
**ID:** 458632
**Sample Name:** doc_2021_98666_SIGNED - PRO FACTURA.exe
**Cookbook:** default.jbs
**Time:** 15:55:41
**Date:** 03/08/2021
**Version:** 33.0.0 White Diamond

# Table of Contents


Table of Contents 2
Windows Analysis Report doc_2021_98666_SIGNED - PRO FACTURA.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: NanoCore 4
Yara Overview 5
Memory Dumps 5
Unpacked PEs 6
Sigma Overview 6
Jbx Signature Overview 6
AV Detection: 6
Networking: 7
E-Banking Fraud: 7
System Summary: 7
Boot Survival: 7
Malware Analysis System Evasion: 7
Stealing of Sensitive Information: 7
Remote Access Functionality: 7
Mitre Att&ck Matrix 7
Behavior Graph 8
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 9
Domains and IPs 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 9
Contacted IPs 9
General Information 9
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 10
ASN 10
JA3 Fingerprints 10
Dropped Files 10
Created / dropped Files 10
Static File Info 12
General 12
File Icon 12
Static PE Info 12
General 12
Entrypoint Preview 12
Data Directories 12
Sections 12
Resources 13
Imports 13
Version Infos 13
Network Behavior 13
Code Manipulations 13
Statistics 13
Behavior 13
System Behavior 13
Analysis Process: doc_2021_98666_SIGNED - PRO FACTURA.exe PID: 6512 Parent PID: 5840 13
General 13
File Activities 14
File Created 14
File Deleted 14
File Written 14
File Read 14
Analysis Process: schtasks.exe PID: 6744 Parent PID: 6512 14
General 14
File Activities 14
File Read 14
Analysis Process: conhost.exe PID: 6752 Parent PID: 6744 14
General 14
Analysis Process: doc_2021_98666_SIGNED - PRO FACTURA.exe PID: 6788 Parent PID: 6512 15

General 15
Analysis Process: doc_2021_98666_SIGNED - PRO FACTURA.exe PID: 6804 Parent PID: 6512 15
General 15
Analysis Process: doc_2021_98666_SIGNED - PRO FACTURA.exe PID: 6820 Parent PID: 6512 15
General 15
Analysis Process: doc_2021_98666_SIGNED - PRO FACTURA.exe PID: 6836 Parent PID: 6512 16
General 16
Analysis Process: doc_2021_98666_SIGNED - PRO FACTURA.exe PID: 6848 Parent PID: 6512 16
General 16
Disassembly 16
Code Analysis 16

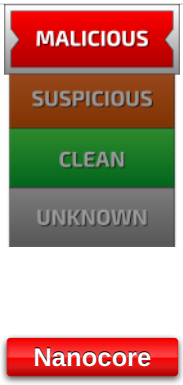
# Windows Analysis Report doc_2021_98666_SIGNED - P…

## Overview

### General Information

| | |
|---|---|
| Sample Name: | doc_2021_98666_SIGNED - PRO FACTURA.exe |
| Analysis ID: | 458632 |
| MD5: | 532b5c7f4e3212a. |
| SHA1: | 9a46dd2c45b724.. |
| SHA256: | 46510a62d266a7.. |
| Tags: | exe null |
| Infos: | |

### Detection

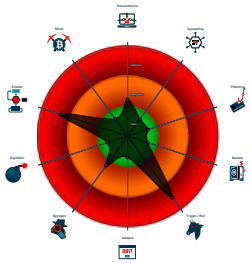



| | |
|---|---|
| Score: | 100 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 100% |

### Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected AntiVM3
- Yara detected Nanocore RAT
- C2 URLs / IPs found in malware con…
- Initial sample is a PE file and has a …
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Tries to detect sandboxes and other…

### Classification



## Process Tree

- **System is w10x64**
- doc_2021_98666_SIGNED - PRO FACTURA.exe (PID: 6512 cmdline: 'C:\Users\user\Desktop\doc_2021_98666_SIGNED - PRO FACTURA.exe' MD5: 532B5C7F4E3212A0D05E51C85864CAF6)
  - schtasks.exe (PID: 6744 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\bWuIYd' /XML 'C:\Users\user\AppData\Local\Temp\tmpDCE9.tmp' MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
    - conhost.exe (PID: 6752 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - doc_2021_98666_SIGNED - PRO FACTURA.exe (PID: 6788 cmdline: C:\Users\user\Desktop\doc_2021_98666_SIGNED - PRO FACTURA.exe MD5: 532B5C7F4E3212A0D05E51C85864CAF6)
  - doc_2021_98666_SIGNED - PRO FACTURA.exe (PID: 6804 cmdline: C:\Users\user\Desktop\doc_2021_98666_SIGNED - PRO FACTURA.exe MD5: 532B5C7F4E3212A0D05E51C85864CAF6)
  - doc_2021_98666_SIGNED - PRO FACTURA.exe (PID: 6820 cmdline: C:\Users\user\Desktop\doc_2021_98666_SIGNED - PRO FACTURA.exe MD5: 532B5C7F4E3212A0D05E51C85864CAF6)
  - doc_2021_98666_SIGNED - PRO FACTURA.exe (PID: 6836 cmdline: C:\Users\user\Desktop\doc_2021_98666_SIGNED - PRO FACTURA.exe MD5: 532B5C7F4E3212A0D05E51C85864CAF6)
  - doc_2021_98666_SIGNED - PRO FACTURA.exe (PID: 6848 cmdline: C:\Users\user\Desktop\doc_2021_98666_SIGNED - PRO FACTURA.exe MD5: 532B5C7F4E3212A0D05E51C85864CAF6)
- **cleanup**

## Malware Configuration

### Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "7547b95a-3564-48ed-9de2-e9e7593f",
  "Group": "ikenna",
  "Domain1": "194.5.98.127",
  "Domain2": "127.0.0.1",
  "Port": 54984,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Enable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Enable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task"
}
```


# Yara Overview

## Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000000.00000002.668794104.00000000032EA000.00000004.00000001.sdmp | JoeSecurity_AntiVM_3 | Yara detected AntiVM_3 | Joe Security | |
| 00000000.00000002.669660281.0000000012F61000.00000004.00000001.sdmp | Nanocore_RAT_Gen_2 | Detetcs the Nanocore RAT | Florian Roth | • 0x67f4c5:$x1: NanoCore.ClientPluginHost<br>• 0x67f502:$x2: IClientNetworkHost<br>• 0x683035:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe |
| 00000000.00000002.669660281.0000000012F61000.00000004.00000001.sdmp | JoeSecurity_Nanocore | Yara detected Nanocore RAT | Joe Security | |
| 00000000.00000002.669660281.0000000012F61000.00000004.00000001.sdmp | NanoCore | unknown | Kevin Breen <kevin@techanarchy.net> | • 0x67f22d:$a: NanoCore<br>• 0x67f23d:$a: NanoCore<br>• 0x67f471:$a: NanoCore<br>• 0x67f485:$a: NanoCore<br>• 0x67f4c5:$a: NanoCore<br>• 0x67f28c:$b: ClientPlugin<br>• 0x67f48e:$b: ClientPlugin<br>• 0x67f4ce:$b: ClientPlugin<br>• 0x67f3b3:$c: ProjectData<br>• 0x93581f:$c: ProjectData<br>• 0x67fdba:$d: DESCrypto<br>• 0x687786:$e: KeepAlive<br>• 0x685774:$g: LogClientMessage<br>• 0x68196f:$i: get_Connected<br>• 0x6800f0:$j: #=q<br>• 0x680120:$j: #=q<br>• 0x68013c:$j: #=q<br>• 0x68016c:$j: #=q<br>• 0x680188:$j: #=q<br>• 0x6801a4:$j: #=q<br>• 0x6801d4:$j: #=q |

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| Process Memory Space: doc_2021_98666_SIGNED - PRO FACTURA.exe PID: 6512 | Nanocore_RAT_Gen_2 | Detetcs the Nanocore RAT | Florian Roth | • 0x497ae7:$x1: NanoCore.ClientPluginHost<br>• 0x497b24:$x2: IClientNetworkHost<br>• 0x49ae7d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe<br>• 0x4a5ad8:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe |
| Click to see the 3 entries | | | | |

## Unpacked PEs

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 0.2.doc_2021_98666_SIGNED - PRO FACTURA.exe.135d0338.4.unpack | Nanocore_RAT_Gen_2 | Detetcs the Nanocore RAT | Florian Roth | • 0xe38d:$x1: NanoCore.ClientPluginHost<br>• 0xe3ca:$x2: IClientNetworkHost<br>• 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe |
| 0.2.doc_2021_98666_SIGNED - PRO FACTURA.exe.135d0338.4.unpack | Nanocore_RAT_Feb18_1 | Detects Nanocore RAT | Florian Roth | • 0xe105:$x1: NanoCore Client.exe<br>• 0xe38d:$x2: NanoCore.ClientPluginHost<br>• 0xf9c6:$s1: PluginCommand<br>• 0xf9ba:$s2: FileCommand<br>• 0x1086b:$s3: PipeExists<br>• 0x16622:$s4: PipeCreated<br>• 0xe3b7:$s5: IClientLoggingHost |
| 0.2.doc_2021_98666_SIGNED - PRO FACTURA.exe.135d0338.4.unpack | JoeSecurity_Nanocore | Yara detected Nanocore RAT | Joe Security | |
| 0.2.doc_2021_98666_SIGNED - PRO FACTURA.exe.135d0338.4.unpack | NanoCore | unknown | Kevin Breen <kevin@techanarchy.net> | • 0xe0f5:$a: NanoCore<br>• 0xe105:$a: NanoCore<br>• 0xe339:$a: NanoCore<br>• 0xe34d:$a: NanoCore<br>• 0xe38d:$a: NanoCore<br>• 0xe154:$b: ClientPlugin<br>• 0xe356:$b: ClientPlugin<br>• 0xe396:$b: ClientPlugin<br>• 0xe27b:$c: ProjectData<br>• 0xec82:$d: DESCrypto<br>• 0x1664e:$e: KeepAlive<br>• 0x1463c:$g: LogClientMessage<br>• 0x10837:$i: get_Connected<br>• 0xefb8:$j: #=q<br>• 0xefe8:$j: #=q<br>• 0xf004:$j: #=q<br>• 0xf034:$j: #=q<br>• 0xf050:$j: #=q<br>• 0xf06c:$j: #=q<br>• 0xf09c:$j: #=q<br>• 0xf0b8:$j: #=q |
| 0.2.doc_2021_98666_SIGNED - PRO FACTURA.exe.135d0338.4.raw.unpack | Nanocore_RAT_Gen_2 | Detetcs the Nanocore RAT | Florian Roth | • 0x1018d:$x1: NanoCore.ClientPluginHost<br>• 0x101ca:$x2: IClientNetworkHost<br>• 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe |
| Click to see the 2 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 dropped file**

**Multi AV Scanner detection for submitted file**

**Yara detected Nanocore RAT**

**Machine Learning detection for dropped file**

Machine Learning detection for sample

## Networking:

C2 URLs / IPs found in malware configuration

## E-Banking Fraud:

Yara detected Nanocore RAT

## System Summary:

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

## Boot Survival:

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

## Malware Analysis System Evasion:

Yara detected AntiVM3

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

## Stealing of Sensitive Information:

Yara detected Nanocore RAT

## Remote Access Functionality:

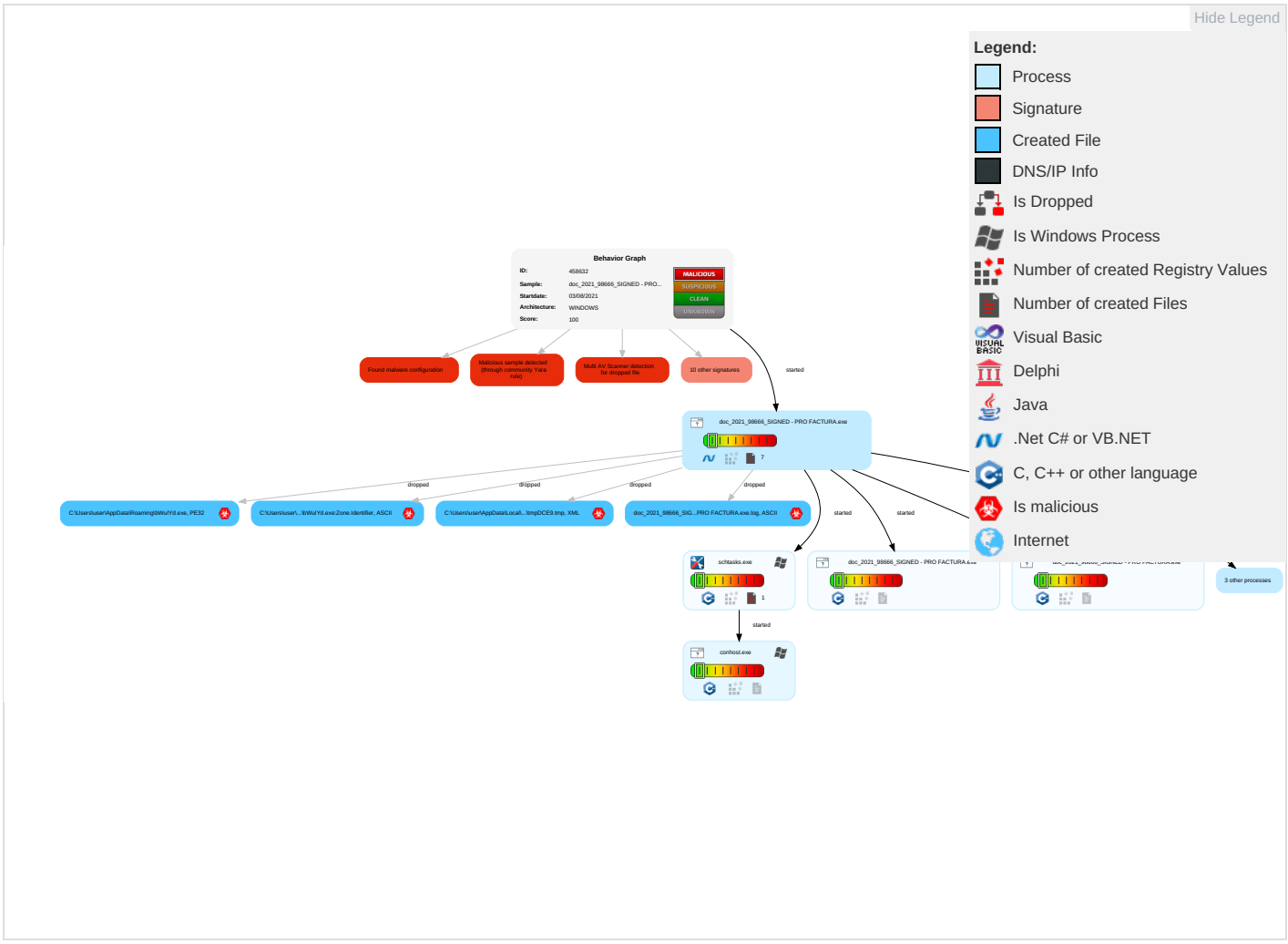
Detected Nanocore Rat

Yara detected Nanocore RAT

# 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 1 1 | Masquerading 1 | OS Credential Dumping | Query Registry 1 | Remote Services | Archive Collected Data 1 | Exfiltration Over Other Network Medium | Encrypted Channel 1 | Eavesdrop on Insecure Network Communication |
| Default Accounts | Scheduled Task/Job | Boot or Logon Initialization Scripts | Scheduled Task/Job 1 | Disable or Modify Tools 1 | LSASS Memory | Security Software Discovery 2 1 | Remote Desktop Protocol | Data from Removable Media | Exfiltration Over Bluetooth | Remote Access Software 1 | Exploit SS7 to Redirect Phone Calls/SMS |
| Domain Accounts | At (Linux) | Logon Script (Windows) | Logon Script (Windows) | Virtualization/Sandbox Evasion 2 1 | Security Account Manager | Process Discovery 1 | SMB/Windows Admin Shares | Data from Network Shared Drive | Automated Exfiltration | Application Layer Protocol 1 | Exploit SS7 to Track Device Location |
| Local Accounts | At (Windows) | Logon Script (Mac) | Logon Script (Mac) | Process Injection 1 1 | NTDS | Virtualization/Sandbox Evasion 2 1 | Distributed Component Object Model | Input Capture | Scheduled Transfer | Protocol Impersonation | SIM Card Swap |
| Cloud Accounts | Cron | Network Logon Script | Network Logon Script | Obfuscated Files or Information 2 | LSA Secrets | File and Directory Discovery 1 | SSH | Keylogging | Data Transfer Size Limits | Fallback Channels | Manipulate Device Communication |
| Replication Through Removable Media | Launchd | Rc.common | Rc.common | Software Packing 2 | Cached Domain Credentials | System Information Discovery 1 2 | VNC | GUI Input Capture | Exfiltration Over C2 Channel | Multiband Communication | Jamming or Denial of Service |

# Behavior Graph




# Antivirus, Machine Learning and Genetic Malware Detection

## Initial Sample

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| doc_2021_98666_SIGNED - PRO FACTURA.exe | 24% | Virustotal | | Browse |
| doc_2021_98666_SIGNED - PRO FACTURA.exe | 43% | ReversingLabs | ByteCode-MSIL.Backdoor.NanoBot | |
| doc_2021_98666_SIGNED - PRO FACTURA.exe | 100% | Joe Sandbox ML | | |

## Dropped Files

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| C:\Users\user\AppData\Roaming\bWuIYd.exe | 100% | Joe Sandbox ML | | |
| C:\Users\user\AppData\Roaming\bWuIYd.exe | 24% | Virustotal | | Browse |
| C:\Users\user\AppData\Roaming\bWuIYd.exe | 43% | ReversingLabs | ByteCode-MSIL.Backdoor.NanoBot | |

## Unpacked PE Files

No Antivirus matches

## Domains

No Antivirus matches

## URLs

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| 194.5.98.127 | 0% | Avira URL Cloud | safe | |
| 127.0.0.1 | 0% | Virustotal | | Browse |
| 127.0.0.1 | 0% | Avira URL Cloud | safe | |

# Domains and IPs

## Contacted Domains

**No contacted domains info**

## Contacted URLs

| Name | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|
| 194.5.98.127 | true | • Avira URL Cloud: safe | unknown |
| 127.0.0.1 | true | • 0%, Virustotal, Browse<br>• Avira URL Cloud: safe | unknown |

## URLs from Memory and Binaries

## Contacted IPs

**No contacted IP infos**

# General Information

| | |
|---|---|
| Joe Sandbox Version: | 33.0.0 White Diamond |
| Analysis ID: | 458632 |
| Start date: | 03.08.2021 |
| Start time: | 15:55:41 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 8m 17s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | doc_2021_98666_SIGNED - PRO FACTURA.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: | 12 |
| 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@14/4@0/0 |
| EGA Information: | Failed |
| HDC Information: | • Successful, ratio: 6.9% (good quality ratio 3.3%)<br>• Quality average: 32.2%<br>• Quality standard deviation: 34% |
| HCA Information: | • Successful, ratio: 82%<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<br>• Stop behavior analysis, all processes terminated |
| Warnings: | Show All |

# Simulations

## Behavior and APIs

| Time | Type | Description |
|---|---|---|
| 15:56:31 | API Interceptor | 2x Sleep call for process: doc_2021_98666_SIGNED - PRO FACTURA.exe modified |

# 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\UsageLogs\doc_2021_98666_SIGNED - PRO FACTURA.exe.log**

| | |
|---|---|
| Process: | C:\Users\user\Desktop\doc_2021_98666_SIGNED - PRO FACTURA.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | modified |
| Size (bytes): | 1742 |
| Entropy (8bit): | 5.381353871108486 |
| Encrypted: | false |
| SSDEEP: | 48:MxHKEYHKGD8Ao6+vxpNl1qHGiD0HKeGitHTG1hAHKKPJAmHKoA9:iqEYqGgAo9ZPlwmI0qertzG1eqKPJ/qT |
| MD5: | 978918F6120A43D1FA5899938A5A542F |
| SHA1: | 6567A2E687B40BFD3A46246F51F4C89D93D89455 |
| SHA-256: | F814F290A540B3FD755D05F3434317D7B26F2C33D2087F9E63233CD88AB510FC |
| SHA-512: | 1DF2AF5A3F8212BF591AAA366FE96F167F3E6D43746E07B7CD44F1B2F06C63B1D290412891AD0B4D0A82D1DFD6EB2EB7D70981C35941F370DC97729E9205DD5 |
| Malicious: | **true** |
| Reputation: | moderate, very likely benign file |

| C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\doc_2021_98666_SIGNED - PRO FACTURA.exe.log | |
|---|---|
| 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_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll",0..3,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.V9921e851#\f2e0589ed6d670f264a5f65dd0ad000f\Microsoft.VisualBasic.ni.dll",0..3,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll",0..3,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_6 |

| C:\Users\user\AppData\Local\Temp\tmpDCE9.tmp | |
|---|---|
| Process: | C:\Users\user\Desktop\doc_2021_98666_SIGNED - PRO FACTURA.exe |
| File Type: | XML 1.0 document, ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 1639 |
| Entropy (8bit): | 5.176967825324459 |
| Encrypted: | false |
| SSDEEP: | 24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGktn:cbhK79lNQR/rydbz9I3YODOLNdq3N |
| MD5: | 335DC9045368E50919C4D67D509F2923 |
| SHA1: | DCBC293F1F440B13AF7E3771AF0F273E176ED4D6 |
| SHA-256: | 506CE973705FF1017DAF3E519B36BED172AFFBA6192741E50F9FD8826B7DBFB8 |
| SHA-512: | 8E80894560B11876FD0D606F0202C72FEC66AC745C5C1E32684BECC2B7D4834F8C99F7FBAFEACEAC648F26EFD5CFD2CE587407BCBE063E9AE3BE9EB72858CD5A |
| Malicious: | **true** |
| Reputation: | low |
| 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\bWuIYd.exe | |
|---|---|
| Process: | C:\Users\user\Desktop\doc_2021_98666_SIGNED - PRO FACTURA.exe |
| File Type: | PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows |
| Category: | dropped |
| Size (bytes): | 1202688 |
| Entropy (8bit): | 7.712684433960131 |
| Encrypted: | false |
| SSDEEP: | 24576:qmlBdz3ITXWl+O/JR308rntdkcr2VGSsjv1StbqiXk:RlBdz3OXW/RkAny7sjv0oi |
| MD5: | 532B5C7F4E3212A0D05E51C85864CAF6 |
| SHA1: | 9A46DD2C45B724E23A0E3D316EB7FBC16B144E19 |
| SHA-256: | 46510A62D266A7663F6CBE0A7FFBBBA5019A6C890512E5D050B667A8B44F6EA6 |
| SHA-512: | 55B368430E4B5FAA59CA892A15930B25DF9F571786CD21DBF87EE311B5DA033F24FD660E7750A51E3A92F3777E82F480C287C35C7FFC295B3A2EF7069B38E108 |
| Malicious: | **true** |
| Antivirus: | • Antivirus: Joe Sandbox ML, Detection: 100%<br>• Antivirus: Virustotal, Detection: 24%, Browse<br>• Antivirus: ReversingLabs, Detection: 43% |
| Reputation: | low |
| Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a....."...P..F.....Fe... .....@.. .....@.....d..O..... ..... ..H.....text...LE... ..F..... ..`.rsrc.....H.....@..@.relocc.....X.....@..B.....(e.....H.....$.....V.....0.....(....(.....(.....o.....*.....( .....(!.....("......(#.....($....*N..(....o....(%....*&..(&....*.s'.....s(.....s).....s*.....s+.....*....0.....~....o,....+..*.0.....~....o-....+..*.0.....~....o.....+..*.0.....~....o/....+..*.0.....~....o0....+..*.0..<.....~.....(1.....,lr...p.....(2...o3...s4.....~.....+..*.0..... |

| C:\Users\user\AppData\Roaming\bWuIYd.exe:Zone.Identifier | |
|---|---|
| Process: | C:\Users\user\Desktop\doc_2021_98666_SIGNED - PRO FACTURA.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 |

| C:\Users\user\AppData\Roaming\bWuIYd.exe:Zone.Identifier | |
|---|---|
| Preview: | [ZoneTransfer]....ZoneId=0 |

# Static File Info

## General

| | |
|---|---|
| File type: | PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows |
| Entropy (8bit): | 7.712684433960131 |
| TrID: | • Win32 Executable (generic) Net Framework (10011505/4) 49.80%<br>• Win32 Executable (generic) a (10002005/4) 49.75%<br>• Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36%<br>• Windows Screen Saver (13104/52) 0.07%<br>• Generic Win/DOS Executable (2004/3) 0.01% |
| File name: | doc_2021_98666_SIGNED - PRO FACTURA.exe |
| File size: | 1202688 |
| MD5: | 532b5c7f4e3212a0d05e51c85864caf6 |
| SHA1: | 9a46dd2c45b724e23a0e3d316eb7fbc16b144e19 |
| SHA256: | 46510a62d266a7663f6cbe0a7ffbbba5019a6c890512e5d050b667a8b44f6ea6 |
| SHA512: | 55b368430e4b5faa59ca892a15930b25df9f571786cd21dbf87ee311b5da033f24fd660e7750a51e3a92f3777e82f480c287c35c7ffc295b3a2ef7069b38e108 |
| SSDEEP: | 24576:qmlBdz3ITXWl+O/JR308rntdkcr2VGSsjv1StbqiXk:RlBdz3OXW/RkAny7sjv0oi |
| File Content Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a....."...P..F.....Fe... .....@.. .....@..... |

## File Icon

| | |
|---|---|
| Icon Hash: | 00828e8e8686b000 |

## Static PE Info

### General

| | |
|---|---|
| Entrypoint: | 0x526546 |
| Entrypoint Section: | .text |
| Digitally signed: | false |
| Imagebase: | 0x400000 |
| Subsystem: | windows gui |
| Image File Characteristics: | EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE |
| DLL Characteristics: | NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT |
| Time Stamp: | 0x61088FEA [Tue Aug 3 00:38:02 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 | 0x12454c | 0x124600 | False | 0.868892622381 | data | 7.71708373294 | IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ |
| .rsrc | 0x128000 | 0xfd4 | 0x1000 | False | 0.455322265625 | data | 5.68049715964 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .reloc | 0x12a000 | 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

**No network behavior found**

## Code Manipulations

## Statistics

### Behavior

Click to jump to process

## System Behavior

### Analysis Process: doc_2021_98666_SIGNED - PRO FACTURA.exe PID: 6512 Parent PID: 5840

### General

| | |
|---|---|
| Start time: | 15:56:30 |
| Start date: | 03/08/2021 |
| Path: | C:\Users\user\Desktop\doc_2021_98666_SIGNED - PRO FACTURA.exe |
| Wow64 process (32bit): | false |
| Commandline: | 'C:\Users\user\Desktop\doc_2021_98666_SIGNED - PRO FACTURA.exe' |
| Imagebase: | 0xa80000 |
| File size: | 1202688 bytes |
| MD5 hash: | 532B5C7F4E3212A0D05E51C85864CAF6 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | .Net C# or VB.NET |

| | |
|---|---|
| Yara matches: | • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.668794104.00000000032EA000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.669660281.0000000012F61000.00000004.00000001.sdmp, Author: Florian Roth<br>• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.669660281.0000000012F61000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: NanoCore, Description: unknown, Source: 00000000.00000002.669660281.0000000012F61000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> |
| Reputation: | low |

**File Activities** Show Windows behavior

**File Created**

**File Deleted**

**File Written**

**File Read**

## Analysis Process: schtasks.exe PID: 6744 Parent PID: 6512

### General

| | |
|---|---|
| Start time: | 15:56:34 |
| Start date: | 03/08/2021 |
| Path: | C:\Windows\System32\schtasks.exe |
| Wow64 process (32bit): | false |
| Commandline: | 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\bWuIYd' /XML 'C:\Users\user\AppData\Local\Temp\tmpDCE9.tmp' |
| Imagebase: | 0x7ff6fe380000 |
| File size: | 226816 bytes |
| MD5 hash: | 838D346D1D28F00783B7A6C6BD03A0DA |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | moderate |

**File Activities** Show Windows behavior

**File Read**

## Analysis Process: conhost.exe PID: 6752 Parent PID: 6744

### General

| | |
|---|---|
| Start time: | 15:56:34 |
| Start date: | 03/08/2021 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff724c50000 |
| File size: | 625664 bytes |
| MD5 hash: | EA777DEEA782E8B4D7C7C33BBF8A4496 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

## Analysis Process: doc_2021_98666_SIGNED - PRO FACTURA.exe PID: 6788 Parent PID: 6512

### General

| | |
|---|---|
| Start time: | 15:56:35 |
| Start date: | 03/08/2021 |
| Path: | C:\Users\user\Desktop\doc_2021_98666_SIGNED - PRO FACTURA.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Users\user\Desktop\doc_2021_98666_SIGNED - PRO FACTURA.exe |
| Imagebase: | 0xd50000 |
| File size: | 1202688 bytes |
| MD5 hash: | 532B5C7F4E3212A0D05E51C85864CAF6 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | low |

## Analysis Process: doc_2021_98666_SIGNED - PRO FACTURA.exe PID: 6804 Parent PID: 6512

### General

| | |
|---|---|
| Start time: | 15:56:35 |
| Start date: | 03/08/2021 |
| Path: | C:\Users\user\Desktop\doc_2021_98666_SIGNED - PRO FACTURA.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Users\user\Desktop\doc_2021_98666_SIGNED - PRO FACTURA.exe |
| Imagebase: | 0xc70000 |
| File size: | 1202688 bytes |
| MD5 hash: | 532B5C7F4E3212A0D05E51C85864CAF6 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | low |

## Analysis Process: doc_2021_98666_SIGNED - PRO FACTURA.exe PID: 6820 Parent PID: 6512

### General

| | |
|---|---|
| Start time: | 15:56:36 |
| Start date: | 03/08/2021 |
| Path: | C:\Users\user\Desktop\doc_2021_98666_SIGNED - PRO FACTURA.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Users\user\Desktop\doc_2021_98666_SIGNED - PRO FACTURA.exe |
| Imagebase: | 0xbf0000 |
| File size: | 1202688 bytes |
| MD5 hash: | 532B5C7F4E3212A0D05E51C85864CAF6 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | low |

## Analysis Process: doc_2021_98666_SIGNED - PRO FACTURA.exe PID: 6836 Parent PID: 6512

### General

| | |
|---|---|
| Start time: | 15:56:37 |
| Start date: | 03/08/2021 |
| Path: | C:\Users\user\Desktop\doc_2021_98666_SIGNED - PRO FACTURA.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Users\user\Desktop\doc_2021_98666_SIGNED - PRO FACTURA.exe |
| Imagebase: | 0xbb0000 |
| File size: | 1202688 bytes |
| MD5 hash: | 532B5C7F4E3212A0D05E51C85864CAF6 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | low |

## Analysis Process: doc_2021_98666_SIGNED - PRO FACTURA.exe PID: 6848 Parent PID: 6512

### General

| | |
|---|---|
| Start time: | 15:56:37 |
| Start date: | 03/08/2021 |
| Path: | C:\Users\user\Desktop\doc_2021_98666_SIGNED - PRO FACTURA.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Users\user\Desktop\doc_2021_98666_SIGNED - PRO FACTURA.exe |
| Imagebase: | 0x7c0000 |
| File size: | 1202688 bytes |
| MD5 hash: | 532B5C7F4E3212A0D05E51C85864CAF6 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | low |

# Disassembly

## Code Analysis