**ID:** 502357
**Sample Name:** Factura de proforma.exe
**Cookbook:** default.jbs
**Time:** 20:33:12
**Date:** 13/10/2021
**Version:** 33.0.0 White Diamond

# Table of Contents

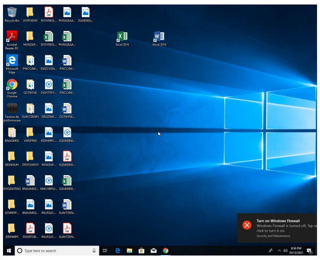
# Windows Analysis Report Factura de proforma.exe

## Overview

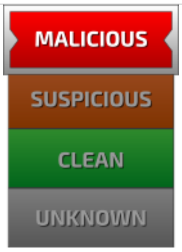
### General Information

| | |
|---|---|
| Sample Name: | Factura de proforma.exe |
| Analysis ID: | 502357 |
| MD5: | 16f7045eebb4512. |
| SHA1: | 99e8f263f9e34ad.. |
| SHA256: | ff344e635b26809.. |
| Tags: | ESP exe geo |
| Infos: | |

Most interesting Screenshot:



### Detection



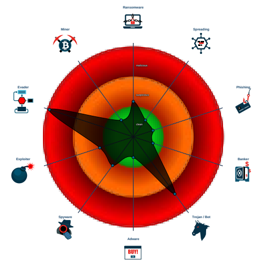

FormBook

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

### Signatures

- Found malware configuration
- Yara detected FormBook
- Malicious sample detected (through …
- Yara detected AntiVM3
- System process connects to networ…
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Sigma detected: Bad Opsec Default…
- Tries to detect sandboxes and other…
- Performs DNS queries to domains w…
- Modifies the prolog of user mode fun…
- .NET source code contains potentia…
- Queues an APC in another process …
- Tries to detect virtualization through…
- Modifies the context of a thread in a…

### Classification



## Process Tree

- System is w10x64
- Factura de proforma.exe (PID: 6952 cmdline: 'C:\Users\user\Desktop\Factura de proforma.exe' MD5: 16F7045EEBB451234CA8078222C5994C)
  - schtasks.exe (PID: 6436 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\tskpCbAwtxoaw' /XML 'C:\Users\user\AppData\Local\Temp\tmpD689.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6824 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 6388 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
    - explorer.exe (PID: 3352 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - cscript.exe (PID: 4716 cmdline: C:\Windows\SysWOW64\cscript.exe MD5: 00D3041E47F99E48DD5FFFEDF60F6304)
        - cmd.exe (PID: 3408 cmdline: /c del 'C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6960 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cleanup

## Malware Configuration

### Threatname: FormBook

```
{
  "C2 list": [
    "www.thefanlounge.com/cb3b/"
  ],
  "decoy": [
    "listenlocker.com",
    "jumpstartnotarybiz.com",
    "new-post-vehicle-site.xyz",
    "summon-entertainment.com",
    "johnandtracy-adopt.com",
    "bferety.info",
    "palmonlae.space",
    "yx1889.com",
    "janetnaufranck.com",
    "banditanalytics.com",
    "agenciahologram.com",
    "artemojo.com",
    "goldensuninn.com",
    "aminobalm.com",
    "customersme.com",
    "techcareerschool.com",
    "angelahuckeby.com",
    "smoothcontract.com",
    "kartsorgumerkezi.com",
    "houstonhemorrhoidclinic.com",
    "istanbuloz.com",
    "buyrealestatewithcarlos.com",
    "onlinelivehds.xyz",
    "outstandingearth.com",
    "cyclingsunglassestop.com",
    "haras-dors.com",
    "zhuanyekf.com",
    "pps-squad.com",
    "highlovely.com",
    "hudsonvalleymomandpopshop.com",
    "graytielaw.com",
    "orang-gilakali.com",
    "sajaasboutique.com",
    "nwomakrom.com",
    "mobilne-kucice.com",
    "instant-geek.com",
    "brewinginthenameof.com",
    "shopstel.net",
    "alumaber.com",
    "fernoost.info",
    "expandablepocketdeals.com",
    "ritelard.net",
    "elderyochanan.com",
    "gofante.online",
    "americansforbrazil.com",
    "condosofcolor.com",
    "the2gaku.com",
    "mesegeka.com",
    "democratsforesteban.com",
    "vinoporfavor.com",
    "xwaxxc1.com",
    "jinhongtextile.com",
    "festival-du-chanvre.com",
    "abrasivburada.com",
    "pinhoti.net",
    "nestd.online",
    "fendlercart.com",
    "unanox.com",
    "boyscout-site.com",
    "wlctrade.com",
    "gudesigns.net",
    "jandmisia.com",
    "funnyp0sts.com",
    "laveudelamare.com"
  ]
}
```


# Yara Overview

## Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000006.00000002.402637395.0000000001500000.00000040.00020000.sdmp | JoeSecurity_FormBook | Yara detected FormBook | Joe Security | |

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000006.00000002.402637395.0000000001500000.00000040.00020000.sdmp | Formbook_1 | autogenerated rule brought to you by yara-signator | Felix Bilstein - yara-signator at cocacoding dot com | • 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94<br>• 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91<br>• 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F<br>• 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07<br>• 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06<br>• 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8<br>• 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D<br>• 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4<br>• 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00 |
| 00000006.00000002.402637395.0000000001500000.00000040.00020000.sdmp | Formbook | detect Formbook in memory | JPCERT/CC Incident Response Group | • 0x18849:$sqlite3step: 68 34 1C 7B E1<br>• 0x1895c:$sqlite3step: 68 34 1C 7B E1<br>• 0x18878:$sqlite3text: 68 38 2A 90 C5<br>• 0x1899d:$sqlite3text: 68 38 2A 90 C5<br>• 0x1888b:$sqlite3blob: 68 53 D8 7F 8C<br>• 0x189b3:$sqlite3blob: 68 53 D8 7F 8C |
| 00000007.00000000.357102552.0000000010B69000.00000040.00020000.sdmp | JoeSecurity_FormBook | Yara detected FormBook | Joe Security | |
| 00000007.00000000.357102552.0000000010B69000.00000040.00020000.sdmp | Formbook_1 | autogenerated rule brought to you by yara-signator | Felix Bilstein - yara-signator at cocacoding dot com | • 0x26b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94<br>• 0x21a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91<br>• 0x27b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F<br>• 0x292f:$sequence_4: 5D C3 8D 50 7C 80 FA 07<br>• 0x141c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8<br>• 0x8927:$sequence_8: 3C 54 74 04 3C 74 75 F4<br>• 0x992a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00 |

Click to see the 21 entries

### Unpacked PEs

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 6.2.RegSvcs.exe.400000.0.unpack | JoeSecurity_FormBook | Yara detected FormBook | Joe Security | |
| 6.2.RegSvcs.exe.400000.0.unpack | Formbook_1 | autogenerated rule brought to you by yara-signator | Felix Bilstein - yara-signator at cocacoding dot com | • 0x8b08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0x8d82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0x148b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94<br>• 0x143a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91<br>• 0x149b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F<br>• 0x14b2f:$sequence_4: 5D C3 8D 50 7C 80 FA 07<br>• 0x979a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06<br>• 0x1361c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8<br>• 0xa493:$sequence_7: 66 89 0C 02 5B 8B E5 5D<br>• 0x1ab27:$sequence_8: 3C 54 74 04 3C 74 75 F4<br>• 0x1bb2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00 |
| 6.2.RegSvcs.exe.400000.0.unpack | Formbook | detect Formbook in memory | JPCERT/CC Incident Response Group | • 0x17a49:$sqlite3step: 68 34 1C 7B E1<br>• 0x17b5c:$sqlite3step: 68 34 1C 7B E1<br>• 0x17a78:$sqlite3text: 68 38 2A 90 C5<br>• 0x17b9d:$sqlite3text: 68 38 2A 90 C5<br>• 0x17a8b:$sqlite3blob: 68 53 D8 7F 8C<br>• 0x17bb3:$sqlite3blob: 68 53 D8 7F 8C |
| 0.2.Factura de proforma.exe.2bd16b0.1.raw.unpack | JoeSecurity_AntiVM_3 | Yara detected AntiVM_3 | Joe Security | |
| 0.2.Factura de proforma.exe.3cc0560.3.raw.unpack | JoeSecurity_FormBook | Yara detected FormBook | Joe Security | |

Click to see the 8 entries

## Sigma Overview

### System Summary:

**Sigma detected: Bad Opsec Defaults Sacrificial Processes With Improper Arguments**

**Sigma detected: Possible Applocker Bypass**

## Jbx Signature Overview

Click to jump to signature section

## AV Detection:

- Found malware configuration
- Yara detected FormBook

## Networking:

- System process connects to network (likely due to code injection or exploit)
- Performs DNS queries to domains with low reputation
- C2 URLs / IPs found in malware configuration

## E-Banking Fraud:

- Yara detected FormBook

## System Summary:

- Malicious sample detected (through community Yara rule)

## Data Obfuscation:

- .NET source code contains potential unpacker

## Boot Survival:

- Uses schtasks.exe or at.exe to add and modify task schedules

## 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)
- 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

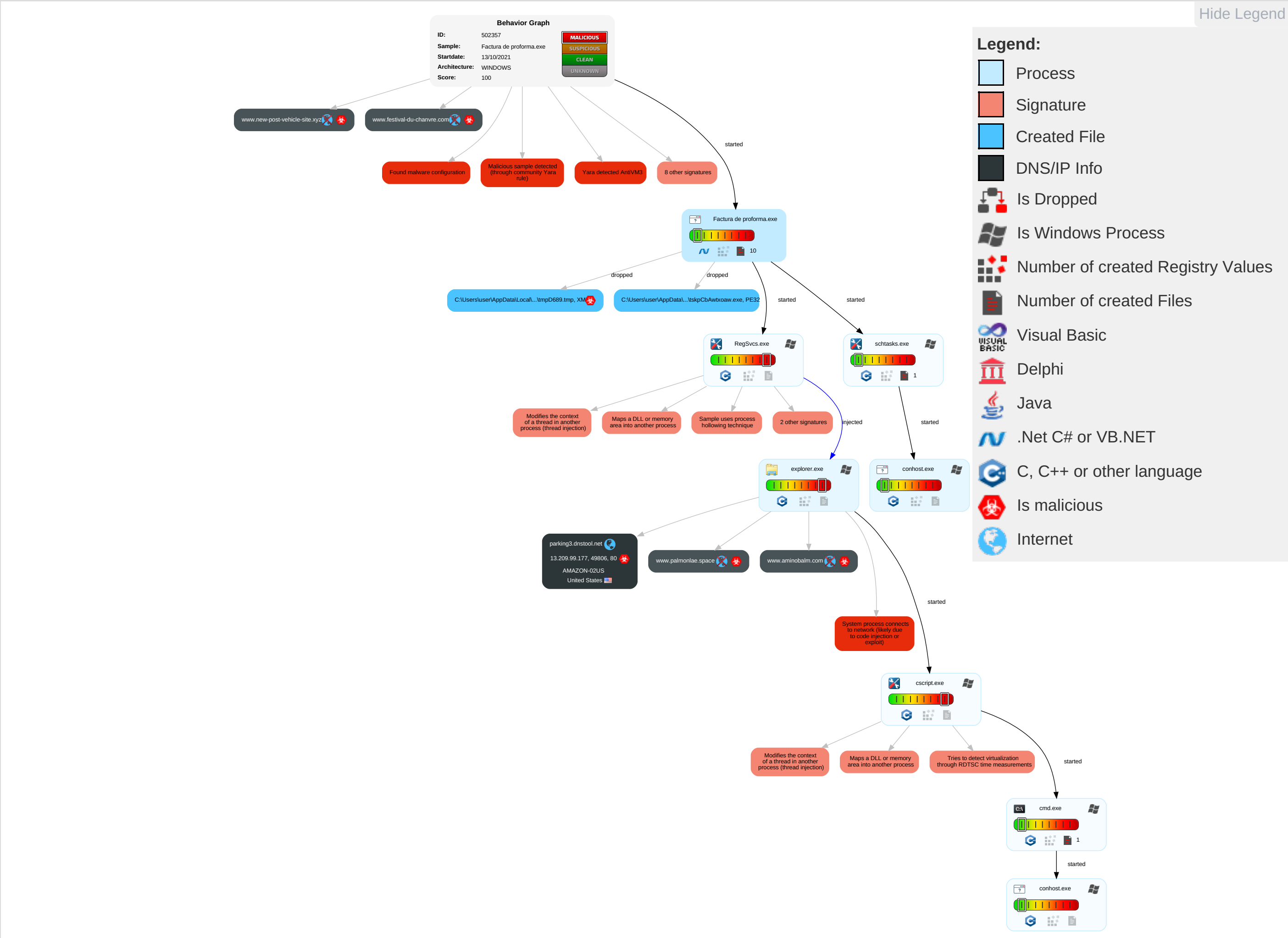
## Remote Access Functionality:

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 | Scheduled Task/Job 1 | Scheduled Task/Job 1 | Process Injection 5 1 2 | Rootkit 1 | Credential API Hooking 1 | Security Software Discovery 2 2 1 | Remote Services | Credential API Hooking 1 | Exfiltration Over Other Network Medium | Encrypted Channel 1 | Eavesdrop Insecure Network Communica |
| Default Accounts | Shared Modules 1 | Boot or Logon Initialization Scripts | Scheduled Task/Job 1 | Masquerading 1 | LSASS Memory | Process Discovery 2 | Remote Desktop Protocol | Archive Collected Data 1 | Exfiltration Over Bluetooth | Ingress Tool Transfer 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 | Data from Network Shared Drive | Automated Exfiltration | Non-Application Layer Protocol 2 | Exploit SS7 Track Devic Location |
| Local Accounts | At (Windows) | Logon Script (Mac) | Logon Script (Mac) | Virtualization/Sandbox Evasion 3 1 | NTDS | Remote System Discovery 1 | Distributed Component Object Model | Input Capture | Scheduled Transfer | Application Layer Protocol 1 2 | SIM Card Swap |
| Cloud Accounts | Cron | Network Logon Script | Network Logon Script | Process Injection 5 1 2 | LSA Secrets | File and Directory Discovery 1 | SSH | Keylogging | Data Transfer Size Limits | Fallback Channels | Manipulate Device Communica |
| Replication Through Removable Media | Launchd | Rc.common | Rc.common | Deobfuscate/Decode Files or Information 1 | Cached Domain Credentials | System Information Discovery 1 1 2 | VNC | GUI Input Capture | Exfiltration Over C2 Channel | Multiband Communication | Jamming or 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-F Access Poi |
| 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 | Downgrade Insecure Protocols |

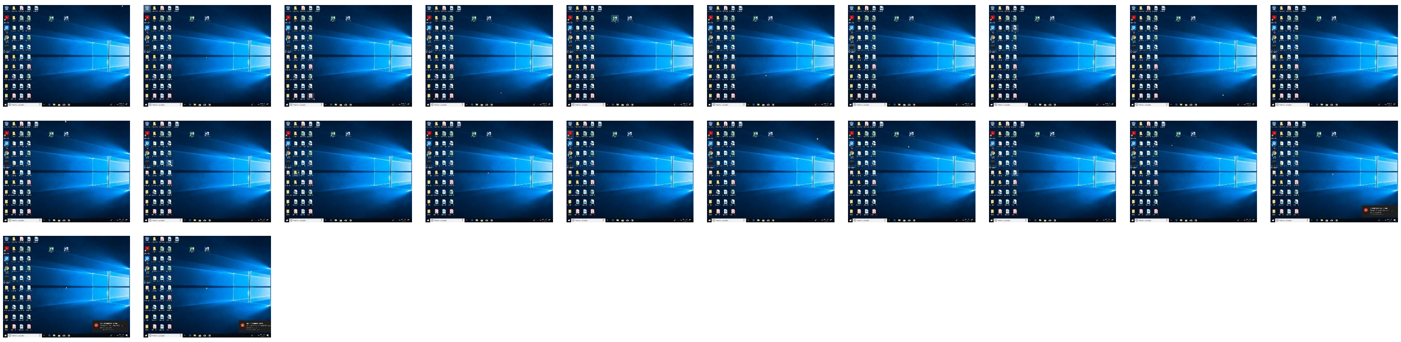
## Behavior Graph




## 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

**No Antivirus matches**

## Dropped Files

**No Antivirus matches**

## Unpacked PE Files

| Source | Detection | Scanner | Label | Link | Download |
|---|---|---|---|---|---|
| 6.2.RegSvcs.exe.400000.0.unpack | 100% | Avira | TR/Crypt.ZPACK.Gen | | Download File |

## Domains

**No Antivirus matches**

## URLs

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://www.jiyu-kobo.co.jp/XDiUa | 0% | Avira URL Cloud | safe | |
| http://www.fonts.comc | 0% | URL Reputation | safe | |
| http://www.founder.com.cn/cn/bThe | 0% | URL Reputation | safe | |
| http://www.founder.com.cn/cn2U% | 0% | Avira URL Cloud | safe | |

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://www.founder.com.cn/cn.U | 0% | Avira URL Cloud | safe | |
| http://www.jiyu-kobo.co.jp/tDMU | 0% | Avira URL Cloud | safe | |
| http://www.aminobalm.com/cb3b/?c6=kr386M7znJup/B2j4KhdpwCgkxfUSLFq19BV4h8BDsMel0JC//DVwypubzBUvp11Q9BD&A0DXb=eZk4rh9h | 0% | Avira URL Cloud | safe | |
| http://www.sandoll.co.krN.TTFs | 0% | Avira URL Cloud | safe | |
| http://www.tiro.com | 0% | URL Reputation | safe | |
| http://www.tiro.comF | 0% | URL Reputation | safe | |
| http://www.goodfont.co.kr | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/a-eoDFU$ | 0% | Avira URL Cloud | safe | |
| http://www.jiyu-kobo.co.jp/jp/ | 0% | URL Reputation | safe | |
| http://www.fonts.com-uT | 0% | Avira URL Cloud | safe | |
| http://en.w | 0% | URL Reputation | safe | |
| http://www.collada.org/2005/11/COLLADASchema9Done | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/ko | 0% | Avira URL Cloud | safe | |
| http://www.carterandcone.coml | 0% | URL Reputation | safe | |
| http://www.sajatypeworks.com | 0% | URL Reputation | safe | |
| http://www.typography.netD | 0% | URL Reputation | safe | |
| http://www.founder.com.cn/cn/cThe | 0% | URL Reputation | safe | |
| http://www.galapagosdesign.com/staff/dennis.htm | 0% | URL Reputation | safe | |
| http://fontfabrik.com | 0% | URL Reputation | safe | |
| http://www.founder.com.cn/cn | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/t | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/7D | 0% | Avira URL Cloud | safe | |
| http://www.jiyu-kobo.co.jp/ | 0% | URL Reputation | safe | |
| http://www.fonts.comn | 0% | URL Reputation | safe | |
| http://www.galapagosdesign.com/DPlease | 0% | URL Reputation | safe | |
| www.thefanlounge.com/cb3b/ | 0% | Avira URL Cloud | safe | |
| http://www.sandoll.co.kr | 0% | URL Reputation | safe | |
| http://www.urwpp.deDPlease | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/JD | 0% | Avira URL Cloud | safe | |
| http://www.zhongyicts.com.cn | 0% | URL Reputation | safe | |
| http://www.sakkal.com | 0% | URL Reputation | safe | |
| http://https://www.dotname.co.kr/customer/event/2019/20190604_landing_dotname?c6=kr386M7znJup/B2j4KhdpwCgkx | 0% | Avira URL Cloud | safe | |

# Domains and IPs

## Contacted Domains

| Name | IP | Active | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|---|
| parking3.dnstool.net | 13.209.99.177 | true | true | | unknown |
| www.festival-du-chanvre.com | unknown | unknown | true | | unknown |
| www.aminobalm.com | unknown | unknown | true | | unknown |
| www.palmonlae.space | unknown | unknown | true | | unknown |
| www.new-post-vehicle-site.xyz | unknown | unknown | true | | unknown |

## Contacted URLs

| Name | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|
| http://www.aminobalm.com/cb3b/?c6=kr386M7znJup/B2j4KhdpwCgkxfUSLFq19BV4h8BDsMel0JC//DVwypubzBUvp11Q9BD&A0DXb=eZk4rh9h | true | • Avira URL Cloud: safe | unknown |
| www.thefanlounge.com/cb3b/ | true | • Avira URL Cloud: safe | low |

## URLs from Memory and Binaries

## Contacted IPs

## Public

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 13.209.99.177 | parking3.dnstool.net | United States | | 16509 | AMAZON-02US | true |

# General Information

| | |
|---|---|
| Joe Sandbox Version: | 33.0.0 White Diamond |
| Analysis ID: | 502357 |
| Start date: | 13.10.2021 |
| Start time: | 20:33:12 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 11m 20s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | Factura de proforma.exe |
| Cookbook file name: | default.jbs |
| Analysis system description: | Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211 |
| Number of analysed new started processes analysed: | 24 |
| Number of new started drivers analysed: | 0 |
| Number of existing processes analysed: | 0 |
| Number of existing drivers analysed: | 0 |
| Number of injected processes analysed: | 0 |
| Technologies: | • HCA enabled<br>• EGA enabled<br>• HDC enabled<br>• AMSI enabled |
| Analysis Mode: | default |
| Analysis stop reason: | Timeout |
| Detection: | MAL |
| Classification: | mal100.troj.evad.winEXE@10/4@4/1 |
| EGA Information: | Failed |
| HDC Information: | • Successful, ratio: 13.8% (good quality ratio 12.5%)<br>• Quality average: 75.1%<br>• Quality standard deviation: 30.9% |
| 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

| Time | Type | Description |
|---|---|---|
| 20:34:22 | API Interceptor | 1x Sleep call for process: Factura de proforma.exe modified |

# Joe Sandbox View / Context

## IPs

| No context |
|---|

## Domains

**No context**

## ASN

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| AMAZON-02US | OHqOvvjgbN.msi | Get hash | malicious | Browse | • 52.95.165.3 |
| | Gsdqz.dll | Get hash | malicious | Browse | • 3.126.56.137 |
| | OCT 13 2021 - PRINT COPY.xlsx | Get hash | malicious | Browse | • 18.197.254.181 |
| | HUTWMrDhov.dll | Get hash | malicious | Browse | • 18.156.0.31 |
| | M1YceQ237E.dll | Get hash | malicious | Browse | • 18.184.201.8 |
| | Sajeeb09908976745344567.xlsx | Get hash | malicious | Browse | • 3.64.163.50 |
| | 2OfuyvjJu1.msi | Get hash | malicious | Browse | • 52.95.163.44 |
| | cvWFjfKtdH | Get hash | malicious | Browse | • 54.103.213.234 |
| | K3h3TPEpze | Get hash | malicious | Browse | • 34.219.214.170 |
| | Jrsuarez-62643-5799-80-950985.HTM | Get hash | malicious | Browse | • 54.230.206.106 |
| | Jrsuarez-62643-5799-80-950985.HTM | Get hash | malicious | Browse | • 54.230.206.106 |
| | Jrsuarez-62643-5799-80-950985.HTM | Get hash | malicious | Browse | • 54.230.206.51 |
| | Jrsuarez-62643-5799-80-950985.HTM | Get hash | malicious | Browse | • 54.230.206.25 |
| | Ref 0180066743.xlsx | Get hash | malicious | Browse | • 13.232.45.220 |
| | pago atrasado.exe | Get hash | malicious | Browse | • 3.64.163.50 |
| | 6AYs2EgVeN.apk | Get hash | malicious | Browse | • 52.222.174.50 |
| | 4f0PBbcOBI | Get hash | malicious | Browse | • 34.249.145.219 |
| | REQUIREMENT.exe | Get hash | malicious | Browse | • 3.121.211.190 |
| | RlypFfB7n8 | Get hash | malicious | Browse | • 54.171.230.55 |
| | 7iw4z5I41w | Get hash | malicious | Browse | • 34.249.145.219 |

## JA3 Fingerprints

**No context**

## Dropped Files

**No context**

# Created / dropped Files

| C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Factura de proforma.exe.log | |
|---|---|
| Process: | C:\Users\user\Desktop\Factura de proforma.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | modified |
| Size (bytes): | 1308 |
| Entropy (8bit): | 5.348115897127242 |
| Encrypted: | false |
| SSDEEP: | 24:MLUE4KJXE4qpE4Ks2E1qE4qpAE4Kzr7RKDE4KhK3VZ9pKhPKIE4oKFKHKorE4x88:MIHKtH2HKXE1qHmAHKzvRYHKhQnoPtH2 |
| MD5: | 832D6A22CE7798D72609B9C21B4AF152 |
| SHA1: | B086DE927BFEE6039F5555CE53C397D1E59B4CA4 |
| SHA-256: | 9E5EE72EF293C66406AF155572BF3B0CF9DA09CC1F60ED6524AAFD65553CE551 |
| SHA-512: | A1A70F76B98C2478830AE737B4F12507D859365F046C5A415E1EBE3D87FFD2B64663A31E1E5142F7C3A7FE9A6A9CB8C143C2E16E94C3DD6041D1CCABEDDD2C 21 |
| Malicious: | false |
| Reputation: | moderate, 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..2,"System.Deployment, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.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..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows |

| C:\Users\user\AppData\Local\Temp\tmpD689.tmp | |
|---|---|
| Process: | C:\Users\user\Desktop\Factura de proforma.exe |

| C:\Users\user\AppData\Local\Temp\tmpD689.tmp | |
|---|---|
| File Type: | XML 1.0 document, ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 1646 |
| Entropy (8bit): | 5.186739433298605 |
| Encrypted: | false |
| SSDEEP: | 24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBTGYtn:cbh47TlNQ//rydbz9I3YODOLNdq3X |
| MD5: | 1E44E6ADAE1C0CA0FD56FA664DDFE899 |
| SHA1: | BED45CA5BDDB3ED71E73A72C6058ED5101440C3F |
| SHA-256: | 55CBE776A65A94D258CC0EA3911132969AED0F6979BE24A24BE4C4FB9F44E20A |
| SHA-512: | 0F7E8D6686C0E5DE421C909904A5116A35E5A55FA3C61388C9665A4A81B145F3B0B0247CC3ED70F07014C2EB76F51EAC224F1F4E3CAB18FB5F0506BF49A42BCA |
| Malicious: | **true** |
| Preview: | <?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true |

| C:\Users\user\AppData\Roaming\tskpCbAwtxoaw.exe | |
|---|---|
| Process: | C:\Users\user\Desktop\Factura de proforma.exe |
| File Type: | PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows |
| Category: | dropped |
| Size (bytes): | 495616 |
| Entropy (8bit): | 7.503647477821442 |
| Encrypted: | false |
| SSDEEP: | 12288:x0K9jbtvzZPJukNeFrmndcPeGGUQSB/a:xh/plBlMFrleGfdB/ |
| MD5: | 16F7045EEBB451234CA8078222C5994C |
| SHA1: | 99E8F263F9E34AD13CB8CD6AF1BB816DEFFB5BDE |
| SHA-256: | FF344E635B268090AAFDB8FA830E76C41F34D7CF9A9BF03ED4EDE2705008BFEF |
| SHA-512: | 147D377F3F05F593E7428F5E5DD70C231E187C73DE1CDF111790156060F59047E80F382805678ECD3F946C58FCF5D80F4E16D8534F07F0F7355BEDEDB7726BB8 |
| Malicious: | false |
| Preview: | MZ......................@...............................................!..L.!This program cannot be run in DOS mode....$.......PE..L...Z.fa.............0.................. ... ....@.. .................................. ..@....................................O.... ............................................................................... ............... ..H...........text... .... ...................... ..`.rsrc........ ......................@..@.reloc........ ......................@..B........................H.......Lb..,O......Y...x...Pk..........................................0..V.........}......*.*s....}......}......}.....(.......(......{....r...po......{....r...po.....*...0.............(....&. {.........,....8....sA...%.{.....\|....(....Z.{.....\|....(....Z . &.s....} ...%.}......{ ...(.........(....o........+c...+C.....X.].......,+..(.......{....Z...{....Z.{.....{....o ........X.....\|....(..........-....X.....\|....(..........- ......,...o!.....sB........\|....(.....\|....(....s" |

| C:\Users\user\AppData\Roaming\tskpCbAwtxoaw.exe:Zone.Identifier | |
|---|---|
| Process: | C:\Users\user\Desktop\Factura de proforma.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: | false |
| Preview: | [ZoneTransfer]....ZoneId=0 |

# Static File Info

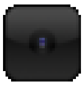
## General

| | |
|---|---|
| File type: | PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows |
| Entropy (8bit): | 7.503647477821442 |

## General

| | |
|---|---|
| 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: | Factura de proforma.exe |
| File size: | 495616 |
| MD5: | 16f7045eebb451234ca8078222c5994c |
| SHA1: | 99e8f263f9e34ad13cb8cd6af1bb816deffb5bde |
| SHA256: | ff344e635b268090aafdb8fa830e76c41f34d7cf9a9bf03ed4ede2705008bfef |
| SHA512: | 147d377f3f05f593e7428f5e5dd70c231e187c73de1cdf111790156060f59047e80f382805678ecd3f946c58fcf5d80f4e16d8534f07f0f7355bededb7726bb8 |
| SSDEEP: | 12288:x0K9jbtvzZPJukNeFrmndcPeGGUQSB/a:xh/plBlMFrleGfdB/ |
| File Content Preview: | MZ......................@...............................................!..L.!This program cannot be run in DOS mode....$.......PE..L...Z.fa..............0.................. ... ....@.. .....................................@................................ |

## File Icon



| | |
|---|---|
| Icon Hash: | c4b28ed696aa92c0 |

## Static PE Info

### General

| | |
|---|---|
| Entrypoint: | 0x461d1a |
| 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: | 0x6166B25A [Wed Oct 13 10:18:02 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 | 0x5fd20 | 0x5fe00 | False | 0.887357908246 | data | 7.7904887088 | IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ |
| .rsrc | 0x62000 | 0x18c84 | 0x18e00 | False | 0.195302685302 | data | 5.06927966627 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .reloc | 0x7c000 | 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

### TCP Packets

### UDP Packets

### DNS Queries

| Timestamp | Source IP | Dest IP | Trans ID | OP Code | Name | Type | Class |
|---|---|---|---|---|---|---|---|
| Oct 13, 2021 20:35:46.794310093 CEST | 192.168.2.3 | 8.8.8.8 | 0x6e9c | Standard query (0) | www.palmonlae.space | A (IP address) | IN (0x0001) |
| Oct 13, 2021 20:36:07.032196999 CEST | 192.168.2.3 | 8.8.8.8 | 0xa477 | Standard query (0) | www.aminobalm.com | A (IP address) | IN (0x0001) |
| Oct 13, 2021 20:36:29.043936014 CEST | 192.168.2.3 | 8.8.8.8 | 0x9873 | Standard query (0) | www.festival-du-chanvre.com | A (IP address) | IN (0x0001) |
| Oct 13, 2021 20:36:49.812874079 CEST | 192.168.2.3 | 8.8.8.8 | 0x8184 | Standard query (0) | www.new-post-vehicle-site.xyz | A (IP address) | IN (0x0001) |

### DNS Answers

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class |
|---|---|---|---|---|---|---|---|---|---|
| Oct 13, 2021 20:35:46.817334890 CEST | 8.8.8.8 | 192.168.2.3 | 0x6e9c | Name error (3) | www.palmonlae.space | none | none | A (IP address) | IN (0x0001) |
| Oct 13, 2021 20:36:07.327236891 CEST | 8.8.8.8 | 192.168.2.3 | 0xa477 | No error (0) | www.aminobalm.com | parking3.dnstool.net | | CNAME (Canonical name) | IN (0x0001) |
| Oct 13, 2021 20:36:07.327236891 CEST | 8.8.8.8 | 192.168.2.3 | 0xa477 | No error (0) | parking3.dnstool.net | | 13.209.99.177 | A (IP address) | IN (0x0001) |
| Oct 13, 2021 20:36:07.327236891 CEST | 8.8.8.8 | 192.168.2.3 | 0xa477 | No error (0) | parking3.dnstool.net | | 3.35.27.175 | A (IP address) | IN (0x0001) |
| Oct 13, 2021 20:36:07.327236891 CEST | 8.8.8.8 | 192.168.2.3 | 0xa477 | No error (0) | parking3.dnstool.net | | 13.125.234.146 | A (IP address) | IN (0x0001) |
| Oct 13, 2021 20:36:07.327236891 CEST | 8.8.8.8 | 192.168.2.3 | 0xa477 | No error (0) | parking3.dnstool.net | | 13.228.77.229 | A (IP address) | IN (0x0001) |
| Oct 13, 2021 20:36:07.327236891 CEST | 8.8.8.8 | 192.168.2.3 | 0xa477 | No error (0) | parking3.dnstool.net | | 13.230.138.127 | A (IP address) | IN (0x0001) |
| Oct 13, 2021 20:36:29.067773104 CEST | 8.8.8.8 | 192.168.2.3 | 0x9873 | Name error (3) | www.festival-du-chanvre.com | none | none | A (IP address) | IN (0x0001) |
| Oct 13, 2021 20:36:49.838001966 CEST | 8.8.8.8 | 192.168.2.3 | 0x8184 | Name error (3) | www.new-post-vehicle-site.xyz | none | none | A (IP address) | IN (0x0001) |

### HTTP Request Dependency Graph

- www.aminobalm.com

### HTTP Packets

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 0 | 192.168.2.3 | 49806 | 13.209.99.177 | 80 | C:\Windows\explorer.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| Oct 13, 2021 20:36:07.588450909 CEST | 5853 | OUT | GET /cb3b/?c6=kr386M7znJup/B2j4KhdpwCgkxfUSLFq19BV4h8BDsMel0JC//DVwypubzBUvp11Q9BD&A0DXb=eZk4rh9h HTTP/1.1<br>Host: www.aminobalm.com<br>Connection: close<br>Data Raw: 00 00 00 00 00 00 00<br>Data Ascii: |
| Oct 13, 2021 20:36:07.845493078 CEST | 5853 | IN | HTTP/1.1 302 Moved Temporarily<br>Server: nginx<br>Date: Wed, 13 Oct 2021 18:36:07 GMT<br>Content-Type: text/html<br>Content-Length: 138<br>Connection: close<br>Location: https://www.dotname.co.kr/customer/event/2019/20190604_landing_dotname?c6=kr386M7znJup/B2j4KhdpwCgkxfUSLFq19BV4h8BDsMel0JC//DVwypubzBUvp11Q9BD&A0DXb=eZk4rh9h<br>X-Content-Type-Options: nosniff<br>X-XSS-Protection: 1; mode=block<br>Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 32 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 32 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a<br>Data Ascii: <html><head><title>302 Found</title></head><body><center><h1>302 Found</h1></center><hr><center>nginx</center></body></html> |

# 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: Factura de proforma.exe PID: 6952 Parent PID: 3212

### General

| | |
|---|---|
| Start time: | 20:34:13 |
| Start date: | 13/10/2021 |
| Path: | C:\Users\user\Desktop\Factura de proforma.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Users\user\Desktop\Factura de proforma.exe' |
| Imagebase: | 0x7a0000 |
| File size: | 495616 bytes |
| MD5 hash: | 16F7045EEBB451234CA8078222C5994C |

| | |
|---|---|
| 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: 00000000.00000002.322614171.0000000003B89000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.322614171.0000000003B89000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.322614171.0000000003B89000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group<br>• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.322371267.0000000002B81000.00000004.00000001.sdmp, Author: Joe Security |
| Reputation: | low |

### File Activities

Show Windows behavior

#### File Created

#### File Deleted

#### File Written

#### File Read

## Analysis Process: schtasks.exe PID: 6436 Parent PID: 6952

### General

| | |
|---|---|
| Start time: | 20:34:24 |
| Start date: | 13/10/2021 |
| Path: | C:\Windows\SysWOW64\schtasks.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\tskpCbAwtxoaw' /XML 'C:\Users\user\AppData\Local\Temp\tmpD689.tmp' |
| Imagebase: | 0x1070000 |
| File size: | 185856 bytes |
| MD5 hash: | 15FF7D8324231381BAD48A052F85DF04 |
| 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: 6824 Parent PID: 6436

### General

| | |
|---|---|
| Start time: | 20:34:24 |
| 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 |

## Analysis Process: RegSvcs.exe PID: 6388 Parent PID: 6952

### General

| | |
|---|---|
| Start time: | 20:34:25 |
| Start date: | 13/10/2021 |
| Path: | C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe |
| Imagebase: | 0xb80000 |
| File size: | 45152 bytes |
| MD5 hash: | 2867A3817C9245F7CF518524DFD18F28 |
| 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: 00000006.00000002.402637395.0000000001500000.00000040.00020000.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.402637395.0000000001500000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.402637395.0000000001500000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group<br>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.401884612.0000000000400000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.401884612.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.401884612.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group<br>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.402727602.0000000001530000.00000040.00020000.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.402727602.0000000001530000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.402727602.0000000001530000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group |
| Reputation: | high |

### File Activities

Show Windows behavior

#### File Read

## Analysis Process: explorer.exe PID: 3352 Parent PID: 6388

### General

| | |
|---|---|
| Start time: | 20:34:26 |
| 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: 00000007.00000000.357102552.0000000010B69000.00000040.00020000.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000000.357102552.0000000010B69000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000000.357102552.0000000010B69000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group |
| Reputation: | high |

### File Activities

Show Windows behavior

## Analysis Process: cscript.exe PID: 4716 Parent PID: 3352

### General

| | |
|---|---|
| Start time: | 20:35:00 |
| Start date: | 13/10/2021 |
| Path: | C:\Windows\SysWOW64\cscript.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\SysWOW64\cscript.exe |
| Imagebase: | 0x260000 |
| File size: | 143360 bytes |
| MD5 hash: | 00D3041E47F99E48DD5FFFEDF60F6304 |
| 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: 0000000A.00000002.570999919.0000000000540000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.570999919.0000000000540000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.570999919.0000000000540000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group<br>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.571846259.0000000002990000.00000040.00020000.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.571846259.0000000002990000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.571846259.0000000002990000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group<br>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.571574263.00000000025D0000.00000040.00020000.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.571574263.00000000025D0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.571574263.00000000025D0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group |
| Reputation: | moderate |

### File Activities

Show Windows behavior

#### File Read

## Analysis Process: cmd.exe PID: 3408 Parent PID: 4716

### General

| | |
|---|---|
| Start time: | 20:35:04 |

| | |
|---|---|
| Start date: | 13/10/2021 |
| Path: | C:\Windows\SysWOW64\cmd.exe |
| Wow64 process (32bit): | true |
| Commandline: | /c del 'C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe' |
| Imagebase: | 0xd80000 |
| File size: | 232960 bytes |
| MD5 hash: | F3BDBE3BB6F734E357235F4D5898582D |
| Has elevated privileges: | false |
| Has administrator privileges: | false |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

### File Activities

Show Windows behavior

## Analysis Process: conhost.exe PID: 6960 Parent PID: 3408

### General

| | |
|---|---|
| Start time: | 20:35:05 |
| 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: | false |
| Has administrator privileges: | false |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

# Disassembly

## Code Analysis



Joe Sandbox Cloud Basic 33.0.0 White Diamond