


**ID:** 433561
**Sample Name:** Facturas Pagadas Al Vencimiento.exe
**Cookbook:** default.jbs
**Time:** 15:15:46
**Date:** 12/06/2021
**Version:** 32.0.0 Black Diamond

# Table of Contents

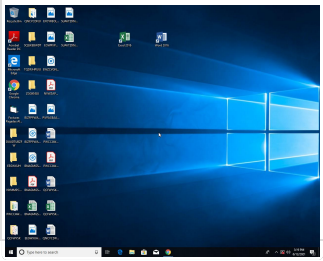
# Analysis Report Facturas Pagadas Al Vencimiento.exe

## Overview

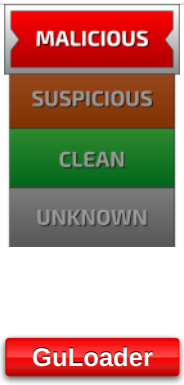
### General Information

| | |
|---|---|
| Sample Name: | Facturas Pagadas Al Vencimiento.exe |
| Analysis ID: | 433561 |
| MD5: | c8d357afda86354. |
| SHA1: | 026b3b6bafa462c. |
| SHA256: | 94bfbe95a21d987. |
| Infos: | |

Most interesting Screenshot:



### Detection

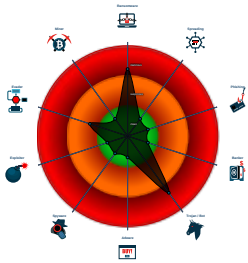



| | |
|---|---|
| Score: | 76 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 100% |

### Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Potential malicious icon found
- Yara detected GuLoader
- C2 URLs / IPs found in malware con…
- Checks if the current process is bein…
- Detected potential crypto function
- One or more processes crash
- PE file contains strange resources
- Sample file is different than original …
- Uses 32bit PE files
- Uses code obfuscation techniques (…

### Classification



## Process Tree

- **System is w10x64**
- Facturas Pagadas Al Vencimiento.exe (PID: 5992 cmdline: 'C:\Users\user\Desktop\Facturas Pagadas Al Vencimiento.exe' MD5: C8D357AFDA8635441BC5838244CA0029)
  - WerFault.exe (PID: 4020 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5992 -s 700 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 3468 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5992 -s 700 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

## Malware Configuration

### Threatname: GuLoader


```
{
  "Payload URL": "https://drive.google.com/uc?export=download&id=1dBTGLOe-ZeMuRpNWg8qsJp7BOE8QNF9s5l"
}
```


## Yara Overview

### Initial Sample

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| Facturas Pagadas Al Vencimiento.exe | JoeSecurity_GuLoader_1 | Yara detected GuLoader | Joe Security | |

## Sigma Overview

**No Sigma rule has matched**

# Signature Overview

Click to jump to signature section

## AV Detection:

**Found malware configuration**

**Multi AV Scanner detection for submitted file**

## Networking:

**C2 URLs / IPs found in malware configuration**

## System Summary:

**Potential malicious icon found**

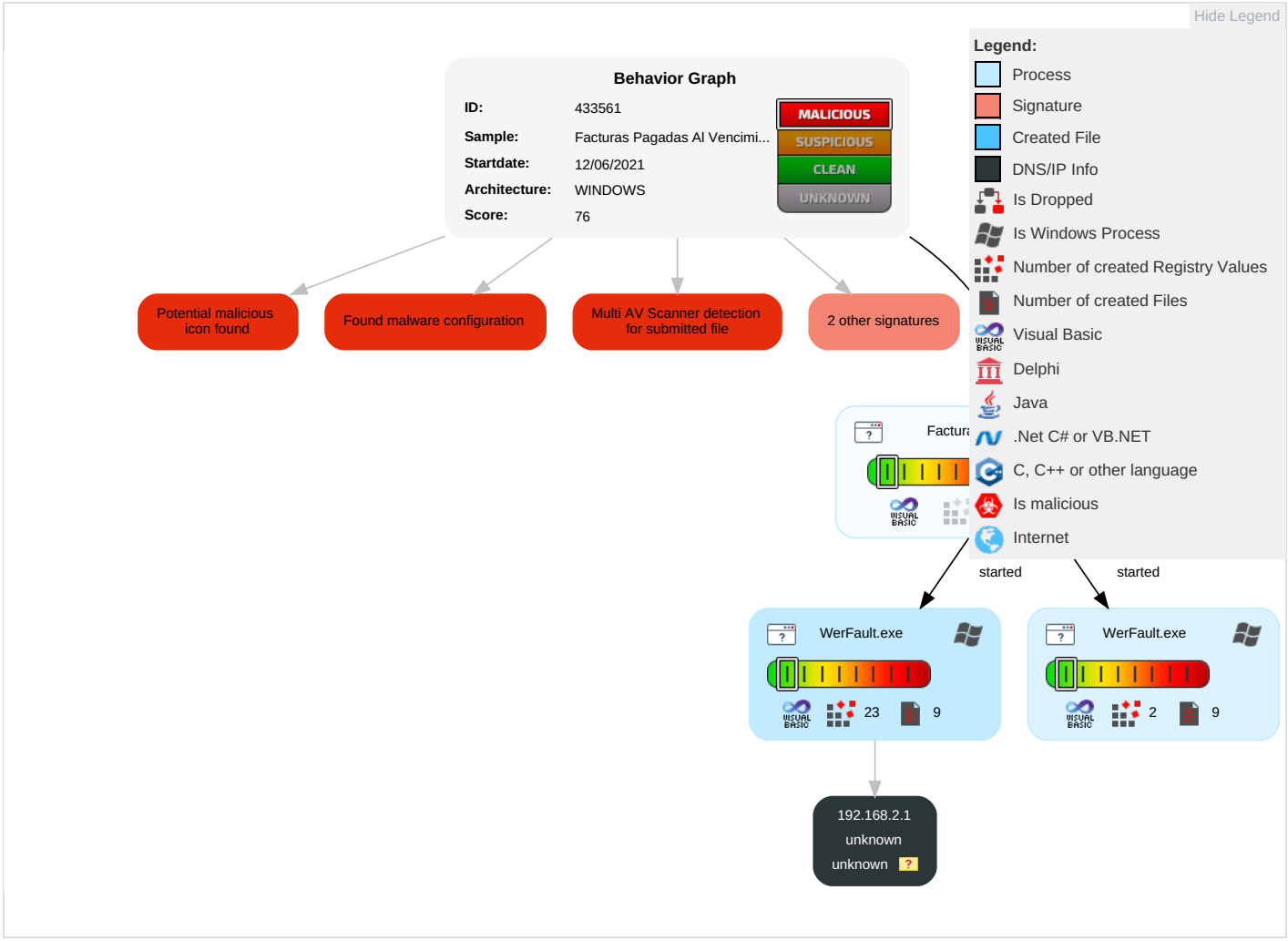
## Data Obfuscation:

**Yara detected GuLoader**

# Mitre Att&ck Matrix

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Network Effects | R S E |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Valid Accounts | Windows Management Instrumentation | Path Interception | Process Injection 2 | Virtualization/Sandbox Evasion 1 | OS Credential Dumping | Security Software Discovery 1 | Remote Services | Archive Collected Data 1 | Exfiltration Over Other Network Medium | Encrypted Channel 1 | Eavesdrop on Insecure Network Communication | R Tr W A |
| Default Accounts | Scheduled Task/Job | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | Process Injection 2 | LSASS Memory | Virtualization/Sandbox Evasion 1 | Remote Desktop Protocol | Data from Removable Media | Exfiltration Over Bluetooth | Application Layer Protocol 1 | Exploit SS7 to Redirect Phone Calls/SMS | R W W A |
| Domain Accounts | At (Linux) | Logon Script (Windows) | Logon Script (Windows) | Obfuscated Files or Information 1 | Security Account Manager | Process Discovery 1 | SMB/Windows Admin Shares | Data from Network Shared Drive | Automated Exfiltration | Steganography | Exploit SS7 to Track Device Location | O D C Ba |
| Local Accounts | At (Windows) | Logon Script (Mac) | Logon Script (Mac) | Binary Padding | NTDS | System Information Discovery 1 | Distributed Component Object Model | Input Capture | Scheduled Transfer | Protocol Impersonation | SIM Card Swap | |
| Cloud Accounts | Cron | Network Logon Script | Network Logon Script | Software Packing | LSA Secrets | Remote System Discovery 1 | SSH | Keylogging | Data Transfer Size Limits | Fallback Channels | Manipulate Device Communication | |

# Behavior Graph




## Screenshots

### Thumbnails

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


## Antivirus, Machine Learning and Genetic Malware Detection

### Initial Sample

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| Facturas Pagadas Al Vencimiento.exe | 71% | Virustotal | | Browse |
| Facturas Pagadas Al Vencimiento.exe | 49% | Metadefender | | Browse |
| Facturas Pagadas Al Vencimiento.exe | 70% | ReversingLabs | Win32.Trojan.Midie | |

### Dropped Files

No Antivirus matches

### Unpacked PE Files

No Antivirus matches

### Domains

No Antivirus matches

### URLs

No Antivirus matches

# Domains and IPs

## Contacted Domains

**No contacted domains info**

## Contacted IPs

### Public

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|

### Private

| IP |
|---|
| 192.168.2.1 |

# General Information

| | |
|---|---|
| Joe Sandbox Version: | 32.0.0 Black Diamond |
| Analysis ID: | 433561 |
| Start date: | 12.06.2021 |
| Start time: | 15:15:46 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 6m 19s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | Facturas Pagadas Al Vencimiento.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 |
| Run name: | Run with higher sleep bypass |
| Number of analysed new started processes analysed: | 32 |
| 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: | mal76.rans.troj.winEXE@3/8@0/1 |
| EGA Information: | • Successful, ratio: 100% |
| HDC Information: | • Successful, ratio: 14.2% (good quality ratio 2.9%)<br>• Quality average: 15.3%<br>• Quality standard deviation: 28.6% |
| HCA Information: | Failed |
| Cookbook Comments: | • Adjust boot time<br>• Enable AMSI<br>• Sleeps bigger than 120000ms are automatically reduced to 1000ms<br>• Found application associated with file extension: .exe |
| Warnings: | Show All |

# Simulations

## Behavior and APIs

No simulations

# Joe Sandbox View / Context

## IPs

No context

## Domains

No context

## ASN

No context

## JA3 Fingerprints

No context

## Dropped Files

No context

# Created / dropped Files

**C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_Facturas Pagadas_2024e1b44264dba4d9a5d8d4883c883c62d1e68_380e93cd_0deaea8c\Report.wer**

| | |
|---|---|
| Process: | C:\Windows\SysWOW64\WerFault.exe |
| File Type: | Little-endian UTF-16 Unicode text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 11522 |
| Entropy (8bit): | 3.7779875477893152 |
| Encrypted: | false |
| SSDEEP: | 96:E0WeR7FA3gQzFD7DcSpXIQcQ5c6ScE4cw3M+HbHg/TVG4rmMoVazWbSmnFdOyPnn:V/RZKC0HnWSZja0l/u7sBS274ItSBH |
| MD5: | 4B4AAAB6AA87EE3404CD940DAFFD5E10 |
| SHA1: | 9D8F2B8D18BB78CE8FA09F90FFB6CF1AA7B0633B |
| SHA-256: | 60A9774D4EAE77F5E8FEA37CDC7A02F19AD6D43A828CDEB930846AE9ED8F5639 |
| SHA-512: | CE4A08AAC1F739181241AE00918C2E98871697520D655A187CC5AAF3CB2F3044E3CBEE17BDE38D347A593F146889A9F70A2F15F2187234FD771DB48B7412F8DF |
| Malicious: | false |
| Reputation: | low |
| Preview: | ..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.6.8.0.0.9.8.1.6.5.5.6.1.6.4.2.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.6.8.0.0.9.8.1.7.2.5.9.2.8.7.6.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.2.7.e.6.b.0.4.2.-.7.f.6.4.-.4.5.7.d.-.b.4.7.5.-.4.8.1.6.6.8.6.f.7.0.c.0.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.1.2.4.8.6.8.0.7.-.7.2.d.6.-.4.5.5.e.-.b.8.f.0.-.a.6.b.0.c.0.1.8.8.a.c.9.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.F.a.c.t.u.r.a.s. .P.a.g.a.d.a.s. .A.l. .V.e.n.c.i.m.i.e.n.t.o...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.G.R.F.T.N.I.N.G...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.1.7.6.8.-.0.0.0.1.-.0.0.1.7.-.f.3.6.3.-.b.4.9.9.d.8.5.f.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.7.2.e.9.0.d.e.3.b.2.2.c.3.8.1.3.0.2.7.1.1.4.8.7.a.2.3.3.c.3.1.6.0.0.0.0.3.0.0.4.!.0.0.0.0.0.2.6.b.3.b.6.b.a.f.a. |

**C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_Facturas Pagadas_e1b59d2026da206526c3718df9ca6d5772b50_380e93cd_0fd4bcc5\Report.wer**

| | |
|---|---|
| Process: | C:\Windows\SysWOW64\WerFault.exe |
| File Type: | Little-endian UTF-16 Unicode text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 11522 |
| Entropy (8bit): | 3.7742938090874323 |

| C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_Facturas Pagadas_e1b59d2026da206526c3718df9ca6d5772b50_380e93cd_0fd4bcc5\Report.wer | |
|---|---|
| Encrypted: | false |
| SSDEEP: | 96:t6GRK3gQzFD7fcSpXIQcQNc6LmgcEdcw3++HbHg/TVG4rmMoVazWbSmnFdOyPnri:sGRs+0HDOgHTja0l/u7sBS274ItSBu |
| MD5: | 8260AD2649897CE3374067EF099A5818 |
| SHA1: | 4F6FD36E5C60F25339EC5B4875FACF7FA5657B9D |
| SHA-256: | 41C4BD73CDC2CAB31F0D1CE35988A27921BEADE4B3C247A184F70E1F97E1D605 |
| SHA-512: | B78DA89F6631DFEDF6D4468A22519810FACA74DF1AEC319DEBF84FCA179744636A6B5D13DF7FABEE05C81787EA16CA712BB5A3D86F7348F9ED79B47EB6600E43 |
| Malicious: | false |
| Reputation: | low |
| Preview: | ..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.6.8.0.0.9.8.0.4.6.0.3.0.7.5.2.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.6.8.0.0.9.8.0.5.3.5.3.0.6.5.2.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.e.7.2.c.d.9.b.b.-.b.5.a.4.-.4.d.8.e.-.b.e.0.9.-.a.b.1.d.a.7.8.e.b.a.8.8.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.f.5.b.d.6.d.f.6.-.7.8.3.7.-.4.8.a.c.-.b.5.b.e.-.f.4.0.6.c.e.a.9.9.3.0.b.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.F.a.c.t.u.r.a.s. .P.a.g.a.d.a.s. .A.l. .V.e.n.c.i.m.i.e.n.t.o...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.G.R.F.T.N.I.N.G...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.1.7.6.8.-.0.0.0.1.-.0.0.1.7.-.f.3.6.3.-.b.4.9.9.d.8.5.f.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.7.2.e.9.0.d.e.3.b.2.2.c.3.8.1.3.0.2.7.1.1.4.8.7.a.2.3.3.c.3.1.6.0.0.0.0.3.0.0.4.!.0.0.0.0.0.2.6.b.3.b.6.b.a.f.a. |

| C:\ProgramData\Microsoft\Windows\WER\Temp\WERB3CC.tmp.dmp | |
|---|---|
| Process: | C:\Windows\SysWOW64\WerFault.exe |
| File Type: | Mini DuMP crash report, 14 streams, Sat Jun 12 22:16:45 2021, 0x1205a4 type |
| Category: | dropped |
| Size (bytes): | 51454 |
| Entropy (8bit): | 2.2977818654342994 |
| Encrypted: | false |
| SSDEEP: | 192:CIht6jjRywPqC8vPl/SM4Lek2kIZm2Gi8mzF9Vm2gOf73qTf5ByX:RD6AqV8vPlKM22TZ6uY2U5I |
| MD5: | 40BA2704DA382E2ED63FDA445C8C5137 |
| SHA1: | FE7AA8F39E0CD12428DFF528EF7B98C703F56187 |
| SHA-256: | 9E1F43BC1230C158B5E0AC5B5C1D40F66331BD39DD442F4865515EA77A6F1F63 |
| SHA-512: | A701B0AAA880183C72FBC1F1CC453A8DCD4B53AD12E14946A4142139F68A57D3F7FD5CC71506BBEC2F5527E2E7998DCA406AAE55B3467695F1C3376A282A375 |
| Malicious: | false |
| Reputation: | low |
| Preview: | MDMP..... .....M2.`.....U.....B.....GenuineIntelW.....T.....h...@2.`.....0..2.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1..... |

| C:\ProgramData\Microsoft\Windows\WER\Temp\WERB592.tmp.WERInternalMetadata.xml | |
|---|---|
| Process: | C:\Windows\SysWOW64\WerFault.exe |
| File Type: | XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 8388 |
| Entropy (8bit): | 3.697296467124024 |
| Encrypted: | false |
| SSDEEP: | 192:Rrl7r3GLNipiD6IDNLMecp6YSISUuUn95ksgmfo0vFSBWCpr+89bILsfw4m:RrlsNip+6IDa6Y9SUPnjgmfo0NSvIQfW |
| MD5: | A5F48B31EED215788A3E197603FB151A |
| SHA1: | E5DE19D278B807DF7BB2CCF62B5BD36A9EA1D014 |
| SHA-256: | 308D44600633D8C49F628B22BB7FB449651E45201EDE94024F48391CB5BA4E57 |
| SHA-512: | 687D5ABC5F672398B06A05851BF4FD205F03D0CF5EE8D9E9FFE7C4017C9FE5AB82E60555BE04CAD5B59DEA930EB198EED8CFE7286ECC29A0D5F1ABE0AAB07E3F |
| Malicious: | false |
| Reputation: | low |
| Preview: | ..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.9.9.2.<./.P.i.d.>..... |

| C:\ProgramData\Microsoft\Windows\WER\Temp\WERB620.tmp.xml | |
|---|---|
| Process: | C:\Windows\SysWOW64\WerFault.exe |
| File Type: | XML 1.0 document, ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 4741 |
| Entropy (8bit): | 4.500617379796648 |
| Encrypted: | false |
| SSDEEP: | 48:cvIwSD8zskJgtWI9tpWSC8B28fm8M4JXT7/SIFAo+q8a7IIclCzX3XH8Pd:uITfiqYSNFJHNlEHHgd |

| C:\ProgramData\Microsoft\Windows\WER\Temp\WERB620.tmp.xml | |
|---|---|
| MD5: | 82480489627A469CB8B64F9F25FBA641 |
| SHA1: | AF29C719D34F13F8177C9801C1B02782035AF5B5 |
| SHA-256: | DB82AA4A5A7E71C2110B36F53DEC4A46B11A12F9279757444E5D15CB4FA982C6 |
| SHA-512: | 7853DFE8AD7648CBBFC4F180D9995173884D689F6591218C37C9F0E99F72CE4C46215C5A4D524725D777A3D3BC14E306B1BAA098BDAFF5CAF1A433E6C874D72 |
| Malicious: | false |
| Reputation: | low |
| Preview: | <?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1031487" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />.. |

| C:\ProgramData\Microsoft\Windows\WER\Temp\WERE27D.tmp.dmp | |
|---|---|
| Process: | C:\Windows\SysWOW64\WerFault.exe |
| File Type: | Mini DuMP crash report, 14 streams, Sat Jun 12 22:16:56 2021, 0x1205a4 type |
| Category: | dropped |
| Size (bytes): | 46842 |
| Entropy (8bit): | 2.142337644740741 |
| Encrypted: | false |
| SSDEEP: | 192:TIh/7xjYsPSk2kIZi270hF8mzF3hp8yDOQOSObI5ehZrL2:s97vPp2TlQwudOI5GG |
| MD5: | 4C981AA79224125A1E780F9D1015A72B |
| SHA1: | 85C83302C1E9528E18916BD10692C77DA2E53EF4 |
| SHA-256: | 34B661D83ACF83D81780724FCC6CE328D8E21BEFF02EF9F37A693B3F93C8E5D5 |
| SHA-512: | 5D823E8792151DED4C21678212301893B9C633508BCE07FD1CAFB30515A3AA6D8810CA4788C78BD0461FAB06475DA533D6AB2B1BE5A6BCFECBC06EF76787F09 |
| Malicious: | false |
| Reputation: | low |
| Preview: | MDMP..... .....X2.`.....U.....B.....GenuineIntelW.....T.....h...@2.`.....0..2.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1..... |

| C:\ProgramData\Microsoft\Windows\WER\Temp\WERE443.tmp.WERInternalMetadata.xml | |
|---|---|
| Process: | C:\Windows\SysWOW64\WerFault.exe |
| File Type: | XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 8394 |
| Entropy (8bit): | 3.7033486108502083 |
| Encrypted: | false |
| SSDEEP: | 192:Rrl7r3GLNipiH6IDChcp6YS9SUTnCZgmfo0jFSKCpDW89bbLsfVpm:RrlsNipa6IDD6YYSUTncgmfo05SlbQfC |
| MD5: | F5C74121B5DC9EE9131757F8F2AFE6A4 |
| SHA1: | 4FF4B4382606315D7340C280370D0243AF67A8CD |
| SHA-256: | 25F595AB58251EDA060DD93BFCFE1C0070E007F5AEF3F5B1F08AD57D3A09A1B7 |
| SHA-512: | CF911D20F34F8F87D18CFE32B1D431E35AFFC0ABA46C4DBD00B185E2A06620F2234E4B7051AD24BA5DAA104E8EC1D2CC0AA75ACFB1A288FA74713AC5945A8AA1 |
| Malicious: | false |
| Reputation: | low |
| Preview: | ..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.9.9.2.<./.P.i.d.>..... |

| C:\ProgramData\Microsoft\Windows\WER\Temp\WERE4B2.tmp.xml | |
|---|---|
| Process: | C:\Windows\SysWOW64\WerFault.exe |
| File Type: | XML 1.0 document, ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 4741 |
| Entropy (8bit): | 4.499433919214349 |
| Encrypted: | false |
| SSDEEP: | 48:cvIwSD8zskJgtWI9tpWSC8BNs8fm8M4JXT7/SWFGm+q8a7l2clCzX3XH8Pd:uITfiqYSN3RJrTlEHHgd |
| MD5: | 247823C0DFE1056D126DCFEFF884585A |
| SHA1: | E5795350EAAE9A34C6E9D540BC0BFDF6345CBA37 |
| SHA-256: | 31458DB04F33FEB4CC874E0F39C370A98C637DA7FE1A95D00CB04AFA209ADFEA |

| C:\ProgramData\Microsoft\Windows\WER\Temp\WERE4B2.tmp.xml | |
|---|---|
| SHA-512: | F35626524A9F16C3B863B3CE2EA6C66584994FE1CE9699EB15985EE807469C7E1B477C7BFCB84ED33B5AE6C77539D5043DE4CFB58659D8D98AF4881F399CC11 |
| Malicious: | false |
| Reputation: | low |
| Preview: | <?xml version="1.0" encoding="UTF-8" standalone="yes"?..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1031487" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />.. |

# Static File Info

## General

| | |
|---|---|
| File type: | PE32 executable (GUI) Intel 80386, for MS Windows |
| Entropy (8bit): | 4.463887810480926 |
| TrID: | • Win32 Executable (generic) a (10002005/4) 99.15%<br>• Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81%<br>• Generic Win/DOS Executable (2004/3) 0.02%<br>• DOS Executable Generic (2002/1) 0.02%<br>• Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00% |
| File name: | Facturas Pagadas Al Vencimiento.exe |
| File size: | 135168 |
| MD5: | c8d357afda8635441bc5838244ca0029 |
| SHA1: | 026b3b6bafa462c763860afeb21b3cfe05aeb600 |
| SHA256: | 94bfbe95a21d987080ac95825abde8cf1aa7955fa711c8daeea32ba18590979d |
| SHA512: | 0630394ea500b46626aeb13033d6d6c213c79f1d7babc187e3bc62e4dc43272b57863fe1cdd33d83312866374801147b4975f2631c44c96aa23f48150b8498bd |
| SSDEEP: | 1536:8r2A295OAR92knLfapZm5sXu0dtyb/vxG8A:9A295OAR9ffUb+3m |
| File Content Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#...B...B...B..L^...B...`...B...d...B..Rich.B.....PE..L...hO.`.....0.....@..... |

## File Icon

| | |
|---|---|
| Icon Hash: | 20047c7c70f0e004 |

## Static PE Info

### General

| | |
|---|---|
| Entrypoint: | 0x4014bc |
| Entrypoint Section: | .text |
| Digitally signed: | false |
| Imagebase: | 0x400000 |
| Subsystem: | windows gui |
| Image File Characteristics: | LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED |
| DLL Characteristics: | |
| Time Stamp: | 0x60BD4F68 [Sun Jun 6 22:42:48 2021 UTC] |
| TLS Callbacks: | |
| CLR (.Net) Version: | |
| OS Version Major: | 4 |
| OS Version Minor: | 0 |
| File Version Major: | 4 |
| File Version Minor: | 0 |
| Subsystem Version Major: | 4 |
| Subsystem Version Minor: | 0 |

### General

| | |
|---|---|
| Import Hash: | 54ea68151857c1f30c42224007018bf1 |

### Entrypoint Preview

### Data Directories

### Sections

| Name | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy | Characteristics |
|---|---|---|---|---|---|---|---|---|
| .text | 0x1000 | 0x1db78 | 0x1e000 | False | 0.337109375 | data | 4.7219788122 | IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ |
| .data | 0x1f000 | 0x1230 | 0x1000 | False | 0.00634765625 | data | 0.0 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ |
| .rsrc | 0x21000 | 0x9b8 | 0x1000 | False | 0.178466796875 | data | 2.11818351755 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |

### Resources

### Imports

### Version Infos

### Possible Origin

| Language of compilation system | Country where language is spoken | Map |
|---|---|---|
| Sesotho (Sutu) | South Africa |  |

## Network Behavior

### Network Port Distribution

### UDP Packets

## Code Manipulations

## Statistics

### Behavior

Click to jump to process

## System Behavior

### Analysis Process: Facturas Pagadas Al Vencimiento.exe PID: 5992 Parent PID: 5660

### General

| | |
|---|---|
| Start time: | 15:16:32 |
| Start date: | 12/06/2021 |
| Path: | C:\Users\user\Desktop\Facturas Pagadas Al Vencimiento.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Users\user\Desktop\Facturas Pagadas Al Vencimiento.exe' |
| Imagebase: | 0x400000 |
| File size: | 135168 bytes |
| MD5 hash: | C8D357AFDA8635441BC5838244CA0029 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | Visual Basic |
| Reputation: | low |

### File Activities

Show Windows behavior

## Analysis Process: WerFault.exe PID: 4020 Parent PID: 5992

### General

| | |
|---|---|
| Start time: | 15:16:43 |
| Start date: | 12/06/2021 |
| Path: | C:\Windows\SysWOW64\WerFault.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\SysWOW64\WerFault.exe -u -p 5992 -s 700 |
| Imagebase: | 0xbb0000 |
| File size: | 434592 bytes |
| MD5 hash: | 9E2B8ACAD48ECCA55C0230D63623661B |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | Visual Basic |
| Reputation: | high |

### File Activities

Show Windows behavior

#### File Created

#### File Deleted

#### File Written

### Registry Activities

Show Windows behavior

#### Key Created

#### Key Value Created

## Analysis Process: WerFault.exe PID: 3468 Parent PID: 5992

### General

| | |
|---|---|
| Start time: | 15:16:56 |
| Start date: | 12/06/2021 |
| Path: | C:\Windows\SysWOW64\WerFault.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\SysWOW64\WerFault.exe -u -p 5992 -s 700 |
| Imagebase: | 0xbb0000 |
| File size: | 434592 bytes |

| | |
|---|---|
| MD5 hash: | 9E2B8ACAD48ECCA55C0230D63623661B |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | Visual Basic |
| Reputation: | high |

**File Activities** Show Windows behavior

**File Created**

**File Deleted**

**File Written**

**Registry Activities** Show Windows behavior

**Key Created**

**Key Value Modified**

# Disassembly

## Code Analysis