER17.exe | 100% | Joe Sandbox ML | | |

## Dropped Files

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| C:\Users\user\AppData\Local\Temp\CNEW ORDER17.exe | 100% | Avira | HEUR/AGEN.1142543 | |
| C:\Users\user\AppData\Local\Temp\CNEW ORDER17.exe | 100% | Joe Sandbox ML | | |

## Unpacked PE Files

| Source | Detection | Scanner | Label | Link | Download |
|---|---|---|---|---|---|
| 0.0.CNEW ORDER17.exe.1a0000.0.unpack | 100% | Avira | HEUR/AGEN.1142543 | | Download File |
| 15.2.CNEW ORDER17.exe.4d0000.1.unpack | 100% | Avira | HEUR/AGEN.1142543 | | Download File |
| 15.0.CNEW ORDER17.exe.4d0000.0.unpack | 100% | Avira | HEUR/AGEN.1142543 | | Download File |
| 15.2.CNEW ORDER17.exe.400000.0.unpack | 100% | Avira | TR/Crypt.ZPACK.Gen | | Download File |
| 0.2.CNEW ORDER17.exe.1a0000.0.unpack | 100% | Avira | HEUR/AGEN.1142543 | | Download File |

## Domains

| No Antivirus matches |
|---|

### URLs

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| www.cursoukulelegospel.com/h0c4/ | 0% | Avira URL Cloud | safe | |

## Domains and IPs

### Contacted Domains

**No contacted domains info**

### Contacted URLs

| Name | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|
| www.cursoukulelegospel.com/h0c4/ | true | • Avira URL Cloud: safe | low |

### Contacted IPs

**No contacted IP infos**

## General Information

| | |
|---|---|
| Joe Sandbox Version: | 33.0.0 White Diamond |
| Analysis ID: | 502245 |
| Start date: | 13.10.2021 |
| Start time: | 18:34:34 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 9m 44s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | CNEW ORDER17.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: | 23 |
| Number of new started drivers analysed: | 0 |
| Number of existing processes analysed: | 0 |
| Number of existing drivers analysed: | 0 |
| Number of injected processes analysed: | 0 |
| Technologies: | • HCA enabled<br>• EGA enabled<br>• HDC enabled<br>• AMSI enabled |
| Analysis Mode: | default |
| Analysis stop reason: | Timeout |
| Detection: | MAL |
| Classification: | mal100.troj.evad.winEXE@8/3@0/0 |
| EGA Information: | Failed |
| HDC Information: | • Successful, ratio: 44% (good quality ratio 39.1%)<br>• Quality average: 68.5%<br>• Quality standard deviation: 33.4% |
| HCA Information: | • Successful, ratio: 100%<br>• Number of executed functions: 0<br>• Number of non-executed functions: 0 |
| Cookbook Comments: | • Adjust boot time<br>• Enable AMSI<br>• Found application associated with file extension: .exe |
| Warnings: | Show All |

# Simulations

## Behavior and APIs

**No simulations**

# Joe Sandbox View / Context

## IPs

**No context**

## Domains

**No context**

## ASN

**No context**

## JA3 Fingerprints

**No context**

## Dropped Files

**No context**

# Created / dropped Files

### C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\CNEW ORDER17.exe.log

| | |
|---|---|
| Process: | C:\Users\user\Desktop\CNEW ORDER17.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | modified |
| Size (bytes): | 425 |
| Entropy (8bit): | 5.340009400190196 |
| Encrypted: | false |
| SSDEEP: | 12:Q3La/KDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9I0ZKhav:ML9E4Ks2wKDE4KhK3VZ9pKhk |
| MD5: | CC144808DBAF00E03294347EADC8E779 |
| SHA1: | A3434FC71BA82B7512C813840427C687ADDB5AEA |
| SHA-256: | 3FC7B9771439E777A8F8B8579DD499F3EB90859AD30EFD8A765F341403FC7101 |
| SHA-512: | A4F9EB98200BCAF388F89AABAF7EA57661473687265597B13192C24F06638C6339A3BD581DF4E002F26EE1BA09410F6A2BBDB4DA0CD40B59D63A09BAA1AADD D |
| Malicious: | **true** |
| Reputation: | moderate, very likely benign file |
| Preview: | 1,"fusion","GAC",0..1,"WinRT","NotApp",1..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..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.. |

### C:\Users\user\AppData\Local\Temp\CNEW ORDER17.exe

| | |
|---|---|
| Process: | C:\Users\user\Desktop\CNEW ORDER17.exe |
| File Type: | PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows |
| Category: | dropped |
| Size (bytes): | 983040 |
| Entropy (8bit): | 7.643700581671609 |
| Encrypted: | false |
| SSDEEP: | 12288:lxGAAVPJ9rY0Vjf23ZgTJt8mwSwtpaYKXrEUpDK30dBlVhxYuWyrZFvn6+OhO:eAGNYoOiT/8mN+aYW4OHboirZFv6/ |

### C:\Users\user\AppData\Local\Temp\CNEW ORDER17.exe

| | |
|---|---|
| MD5: | C54EDC9EF9D72FE0FE048E8AC884626B |
| SHA1: | 11DCE70F33E490EB9B89726776915A374BB59A59 |
| SHA-256: | 43FCB442B80665D42271689310EBD569E84F74287063A62E14BEBA808178E098 |
| SHA-512: | C65D37DE77AD4598EE0B665145C988681D38FC26AA2EB2F5B5D1B73646EAA843CB18C4172D0ED7DCEE4BD25BDF692E7B1AACC410A56B6959158F9E3BAB1F0C81 |
| Malicious: | **true** |
| Antivirus: | • Antivirus: Avira, Detection: 100%<br>• Antivirus: Joe Sandbox ML, Detection: 100% |
| Reputation: | low |
| Preview: | MZ......................@...............................................!..L.!This program cannot be run in DOS mode....$.......PE..L....Y,................0..l..........j.... ........@.. .......................`.......... ..@....................................O............................@....................................................... ............... ..H............text...pj... ...l.................. ..`.rsrc................n..............@..@.rel oc.......@......................@..B................L.......H.......(#...............3...V..........................................~r...p(......-.(....*r...p(....*.0..H.......s......o....+..o.......(....(......(.....o.......(.... #......3@2..o....*.0..M.......(....(....o.......+2.....o....,"..( ...,..o!...r...p("...,..(....&..X....i2.*....0..4.......ri..p(#...r...p ............%.(....(.....o$...t....*.0.."........r...p .......o$....$......&...*.*......... .........(....*..0.......... .....%..... .....%.......i.&.....(%...r...po&...... |

### C:\Users\user\AppData\Local\Temp\CNEW ORDER17.exe:Zone.Identifier

| | |
|---|---|
| Process: | C:\Users\user\Desktop\CNEW ORDER17.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 26 |
| Entropy (8bit): | 3.95006375643621 |
| Encrypted: | false |
| SSDEEP: | 3:ggPYV:rPYV |
| MD5: | 187F488E27DB4AF347237FE461A079AD |
| SHA1: | 6693BA299EC1881249D59262276A0D2CB21F8E64 |
| SHA-256: | 255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309 |
| SHA-512: | 89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64 |
| Malicious: | **true** |
| Reputation: | high, very likely benign file |
| Preview: | [ZoneTransfer]....ZoneId=0 |

## Static File Info

### General

| | |
|---|---|
| File type: | PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows |
| Entropy (8bit): | 7.643700581671609 |
| TrID: | • Win32 Executable (generic) Net Framework (10011505/4) 49.83%<br>• Win32 Executable (generic) a (10002005/4) 49.78%<br>• Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36%<br>• Generic Win/DOS Executable (2004/3) 0.01%<br>• DOS Executable Generic (2002/1) 0.01% |
| File name: | CNEW ORDER17.exe |
| File size: | 983040 |
| MD5: | c54edc9ef9d72fe0fe048e8ac884626b |
| SHA1: | 11dce70f33e490eb9b89726776915a374bb59a59 |
| SHA256: | 43fcb442b80665d42271689310ebd569e84f74287063a62e14beba808178e098 |
| SHA512: | c65d37de77ad4598ee0b665145c988681d38fc26aa2eb2f5b5d1b73646eaa843cb18c4172d0ed7dcee4bd25bdf692e7b1aacc410a56b6959158f9e3bab1f0c81 |
| SSDEEP: | 12288:lxGAAVPJ9rY0Vjf23ZgTJt8mwSwtpaYKXrEUpDK30dBlVhxYuWyrZFvn6+OhO:eAGNYoOiT/8mN+aYW4OHboirZFv6/ |
| File Content Preview: | MZ......................@...............................................!..L.!This program cannot be run in DOS mode....$.......PE..L....Y,................0..l..........j.... ........@.. .......................`...........@................................ |

### File Icon

| | |
|---|---|
| Icon Hash: | 07d8d8d4d4d85026 |

## Static PE Info

### General

| | |
|---|---|
| Entrypoint: | 0x4c8a6a |
| 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: | 0xE32C5996 [Tue Oct 10 16:02:30 2090 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

### Data Directories

### Sections

| Name | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy | Characteristics |
|---|---|---|---|---|---|---|---|---|
| .text | 0x2000 | 0xc6a70 | 0xc6c00 | False | 0.997636595912 | data | 7.99906118019 | IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ |
| .rsrc | 0xca000 | 0x28f18 | 0x29000 | False | 0.0645364900915 | data | 3.05282770232 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .reloc | 0xf4000 | 0xc | 0x200 | False | 0.044921875 | data | 0.0980041756627 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ |

### Resources

### Imports

### Version Infos

# Network Behavior

**No network behavior found**

# 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 |

| Function Name | Hook Type | Active in Processes |
|---|---|---|
| GetMessageA | INLINE | explorer.exe |

### Processes

## Statistics

### Behavior

Click to jump to process

## System Behavior

### Analysis Process: CNEW ORDER17.exe PID: 4344 Parent PID: 3088

### General

| | |
|---|---|
| Start time: | 18:35:34 |
| Start date: | 13/10/2021 |
| Path: | C:\Users\user\Desktop\CNEW ORDER17.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Users\user\Desktop\CNEW ORDER17.exe' |
| Imagebase: | 0x1a0000 |
| File size: | 983040 bytes |
| MD5 hash: | C54EDC9EF9D72FE0FE048E8AC884626B |
| 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: 00000000.00000002.424773076.0000000003719000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.424773076.0000000003719000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.424773076.0000000003719000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group<br>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.424873904.00000000037B2000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.424873904.00000000037B2000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.424873904.00000000037B2000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group |
| Reputation: | low |

### File Activities

Show Windows behavior

#### File Created

#### File Written

#### File Read

### Analysis Process: CNEW ORDER17.exe PID: 5680 Parent PID: 4344

### General

| | |
|---|---|
| Start time: | 18:36:33 |
| Start date: | 13/10/2021 |
| Path: | C:\Users\user\AppData\Local\Temp\CNEW ORDER17.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Users\user\AppData\Local\Temp\CNEW ORDER17.exe |
| Imagebase: | 0x4d0000 |
| File size: | 983040 bytes |
| MD5 hash: | C54EDC9EF9D72FE0FE048E8AC884626B |
| 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.00000002.519487969.0000000000B30000.00000040.00020000.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.519487969.0000000000B30000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.519487969.0000000000B30000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group<br>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000002.518976654.0000000000400000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.518976654.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.518976654.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group<br>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000002.519680465.0000000000F70000.00000040.00020000.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.519680465.0000000000F70000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.519680465.0000000000F70000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group |
| Antivirus matches: | • Detection: 100%, Avira<br>• Detection: 100%, Joe Sandbox ML |
| Reputation: | low |

### File Activities

Show Windows behavior

#### File Read

## Analysis Process: explorer.exe PID: 3352 Parent PID: 5680

### General

| | |
|---|---|
| Start time: | 18:36:35 |
| Start date: | 13/10/2021 |
| Path: | C:\Windows\explorer.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\Explorer.EXE |
| Imagebase: | 0x7ff720ea0000 |
| File size: | 3933184 bytes |
| MD5 hash: | AD5296B280E8F522A8A897C96BAB0E1D |
| Has elevated privileges: | false |
| Has administrator privileges: | false |
| Programmed in: | C, C++ or other language |

| | |
|---|---|
| Yara matches: | • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000010.00000000.455090898.00000000079B2000.00000040.00020000.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000000.455090898.00000000079B2000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000000.455090898.00000000079B2000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group<br>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000010.00000000.472604115.00000000079B2000.00000040.00020000.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000000.472604115.00000000079B2000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000000.472604115.00000000079B2000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group |
| Reputation: | high |

## Analysis Process: raserver.exe PID: 4632 Parent PID: 5680

### General

| | |
|---|---|
| Start time: | 18:37:16 |
| Start date: | 13/10/2021 |
| Path: | C:\Windows\SysWOW64\raserver.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\SysWOW64\raserver.exe |
| Imagebase: | 0xc0000 |
| File size: | 108544 bytes |
| MD5 hash: | 2AADF65E395BFBD0D9B71D7279C8B5EC |
| 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: 00000012.00000002.569532126.0000000000350000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000002.569532126.0000000000350000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000012.00000002.569532126.0000000000350000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group<br>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000012.00000002.570686773.0000000002B40000.00000040.00020000.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000002.570686773.0000000002B40000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000012.00000002.570686773.0000000002B40000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group<br>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000012.00000002.570839920.0000000002E40000.00000040.00020000.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000002.570839920.0000000002E40000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000012.00000002.570839920.0000000002E40000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group |
| Reputation: | moderate |

### File Activities

Show Windows behavior

### File Read

## Analysis Process: cmd.exe PID: 4476 Parent PID: 4632

### General

| | |
|---|---|
| Start time: | 18:37:20 |
| Start date: | 13/10/2021 |
| Path: | C:\Windows\SysWOW64\cmd.exe |
| Wow64 process (32bit): | true |
| Commandline: | /c del 'C:\Users\user\AppData\Local\Temp\CNEW ORDER17.exe' |
| Imagebase: | 0xd80000 |
| 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

Show Windows behavior

## Analysis Process: conhost.exe PID: 6628 Parent PID: 4476

### General

| | |
|---|---|
| Start time: | 18:37:20 |
| Start date: | 13/10/2021 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff7f20f0000 |
| 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

Joe Sandbox Cloud Basic 33.0.0 White Diamond