

JOeSandbox Cloud BASIC



**ID:** 452476

**Sample Name:** Purchase  
Order.exe

**Cookbook:** default.jbs

**Time:** 13:17:13

**Date:** 22/07/2021

**Version:** 33.0.0 White Diamond

# Table of Contents







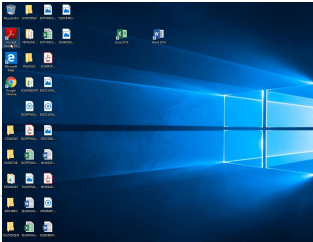
Table of Contents	2
Windows Analysis Report Purchase Order.exe	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Threatname: FormBook	4
Yara Overview	5
Memory Dumps	5
Unpacked PEs	6
Sigma Overview	7
Jbx Signature Overview	7
AV Detection:	7
Networking:	7
E-Banking Fraud:	7
System Summary:	7
Data Obfuscation:	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:	8
Remote Access Functionality:	8
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	10
Domains and IPs	12
Contacted Domains	12
Contacted URLs	12
URLs from Memory and Binaries	12
Contacted IPs	12
General Information	12
Simulations	13
Behavior and APIs	13
Joe Sandbox View / Context	13
IPs	13
Domains	13
ASN	13
JA3 Fingerprints	13
Dropped Files	14
Created / dropped Files	14
Static File Info	14
General	14
File Icon	14
Static PE Info	15
General	15
Entrypoint Preview	15
Data Directories	15
Sections	15
Resources	15
Imports	15
Version Infos	15
Network Behavior	15
Network Port Distribution	15
UDP Packets	15
DNS Queries	15
DNS Answers	15
Code Manipulations	16
User Modules	16
Hook Summary	16
Processes	16
Statistics	16
Behavior	16
System Behavior	16
Analysis Process: Purchase Order.exe PID: 1376 Parent PID: 5620	16

General	16
File Activities	17
File Created	17
File Written	17
File Read	17
Analysis Process: Purchase Order.exe PID: 1784 Parent PID: 1376	17
General	17
File Activities	17
File Read	17
Analysis Process: explorer.exe PID: 3388 Parent PID: 1784	17
General	17
File Activities	18
Analysis Process: cscript.exe PID: 5288 Parent PID: 3388	18
General	18
File Activities	18
File Read	18
Analysis Process: cmd.exe PID: 244 Parent PID: 5288	18
General	18
File Activities	19
Analysis Process: conhost.exe PID: 3596 Parent PID: 244	19
General	19
Disassembly	19
Code Analysis	19

# Windows Analysis Report Purchase Order.exe

## Overview

## General Information

Sample Name:	Purchase Order.exe
Analysis ID:	452476
MD5:	c13f1850e9d955f..
SHA1:	1329de0499fabc6..
SHA256:	419d8b92dc0428..
Tags:	exe
Infos:	     
Most interesting Screenshot:	
	

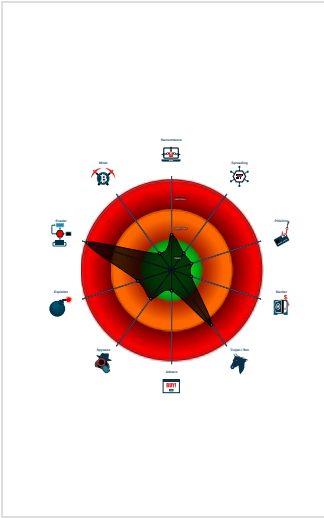
## Detection

[illegible]







## Signatures

- Found malware configuration
- Malicious sample detected (through ...)
- Multi AV Scanner detection for subm...
- System process connects to networ...
- Yara detected AntiVM3
- Yara detected FormBook
- .NET source code contains potentia...
- C2 URLs / IPs found in malware con...
- Initial sample is a PE file and has a ...
- Injects a PE file into a foreign proce...
- Machine Learning detection for samp...
- Maps a DLL or memory area into an...

## Classification



## Process Tree

- System is w10x64
-  **Purchase Order.exe** (PID: 1376 cmdline: 'C:\Users\user\Desktop\Purchase Order.exe' MD5: C13F1850E9D955F826620BD1AE322368)
  -  **Purchase Order.exe** (PID: 1784 cmdline: {path} MD5: C13F1850E9D955F826620BD1AE322368)
    -  **explorer.exe** (PID: 3388 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      -  **cscrip.exe** (PID: 5288 cmdline: C:\Windows\SysWOW64\cscrip.exe MD5: 00D3041E47F99E48DD5FFFEDEF60F6304)
        -  **cmd.exe** (PID: 244 cmdline: /c del 'C:\Users\user\Desktop\Purchase Order.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          -  **conhost.exe** (PID: 3596 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cleanup

## Malware Configuration

Threatname: FormBook

```

{
  "C2 list": [
    "www.valiantfinancial.net/hth0/"
  ],
  "decoy": [
    "grahamandjana.com",
    "surfpodcastnetwork.com",
    "valkyrie20.com",
    "hire4looks.com",
    "wewalkfastasone.com",
    "saveourschoolyear.com",
    "5g23e.com",
    "abusinesssystems.com",
    "telefonepantalla.com",
    "tailorscafe.com",
    "schwarzer-markt.net",
    "stopwatch247.com",
    "458grandbetting.com",
    "xpovision.com",
    "kutkingbarbering.life",
    "kppp-guxxz.xyz",
    "chuckwagon-chow.com",
    "la-casa-delle-vita.com",
    "creativesocials.com",
    "negociacioeshojebr.com",
    "conservativestyle.life",
    "82Stache.com",
    "birthmothersmaine.com",
    "jwrl.net",
    "gardiantparts.com",
    "contodosyparaelbiendetodos.com",
    "actymall.com",
    "oxyde.net",
    "adagiomusicacademy.com",
    "newjerseyscubadiving.net",
    "87oaks.com",
    "overt.website",
    "home-made-gifts.com",
    "viralgoats.com",
    "camediahub.com",
    "bankruptcyprobabilities.com",
    "yourlifematterswellness.email",
    "earnestjourneycourses.com",
    "londonpaints.com",
    "aeseigroup.com",
    "omegle99.com",
    "sparklinnomma.com",
    "cofcwzrf.com",
    "jam-nins.com",
    "mazacz.com",
    "copdrule.info",
    "cahayaqq.life",
    "helps-paxful.com",
    "gerado.online",
    "patanamedia.com",
    "fromfeartotrust.com",
    "deux-studios.com",
    "wallinders.com",
    "nilton-g.com",
    "yijianobile.com",
    "ocheap3dbuy.com",
    "flima2020a.site",
    "battlefieldtitle.site",
    "ferrebaviera.com",
    "plushmint.com",
    "achievementfound.com",
    "dontbringcovidhome.com",
    "cultigique.com",
    "waveplumb.com"
  ]
}

```

## Yara Overview

### Memory Dumps

Source	Rule	Description	Author	Strings
00000010.00000002.362458702.000000000400000.00000 040.00000001.sdmmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000010.00000002.362458702.0000000000400000.0000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	<ul style="list-style-type: none"> <li>0x98e8:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC</li> <li>0x9b62:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC</li> <li>0x15685:\$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94</li> <li>0x15171:\$sequence_2: 3B 4F 14 73 95 85 C9 74 91</li> <li>0x15787:\$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F</li> <li>0x158ff:\$sequence_4: 5D C3 8D 50 7C 80 FA 07</li> <li>0xa57a:\$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06</li> <li>0x143ec:\$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8</li> <li>0xb273:\$sequence_7: 66 89 0C 02 5B 8B E5 5D</li> <li>0x1b4f7:\$sequence_8: 3C 54 74 04 3C 74 75 F4</li> <li>0x1c4fa:\$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00</li> </ul>
00000010.00000002.362458702.0000000000400000.0000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	<ul style="list-style-type: none"> <li>0x18419:\$sqlite3step: 68 34 1C 7B E1</li> <li>0x1852c:\$sqlite3step: 68 34 1C 7B E1</li> <li>0x18448:\$sqlite3text: 68 38 2A 90 C5</li> <li>0x1856d:\$sqlite3text: 68 38 2A 90 C5</li> <li>0x1845b:\$sqlite3blob: 68 53 D8 7F 8C</li> <li>0x18583:\$sqlite3blob: 68 53 D8 7F 8C</li> </ul>
00000013.00000002.480809359.0000000001140000.0000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000013.00000002.480809359.0000000001140000.0000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	<ul style="list-style-type: none"> <li>0x98e8:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC</li> <li>0x9b62:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC</li> <li>0x15685:\$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94</li> <li>0x15171:\$sequence_2: 3B 4F 14 73 95 85 C9 74 91</li> <li>0x15787:\$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F</li> <li>0x158ff:\$sequence_4: 5D C3 8D 50 7C 80 FA 07</li> <li>0xa57a:\$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06</li> <li>0x143ec:\$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8</li> <li>0xb273:\$sequence_7: 66 89 0C 02 5B 8B E5 5D</li> <li>0x1b4f7:\$sequence_8: 3C 54 74 04 3C 74 75 F4</li> <li>0x1c4fa:\$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00</li> </ul>
Click to see the 18 entries				

## Unpacked PEs

Source	Rule	Description	Author	Strings
16.2.Purchase Order.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
16.2.Purchase Order.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	<ul style="list-style-type: none"> <li>0x98e8:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC</li> <li>0x9b62:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC</li> <li>0x15685:\$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94</li> <li>0x15171:\$sequence_2: 3B 4F 14 73 95 85 C9 74 91</li> <li>0x15787:\$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F</li> <li>0x158ff:\$sequence_4: 5D C3 8D 50 7C 80 FA 07</li> <li>0xa57a:\$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06</li> <li>0x143ec:\$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8</li> <li>0xb273:\$sequence_7: 66 89 0C 02 5B 8B E5 5D</li> <li>0x1b4f7:\$sequence_8: 3C 54 74 04 3C 74 75 F4</li> <li>0x1c4fa:\$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00</li> </ul>
16.2.Purchase Order.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	<ul style="list-style-type: none"> <li>0x18419:\$sqlite3step: 68 34 1C 7B E1</li> <li>0x1852c:\$sqlite3step: 68 34 1C 7B E1</li> <li>0x18448:\$sqlite3text: 68 38 2A 90 C5</li> <li>0x1856d:\$sqlite3text: 68 38 2A 90 C5</li> <li>0x1845b:\$sqlite3blob: 68 53 D8 7F 8C</li> <li>0x18583:\$sqlite3blob: 68 53 D8 7F 8C</li> </ul>
16.2.Purchase Order.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
16.2.Purchase Order.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	<ul style="list-style-type: none"> <li>0x8ae8:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC</li> <li>0x8d62:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC</li> <li>0x14885:\$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94</li> <li>0x14371:\$sequence_2: 3B 4F 14 73 95 85 C9 74 91</li> <li>0x14987:\$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F</li> <li>0x14aff:\$sequence_4: 5D C3 8D 50 7C 80 FA 07</li> <li>0x977a:\$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06</li> <li>0x135ec:\$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8</li> <li>0xa473:\$sequence_7: 66 89 0C 02 5B 8B E5 5D</li> <li>0x1a6f7:\$sequence_8: 3C 54 74 04 3C 74 75 F4</li> <li>0x1b6fa:\$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00</li> </ul>
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

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

### 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

### Data Obfuscation:



.NET source code contains potential unpacker

### 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)

Injects a PE file into a foreign processes

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

## Stealing of Sensitive Information:



Yara detected FormBook

## Remote Access Functionality:



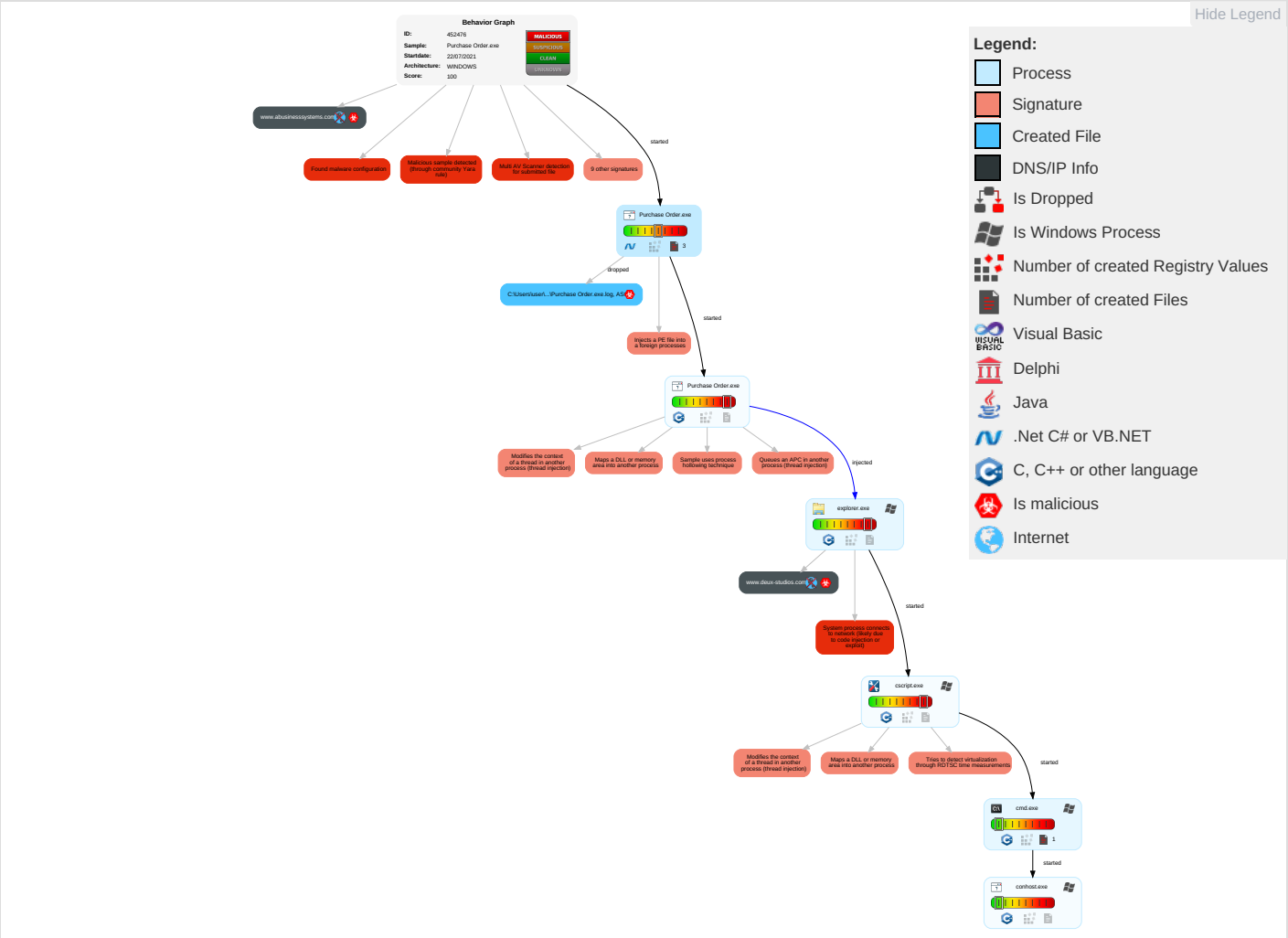
Yara detected FormBook

## 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 6 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 Communic
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Masquerading 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS Redirect P 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	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1 1	Exploit SS Track Devi 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	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 6 1 2	LSA Secrets	System Information Discovery 1 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communic
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 c 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 1 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrad Insecure Protocols

## Behavior Graph







## Antivirus, Machine Learning and Genetic Malware Detection

### Initial Sample

Source	Detection	Scanner	Label	Link
Purchase Order.exe	13%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
Purchase Order.exe	100%	Joe Sandbox ML		

### Dropped Files

No Antivirus matches

### Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
16.2.Purchase Order.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		<a href="#">Download File</a>

### Domains

No Antivirus matches

### URLs

Source	Detection	Scanner	Label	Link
<a href="http://www.jiyu-kobo.co.jp/lt">http://www.jiyu-kobo.co.jp/lt</a>	0%	Virustotal		<a href="#">Browse</a>

Source	Detection	Scanner	Label	Link
<a href="http://www.jiyu-kobo.co.jp/lt">http://www.jiyu-kobo.co.jp/lt</a>	0%	Avira URL Cloud	safe	
<a href="http://www.fontbureau.comsivao">http://www.fontbureau.comsivao</a>	0%	Avira URL Cloud	safe	
<a href="http://www.jiyu-kobo.co.jp/2o">http://www.jiyu-kobo.co.jp/2o</a>	0%	Avira URL Cloud	safe	
<a href="http://www.jiyu-kobo.co.jp/Co">http://www.jiyu-kobo.co.jp/Co</a>	0%	Avira URL Cloud	safe	
<a href="http://www.founder.com.cn/cn/bThe">http://www.founder.com.cn/cn/bThe</a>	0%	URL Reputation	safe	
<a href="http://www.founder.com.cn/cn/bThe">http://www.founder.com.cn/cn/bThe</a>	0%	URL Reputation	safe	
<a href="http://www.founder.com.cn/cn/bThe">http://www.founder.com.cn/cn/bThe</a>	0%	URL Reputation	safe	
<a href="http://www.jiyu-kobo.co.jp/ue">http://www.jiyu-kobo.co.jp/ue</a>	0%	URL Reputation	safe	
<a href="http://www.jiyu-kobo.co.jp/ue">http://www.jiyu-kobo.co.jp/ue</a>	0%	URL Reputation	safe	
<a href="http://www.jiyu-kobo.co.jp/ue">http://www.jiyu-kobo.co.jp/ue</a>	0%	URL Reputation	safe	
<a href="http://www.jiyu-kobo.co.jp/o">http://www.jiyu-kobo.co.jp/o</a>	0%	Avira URL Cloud	safe	
<a href="http://www.tiro.com">http://www.tiro.com</a>	0%	URL Reputation	safe	
<a href="http://www.tiro.com">http://www.tiro.com</a>	0%	URL Reputation	safe	
<a href="http://www.tiro.com">http://www.tiro.com</a>	0%	URL Reputation	safe	
<a href="http://www.fontbureau.comd-o">http://www.fontbureau.comd-o</a>	0%	Avira URL Cloud	safe	
<a href="http://www.goodfont.co.kr">http://www.goodfont.co.kr</a>	0%	URL Reputation	safe	
<a href="http://www.goodfont.co.kr">http://www.goodfont.co.kr</a>	0%	URL Reputation	safe	
<a href="http://www.goodfont.co.kr">http://www.goodfont.co.kr</a>	0%	URL Reputation	safe	
<a href="http://www.jiyu-kobo.co.jp/uo">http://www.jiyu-kobo.co.jp/uo</a>	0%	Avira URL Cloud	safe	
<a href="http://www.carterandcone.com">http://www.carterandcone.com</a>	0%	URL Reputation	safe	
<a href="http://www.carterandcone.com">http://www.carterandcone.com</a>	0%	URL Reputation	safe	
<a href="http://www.carterandcone.com">http://www.carterandcone.com</a>	0%	URL Reputation	safe	
<a href="http://www.founder.com.cn/cnoupyt">http://www.founder.com.cn/cnoupyt</a>	0%	Avira URL Cloud	safe	
<a href="http://www.fontbureau.com.TTFuo">http://www.fontbureau.com.TTFuo</a>	0%	Avira URL Cloud	safe	
<a href="http://www.sajatypeworks.com">http://www.sajatypeworks.com</a>	0%	URL Reputation	safe	
<a href="http://www.sajatypeworks.com">http://www.sajatypeworks.com</a>	0%	URL Reputation	safe	
<a href="http://www.sajatypeworks.com">http://www.sajatypeworks.com</a>	0%	URL Reputation	safe	
<a href="http://www.typography.netD">http://www.typography.netD</a>	0%	URL Reputation	safe	
<a href="http://www.typography.netD">http://www.typography.netD</a>	0%	URL Reputation	safe	
<a href="http://www.typography.netD">http://www.typography.netD</a>	0%	URL Reputation	safe	
<a href="http://www.founder.com.cn/cn/cThe">http://www.founder.com.cn/cn/cThe</a>	0%	URL Reputation	safe	
<a href="http://www.founder.com.cn/cn/cThe">http://www.founder.com.cn/cn/cThe</a>	0%	URL Reputation	safe	
<a href="http://www.founder.com.cn/cn/cThe">http://www.founder.com.cn/cn/cThe</a>	0%	URL Reputation	safe	
<a href="http://www.galapagosdesign.com/staff/dennis.htm">http://www.galapagosdesign.com/staff/dennis.htm</a>	0%	URL Reputation	safe	
<a href="http://www.galapagosdesign.com/staff/dennis.htm">http://www.galapagosdesign.com/staff/dennis.htm</a>	0%	URL Reputation	safe	
<a href="http://www.galapagosdesign.com/staff/dennis.htm">http://www.galapagosdesign.com/staff/dennis.htm</a>	0%	URL Reputation	safe	
<a href="http://fontfabrik.com">http://fontfabrik.com</a>	0%	URL Reputation	safe	
<a href="http://fontfabrik.com">http://fontfabrik.com</a>	0%	URL Reputation	safe	
<a href="http://fontfabrik.com">http://fontfabrik.com</a>	0%	URL Reputation	safe	
<a href="http://www.founder.com.cn/cngib">http://www.founder.com.cn/cngib</a>	0%	Avira URL Cloud	safe	
<a href="http://www.founder.com.cn/cnt">http://www.founder.com.cn/cnt</a>	0%	URL Reputation	safe	
<a href="http://www.founder.com.cn/cnt">http://www.founder.com.cn/cnt</a>	0%	URL Reputation	safe	
<a href="http://www.founder.com.cn/cnt">http://www.founder.com.cn/cnt</a>	0%	URL Reputation	safe	
<a href="http://www.galapagosdesign.com/DPlease">http://www.galapagosdesign.com/DPlease</a>	0%	URL Reputation	safe	
<a href="http://www.galapagosdesign.com/DPlease">http://www.galapagosdesign.com/DPlease</a>	0%	URL Reputation	safe	
<a href="http://www.galapagosdesign.com/DPlease">http://www.galapagosdesign.com/DPlease</a>	0%	URL Reputation	safe	
<a href="http://www.jiyu-kobo.co.jp/Y0">http://www.jiyu-kobo.co.jp/Y0</a>	0%	URL Reputation	safe	
<a href="http://www.jiyu-kobo.co.jp/Y0">http://www.jiyu-kobo.co.jp/Y0</a>	0%	URL Reputation	safe	
<a href="http://www.jiyu-kobo.co.jp/Y0">http://www.jiyu-kobo.co.jp/Y0</a>	0%	URL Reputation	safe	
<a href="http://www.sandoll.co.kr">http://www.sandoll.co.kr</a>	0%	URL Reputation	safe	
<a href="http://www.sandoll.co.kr">http://www.sandoll.co.kr</a>	0%	URL Reputation	safe	
<a href="http://www.sandoll.co.kr">http://www.sandoll.co.kr</a>	0%	URL Reputation	safe	
<a href="http://www.urwpp.deDPlease">http://www.urwpp.deDPlease</a>	0%	URL Reputation	safe	
<a href="http://www.urwpp.deDPlease">http://www.urwpp.deDPlease</a>	0%	URL Reputation	safe	
<a href="http://www.urwpp.deDPlease">http://www.urwpp.deDPlease</a>	0%	URL Reputation	safe	
<a href="http://www.zhongyicts.com.cn">http://www.zhongyicts.com.cn</a>	0%	URL Reputation	safe	
<a href="http://www.zhongyicts.com.cn">http://www.zhongyicts.com.cn</a>	0%	URL Reputation	safe	
<a href="http://www.zhongyicts.com.cn">http://www.zhongyicts.com.cn</a>	0%	URL Reputation	safe	
<a href="http://www.carterandcone.como">http://www.carterandcone.como</a>	0%	URL Reputation	safe	
<a href="http://www.carterandcone.como">http://www.carterandcone.como</a>	0%	URL Reputation	safe	
<a href="http://www.carterandcone.como">http://www.carterandcone.como</a>	0%	URL Reputation	safe	
<a href="http://www.sakkal.com">http://www.sakkal.com</a>	0%	URL Reputation	safe	
<a href="http://www.sakkal.com">http://www.sakkal.com</a>	0%	URL Reputation	safe	
<a href="http://www.sakkal.com">http://www.sakkal.com</a>	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.fontbureau.com.TTF	0%	URL Reputation	safe	
http://www.fontbureau.com.TTF	0%	URL Reputation	safe	
http://www.fontbureau.com.TTF	0%	URL Reputation	safe	
http://www.fontbureau.com=	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Ko	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnoup	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.agfamonotype.	0%	URL Reputation	safe	
http://www.agfamonotype.	0%	URL Reputation	safe	
http://www.agfamonotype.	0%	URL Reputation	safe	
http://www.carterandcone.comcr	0%	Avira URL Cloud	safe	
www.valiantfinancial.net/hth0/	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.come.com	0%	URL Reputation	safe	
http://www.fontbureau.come.com	0%	URL Reputation	safe	
http://www.fontbureau.come.com	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.founder.com.cn/cnmpa-u	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.carterandcone.comof	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.carterandcone.comtGi	0%	Avira URL Cloud	safe	

## Domains and IPs

### Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.deux-studios.com	unknown	unknown	true		unknown
www.abusinesssystems.com	unknown	unknown	true		unknown

### Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.valiantfinancial.net/hth0/	true	<ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul>	low

## URLs from Memory and Binaries

### Contacted IPs

No contacted IP infos

## General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	452476
Start date:	22.07.2021
Start time:	13:17:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Purchase 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:	28
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:	<ul style="list-style-type: none"> <li>• HCA enabled</li> <li>• EGA enabled</li> <li>• HDC enabled</li> <li>• AMSI enabled</li> </ul>
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/1@2/0
EGA Information:	Failed
HDC Information:	<ul style="list-style-type: none"> <li>• Successful, ratio: 12.6% (good quality ratio 10.3%)</li> <li>• Quality average: 64.4%</li> <li>• Quality standard deviation: 37%</li> </ul>
HCA Information:	<ul style="list-style-type: none"> <li>• Successful, ratio: 96%</li> <li>• Number of executed functions: 0</li> <li>• Number of non-executed functions: 0</li> </ul>
Cookbook Comments:	<ul style="list-style-type: none"> <li>• Adjust boot time</li> <li>• Enable AMSI</li> <li>• Found application associated with file extension: .exe</li> </ul>
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\Purchase Order.exe.log	
Process:	C:\Users\user\Desktop\Purchase Order.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCFF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F6
Malicious:	true
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089", "C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\l1d8480152e0da9a60ad49c6d16a3b6d\System.Core.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\l1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a", "C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089", "C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

Static File Info

General	
File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.09707815679182
TrID:	<ul style="list-style-type: none"><li>Win32 Executable (generic) Net Framework (10011505/4) 49.83%</li><li>Win32 Executable (generic) a (10002005/4) 49.78%</li><li>Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36%</li><li>Generic Win/DOS Executable (2004/3) 0.01%</li><li>DOS Executable Generic (2002/1) 0.01%</li></ul>
File name:	Purchase Order.exe
File size:	938496
MD5:	c13f1850e9d955f826620bd1ae322368
SHA1:	1329de0499fabc6fcffd4fa02864968acaac253e
SHA256:	419d8b92dc042882bb3261de70dfe4a158bc9ca436c71f9bf330bb8a6917d04c
SHA512:	8d11bbe6afadbd108f227bb3397334f27eb69859b19e82ae436ea91a9f9b6b786c83a55a2fe0f71b15875ec51df8b19f367941420e5972eb2a06e6163aed2657
SSDEEP:	12288:a+pvoEou45e3hi0CnMBUajS9VF/yEWmym5sD+cSMPQipP5q:a+pvZGe3encUNjFaEWmfipQ
File Content Preview:	MZ.....@.....!..L!Th is program cannot be run in DOS mode....\$.PE.L....`.....0..j.....^.....@.....@.....

File Icon



Icon Hash: f0debeffdf fec70

Static PE Info

General	
Entrypoint:	0x48885e
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:	0x60F8B8F5 [Thu Jul 22 00:16:53 2021 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	0x86864	0x86a00	False	0.862472435005	data	7.75016432791	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x8a000	0x5e320	0x5e400	False	0.167326342838	data	5.6405677251	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xea000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 22, 2021 13:19:57.076951027 CEST	192.168.2.3	8.8.8.8	0xee55	Standard query (0)	www.deux-studios.com	A (IP address)	IN (0x0001)
Jul 22, 2021 13:20:17.673424959 CEST	192.168.2.3	8.8.8.8	0x7fcc	Standard query (0)	www.abusinesssystem.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 13:19:57.153218985 CEST	8.8.8.8	192.168.2.3	0xee55	Name error (3)	www.deux-studios.com	none	none	A (IP address)	IN (0x0001)
Jul 22, 2021 13:20:17.736171007 CEST	8.8.8.8	192.168.2.3	0x7fcc	Name error (3)	www.abusinesssystems.com	none	none	A (IP address)	IN (0x0001)

## 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

## Statistics

### Behavior



Click to jump to process

## System Behavior

Analysis Process: Purchase Order.exe PID: 1376 Parent PID: 5620

### General

Start time:	13:18:09
Start date:	22/07/2021
Path:	C:\Users\user\Desktop\Purchase Order.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Purchase Order.exe'
Imagebase:	0x830000
File size:	938496 bytes
MD5 hash:	C13F1850E9D955F826620BD1AE322368
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	<ul style="list-style-type: none"><li>Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.308021841.0000000002CD8000.00000004.00000001.sdmp, Author: Joe Security</li><li>Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.308917029.0000000003C71000.00000004.00000001.sdmp, Author: Joe Security</li><li>Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.308917029.0000000003C71000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com</li><li>Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.308917029.0000000003C71000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group</li></ul>
Reputation:	low



## File Activities

Show Windows behavior

## File Created

## File Written

## File Read

## Analysis Process: Purchase Order.exe PID: 1784 Parent PID: 1376

## General

Start time:	13:18:50
Start date:	22/07/2021
Path:	C:\Users\user\Desktop\Purchase Order.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xc90000
File size:	938496 bytes
MD5 hash:	C13F1850E9D955F826620BD1AE322368
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	<ul style="list-style-type: none"><li>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000010.00000002.362458702.0000000000400000.00000040.00000001.sdmp, Author: Joe Security</li><li>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.362458702.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com</li><li>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000002.362458702.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group</li><li>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000010.00000002.363133642.0000000001720000.00000040.00000001.sdmp, Author: Joe Security</li><li>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.363133642.0000000001720000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com</li><li>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000002.363133642.0000000001720000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group</li><li>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000010.00000002.363097654.00000000016F0000.00000040.00000001.sdmp, Author: Joe Security</li><li>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.363097654.00000000016F0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com</li><li>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000002.363097654.00000000016F0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group</li></ul>
Reputation:	low

## File Activities

Show Windows behavior

## File Read

## Analysis Process: explorer.exe PID: 3388 Parent PID: 1784

## General

Start time:	13:18:53
Start date:	22/07/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff714890000

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

Show Windows behavior

Analysis Process: cscript.exe PID: 5288 Parent PID: 3388

General

Start time:	13:19:16
Start date:	22/07/2021
Path:	C:\Windows\SysWOW64\cscript.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cscript.exe
Imagebase:	0x11a0000
File size:	143360 bytes
MD5 hash:	00D3041E47F99E48DD5FFFE60F6304
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	<ul style="list-style-type: none"><li>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000013.00000002.480809359.0000000001140000.00000040.00000001.sdmp, Author: Joe Security</li><li>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000013.00000002.480809359.0000000001140000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com</li><li>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000013.00000002.480809359.0000000001140000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group</li><li>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000013.00000002.479738533.0000000000D50000.00000040.00000001.sdmp, Author: Joe Security</li><li>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000013.00000002.479738533.0000000000D50000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com</li><li>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000013.00000002.479738533.0000000000D50000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group</li><li>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000013.00000002.480997579.0000000001170000.00000004.00000001.sdmp, Author: Joe Security</li><li>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000013.00000002.480997579.0000000001170000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com</li><li>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000013.00000002.480997579.0000000001170000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group</li></ul>
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 244 Parent PID: 5288

General

Start time:	13:19:19
Start date:	22/07/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\Purchase Order.exe'

Imagebase:	0xbd0000
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: 3596 Parent PID: 244

### General

Start time:	13:19:19
Start date:	22/07/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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