ID: 433561
Sample Name: Facturas Pagadas Al Vencimiento.exe
Cookbook: default.jbs
Time: 15:09:33
Date: 12/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

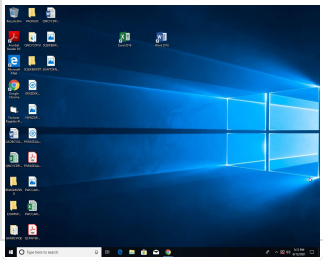
Analysis Report Facturas Pagadas Al Vencimiento.exe

Overview

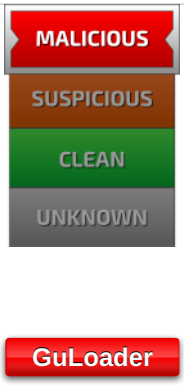
General Information

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

Most interesting Screenshot:



Detection



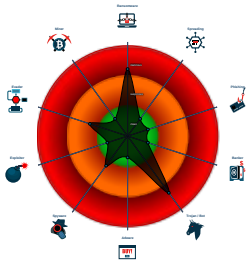
GuLoader

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…
- Creates a DirectInput object (often fo…
- Detected potential crypto function
- One or more processes crash
- PE file contains strange resources
- Sample file is different than original …
- Uses 32bit PE files

Classification



Process Tree

- **System is w10x64**
- Facturas Pagadas Al Vencimiento.exe (PID: 6040 cmdline: 'C:\Users\user\Desktop\Facturas Pagadas Al Vencimiento.exe' MD5: C8D357AFDA8635441BC5838244CA0029)
  - WerFault.exe (PID: 5540 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6040 -s 696 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 3180 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6040 -s 696 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

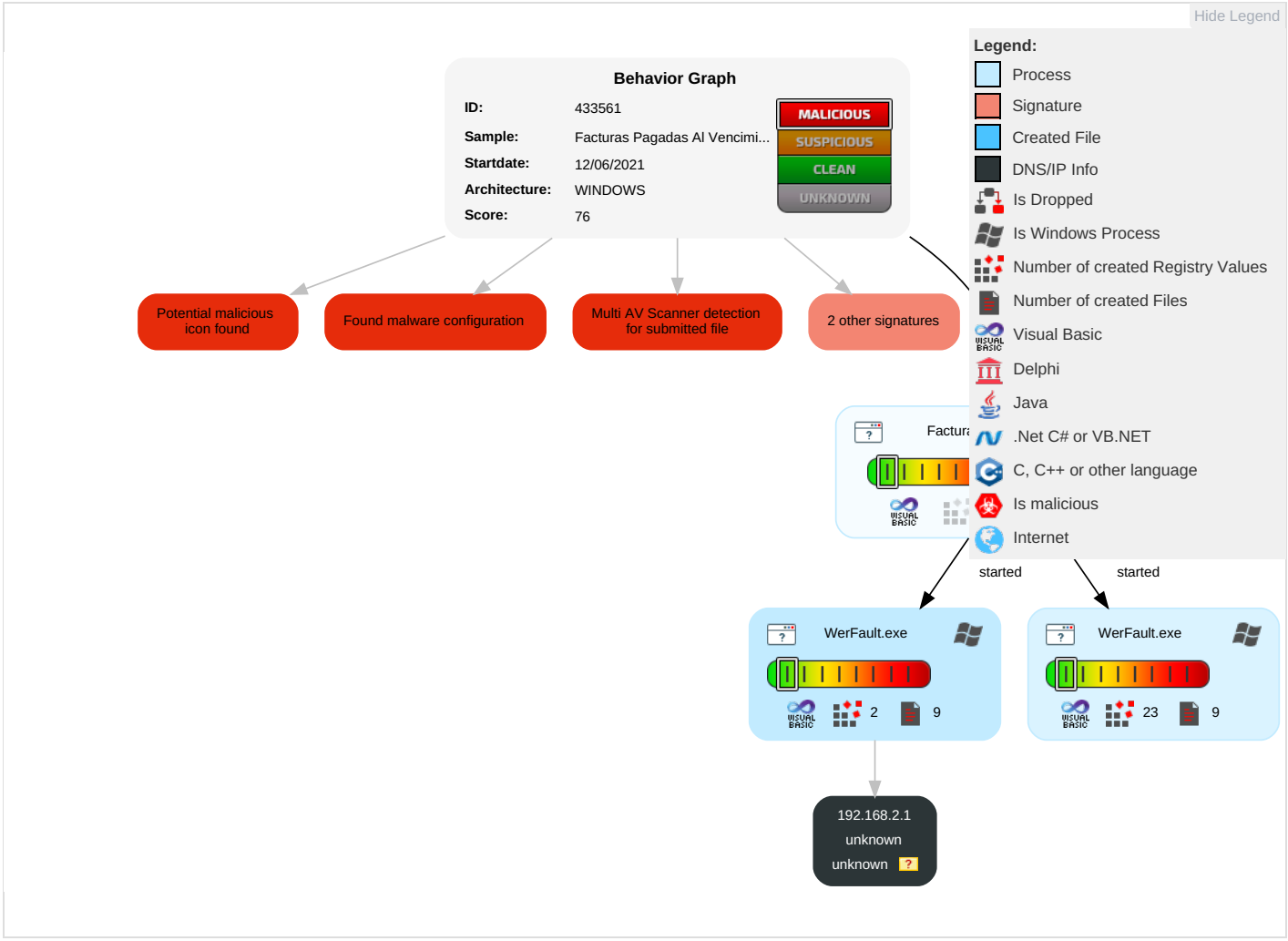
Data Obfuscation:

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	Re Se Ef
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 2	Virtualization/Sandbox Evasion 1	Input Capture 1	Security Software Discovery 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Re Tr W Au
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	Archive Collected Data 1	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Re W W Au
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	Ol De Cl 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	

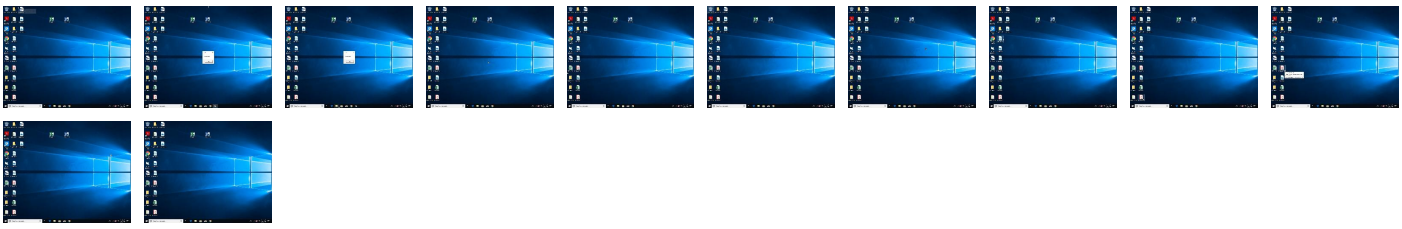
Behavior Graph



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:	15:09:33
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 26s
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
Number of analysed new started processes analysed:	25
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 • EGA enabled • HDC enabled • 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%) • Quality average: 15.3% • Quality standard deviation: 28.6%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
15:10:33	API Interceptor	2x Sleep call for process: WerFault.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:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_Facturas Pagadas_2024e1b44264dba4d9a5d8d4883c883c62d1e68_380e93cd_0c3f9333\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	11524
Entropy (8bit):	3.776556767599868
Encrypted:	false
SSDEEP:	96:UYX3IxwgNFA3gQzFD7DcSpXIQcQ5c6ScE4cw3M+HbHg/TVG4rmMoVazWbSmnFdOx:r4xwg/KC0HnWSZja0l/u7sXS274ItSBw
MD5:	9EA029D2DEC2DAC1871DA0DE53099B26
SHA1:	EC7F053B9C4D11B27BA47633298867D30D4348AE
SHA-256:	DA4F27E735FEA5ECF5F676004681DC59A448345BBB6EA095624B160C2BF7C63A
SHA-512:	FD3C3369C289ED666F47C10EE187B42B089B25C9E49762FD003A5F944B3C8CE00897077152FCC3165F29115C55B02E0DE3B31D6247D5F24F25631B15DBDC9FB
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.=.1.3.2.6.8.0.0.9.4.4.1.7.0.5.0.2.1.8.....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.=.1.3.2.6.8.0.0.9.4.4.2.2.5.1.9.5.0.5.....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.=.4.0.a.1.6.3.d.7.-.9.a.9.1.-.4.a.6.a.-.9.d.7.5.-.3.f.a.c.1.b.8.d.9.7.9.5.....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.=.9.f.b.5.c.2.0.9.-.b.b.5.0.-.4.6.9.c.-.8.c.f.0.-.1.4.f.e.5.4.6.0.0.8.d.e.....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.=.0.0.0.0.0.1.7.9.8.-.0.0.0.1.-.0.0.1.7.-.a.1.e.1.-.9.d.b.a.d.7.5.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_15f7655d\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	11526
Entropy (8bit):	3.7729071083685213
Encrypted:	false

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_Facturas Pagadas_e1b59d2026da206526c3718df9ca6d5772b50_380e93cd_15f7655d\Report.wer	
SSDEEP:	192:4G7zwgC+0HDOgHTja0l/u7sXS274ItSBC:b7zwgCNDHHTjO/u7sXX4ItSw
MD5:	A29547129D5A2CB01A0ACB99A9CDC563
SHA1:	C9AFB5880D3BCA7B7F8D44895DAAECCA6FA30BA5
SHA-256:	35C3B671447641B38440405ABA08AC6B6296BE017A0CE7F9A1D4E394B0C86DB7
SHA-512:	2C3199487863F9191D8BAF336C42F5368241DB588D030449C51DC287E757519F231481CE60D0B5652DBC15CFA3CB07455A38F7D8EC64737FB85BA51635627963
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.=.1.3.2.6.8.0.0.9.4.3.1.1.2.6.9.2.2.6.....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.=.1.3.2.6.8.0.0.9.4.3.1.7.2.0.6.7.3.1.....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.=.7.2.0.e.6.a.7.7.-.8.6.f.8.-.4.d.c.7.-.9.0.d.1.-.4.e.7.5.0.c.9.9.9.b.c.5.....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.=.e.2.0.8.1.8.8.c.-.0.a.6.5.-.4.5.b.1.-.a.1.6.0.-.1.a.0.4.f.9.2.2.d.0.4.e.....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.=.0.0.0.0.0.1.7.9.8.-.0.0.0.1.-.0.0.1.7.-.a.1.e.1.-.9.d.b.a.d.7.5.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\WER5C35.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Sat Jun 12 22:10:31 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	45970
Entropy (8bit):	2.4100728525187844
Encrypted:	false
SSDEEP:	192:yOh/DVldZ7UACdPlSlCyaLbHT1yn/X2iZs2wbGVfZNMdk3/bS5JdUwa0IkM:LdLLdCdPl1yIcej9/dqDStS0+
MD5:	1631B17E646B5ABB302115F47F42516A
SHA1:	6B9FA3B6E2E47306B33C4622A993A43446ACF02E
SHA-256:	635BAF95212741218C99B5A61B6E547E1DB55CC61C49A900BAE3751D9049964B
SHA-512:	8E83BFF4B35A75032CD9F5FE5273A51FFF4AA62A99D8623AF97D86D471935712CBCC40B2FCDF115B1DAFE52BDE5B1F44CE722B110394F45A717B06C7FDA27B9
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....0.`.....U.....B.....GenuineIntelW.....T.....0.`.....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\WER5D8E.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):	8386
Entropy (8bit):	3.693798672862176
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiZu6IDP6YSySUqFgmfo0vFSBiCprV89btMsfpvm:RrlsNiA6IDP6YXSUqFgmfo0NSOtffM
MD5:	6E948DEB4BF5FCA5846D52C14CEB2F19
SHA1:	98419967C462534BCBD83F4D5992DCFBFD2018B3
SHA-256:	E78B92EC4695D4C464298740C0A83F09392971B5A99D945FE41D2AC318F3841D
SHA-512:	04D3A57C5D51C87FDEBB41DC9D24A49D9369D199F704FE0985A6090D1367CBE6E755DA739EAD1E561E8F1A5AE523E58A4CBFD47B28071E067A09A8C7F44AD5C9
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.>.6.0.4.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E2B.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):	4.490976525072211
Encrypted:	false
SSDEEP:	48:cvIwSD8zsKJgtWI9NpWSC8Bws8fm8M4JXT7/SIFK0C+q8a7lIGCzX3XqPd:uITfYuYSNeJutEHSd
MD5:	5C690A8607E83CF1AC15D11729446481

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E2B.tmp.xml	
SHA1:	C1E5152E057B266A70454F0D541FE284F165CE74
SHA-256:	A712512A506D92FC2E5EA1BF56026954E8D67CF61AD60C1CDAA6AED6527858F2
SHA-512:	CA694FD5649DBAB675DCC0B6167867DB16867EDB91607C5B98E29FDC66B954F49D3780A33F9563EBCB2C2ED50F7C7445BB4E62CE5C6600AC460A6DEA67B0E73
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="1031481" />.. <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\WER8587.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Sat Jun 12 22:10:41 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	46862
Entropy (8bit):	2.140785403689248
Encrypted:	false
SSDEEP:	192:sOhCRR2dm20T1yn/72Zhw8mz2EUlSAqzF8ZUU2JSY:BM2opcKZfu7GSDzMJY
MD5:	740B80A74D73165741D221C663BF2747
SHA1:	F9CA62EE3CCA562211EC55E79D567EBB8FD44A22
SHA-256:	4A265581BA51892FC94B803C6E776FF2B2E3FD5004B6E5E7E07FEA1A8F8B8AEC
SHA-512:	5462DC6E03F806A9D063BFA3B7C007C6BBAB750036E861DAF29A248C5D570F09F66C7B503998D015F69572747B0CE24EBDE4DC8443CB39298494C8F6A540D57
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....0.`.....U.....B.....GenuineIntelW.....T.....0.`.....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\WER86B1.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):	3.6980242405197026
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiZf6ID9o6YSfSU8Ajgmfo0jFSeCpDi89bBMsfsrm:RrlsNih6ID9o6Y6SU8Ajgmfo05SlBffN
MD5:	F922260DAAF05B490EB120AEF46E81FE
SHA1:	47DA4C10A2B4B214357A85DC16824168DB99251C
SHA-256:	839A6D242FE912CC16F82DF24F0D0214F1F0E20D7816B49B9FAEA715A575A93A
SHA-512:	A619DF416750571E521ABA7F5621A7A8E94239FF26DD07B034C65C37F1B5B06E518D8483EAF160004188C0E670B15D1E59208E208863530EC5C9E227E96F6120
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.>.6.0.4.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER874F.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):	4.493586948294421
Encrypted:	false
SSDEEP:	48:cvIwSD8zsKJgtWI9NpWSC8BZ8fm8M4JXT7/SWFlL+q8a7l2GCzX3XqPd:uITfYuYSN4J3vEHSd
MD5:	E02DDF099C74EDBE4B94FCE2858DFE5D
SHA1:	050B6AA8F3393539E468BD039BA4C76DFF46D763
SHA-256:	93E8E1A1BED1CE09C3229858CCE21C853F7F958E1B6A29063875123220844AA6
SHA-512:	63BD92AAA8079571025B78252D1A3002482EDCB79EEEAA3E50FA7D0A104BB22E39F647C16904392FBD51247BBC3DA2669BCFC7EAD6494BE27B3773FA310487C2

C:\ProgramData\Microsoft\Windows\WER\Temp\WER874F.tmp.xml	
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="1031481" />.. <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% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • 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:	0630394ea500b46626aeb13033d6d6c213c79f1d7babc187e3bc62e4dc43272b57863fe1cdd33d83312866374801547b4975f2631c44c96aa23f48150b8498bd
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
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: 6040 Parent PID: 5604

General

Start time:	15:10:18
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: 5540 Parent PID: 6040

General

Start time:	15:10:30
Start date:	12/06/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6040 -s 696
Imagebase:	0x180000
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: 3180 Parent PID: 6040

General

Start time:	15:10:41
Start date:	12/06/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6040 -s 696
Imagebase:	0x180000
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