ID: 626150
Sample Name:
Notificaci#U00f3n de pago.exe
Cookbook: default.jbs
Time: 16:43:47
Date: 13/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Copyright Joe Security LLC 2022

Copyright Joe Security LLC 2022

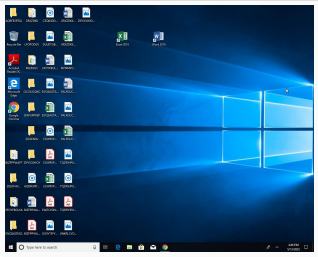
Windows Analysis Report

Notificaci#U00f3n de pago.exe

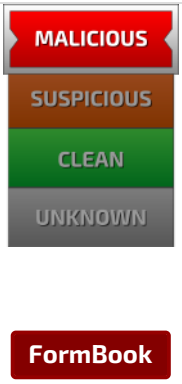
Overview

General Information

Sample Name:	Notificaci#U00f3n de pago.exe
Analysis ID:	626150
MD5:	297e8b7f26a2eb..
SHA1:	4b3e36dcd7ea97..
SHA256:	441ba10d2078c4..
Tags:	exe
Infos:	



Detection



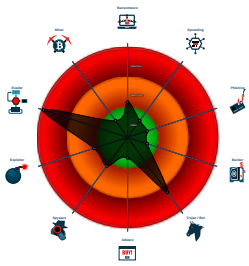
FormBook

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through…
- Yara detected AntiVM3
- System process connects to networ…
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- Self deletion via cmd delete
- .NET source code contains potentia…

Classification



Process Tree

- **System is w10x64**
- Notificaci#U00f3n de pago.exe (PID: 6360 cmdline: "C:\Users\user\Desktop\Notificaci#U00f3n de pago.exe" MD5: 297E8B7F26A2EB1AF366CAC0202ECA9A)
  - Notificaci#U00f3n de pago.exe (PID: 6968 cmdline: C:\Users\user\Desktop\Notificaci#U00f3n de pago.exe MD5: 297E8B7F26A2EB1AF366CAC0202ECA9A)
    - explorer.exe (PID: 3968 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - WWAHost.exe (PID: 6172 cmdline: C:\Windows\SysWOW64\WWAHost.exe MD5: 370C260333EB3149EF4E49C8F64652A0)
        - cmd.exe (PID: 6596 cmdline: /c del "C:\Users\user\Desktop\Notificaci#U00f3n de pago.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6568 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

Copyright Joe Security LLC 2022

```
{
  "C2 list": [
    "www.hkqhdq.com/d6fp/"
  ],
  "decoy": [
    "cwejman.art",
    "chandlerfeed.site",
    "team-ctctitleco.com",
    "yennyalfonsotorres84.com",
    "letseatdonuts.com",
    "runicarcanum.com",
    "info-center.xyz",
    "stemcanada.net",
    "granerde.com",
    "pixelatedkittys.com",
    "selfservicerepait.com",
    "lasvegastechman.com",
    "massage-rino.com",
    "bfederation.com",
    "kjy9.com",
    "homeiexpress.com",
    "hayatiorhan.com",
    "89739134.com",
    "kristin-feireiss-80.com",
    "zfp2.xyz",
    "peq2ulps.com",
    "redgreenbandits.com",
    "doblehuella.com",
    "521xiao.com",
    "freedomadventurescharters.com",
    "424259842.xyz",
    "peachfsg.com",
    "marketery.net",
    "dubhmor-dg.com",
    "sustainabilitymantra.xyz",
    "obivka.site",
    "yoursjoysled.com",
    "neurovirtualusa.com",
    "938323373.com",
    "seabornecap.com",
    "rjxingfu.com",
    "vacationsimplified.com",
    "elramony.com",
    "craftivitycrew.com",
    "cryptoheritageclub.com",
    "tcr8.fund",
    "gloumarc.com",
    "marry-me-today.com",
    "screator.life",
    "tokusou-clean.com",
    "sagesse.agency",
    "borilius.com",
    "www-saber.com",
    "bondjetfuel.com",
    "sedadbir.com",
    "interparking-60years.com",
    "mdartwork.com",
    "materialy.pro",
    "theguiriguide.com",
    "islandacoustical.com",
    "einfachmalgut.com",
    "nonstrappedmedia.club",
    "librevillegabon.com",
    "wasatchholidayclassic.net",
    "shanhaiyizhi.com",
    "triptoasiam.com",
    "s3industrail.com",
    "evertribute.com",
    "marketing-toolbox.com"
  ]
}
```


Copyright Joe Security LLC 2022

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000002.383069133.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000008.00000002.383069133.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8c08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8f92:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x16335:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15de1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x16437:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x165af:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x99aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1505c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa722:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b987:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ca8a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000008.00000002.383069133.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18809:$sqlite3step: 68 34 1C 7B E1 • 0x1891c:$sqlite3step: 68 34 1C 7B E1 • 0x18838:$sqlite3text: 68 38 2A 90 C5 • 0x1895d:$sqlite3text: 68 38 2A 90 C5 • 0x1884b:$sqlite3blob: 68 53 D8 7F 8C • 0x18973:$sqlite3blob: 68 53 D8 7F 8C
00000008.00000002.383525954.0000000001410000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000008.00000002.383525954.0000000001410000.00000040.10000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8c08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8f92:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x16335:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15de1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x16437:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x165af:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x99aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1505c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa722:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b987:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ca8a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00

Click to see the 31 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
8.0.Notificaci#U00f3n de pago.exe.400000.4.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
8.0.Notificaci#U00f3n de pago.exe.400000.4.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7e08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8192:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15535:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14fe1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15637:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x157af:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x8baa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1425c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9922:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ab87:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bc8a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
8.0.Notificaci#U00f3n de pago.exe.400000.4.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17a09:$sqlite3step: 68 34 1C 7B E1 • 0x17b1c:$sqlite3step: 68 34 1C 7B E1 • 0x17a38:$sqlite3text: 68 38 2A 90 C5 • 0x17b5d:$sqlite3text: 68 38 2A 90 C5 • 0x17a4b:$sqlite3blob: 68 53 D8 7F 8C • 0x17b73:$sqlite3blob: 68 53 D8 7F 8C
8.2.Notificaci#U00f3n de pago.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
8.2.Notificaci#U00f3n de pago.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8c08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8f92:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x16335:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15de1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x16437:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x165af:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x99aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 8 3 E3 0F C1 EA 06 • 0x1505c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa722:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b987:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ca8a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE F F FF 6A 00
Click to see the 22 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

Networking

System process connects to network (likely due to code injection or exploit)

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

.NET source code contains potential unpacker

.NET source code contains method to dynamically call methods (often used by packers)

Hooking and other Techniques for Hiding and Protection

Self deletion via cmd delete

Malware Analysis System Evasion

Yara detected AntiVM3

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

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion

System process connects to network (likely due to code injection or exploit)

Sample uses process hollowing technique

Maps a DLL or memory area into another process

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

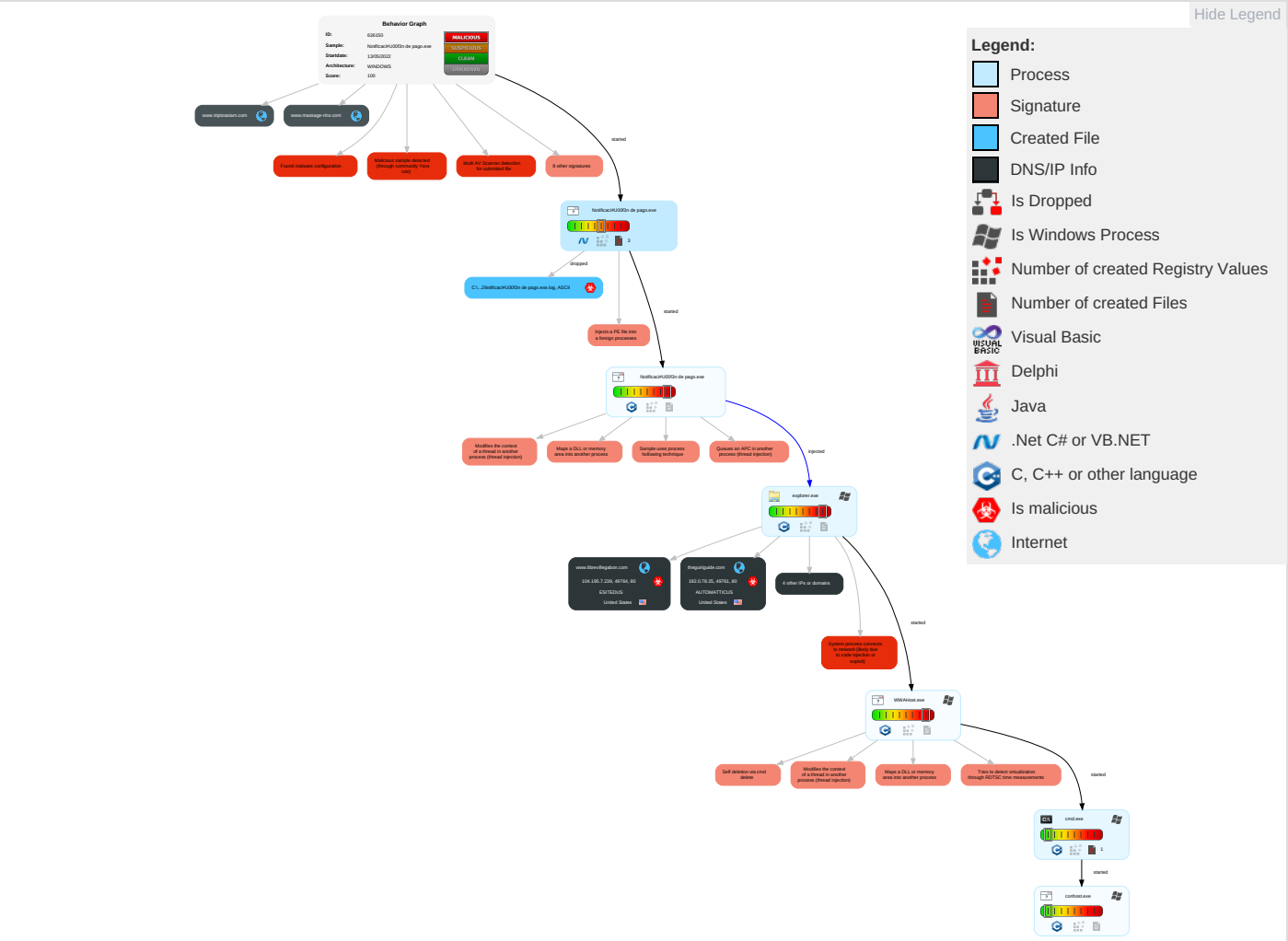
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Shared Modules	Path Interception	6 1 2 Process Injection	1 Masquerading	OS Credential Dumping	2 2 1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	3 1 Virtualization/Sandbox Evasion	Security Account Manager	3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	6 1 2 Process Injection	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 1 2 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	4 Obfuscated Files or Information	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 3 Software Packing	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 File Deletion	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

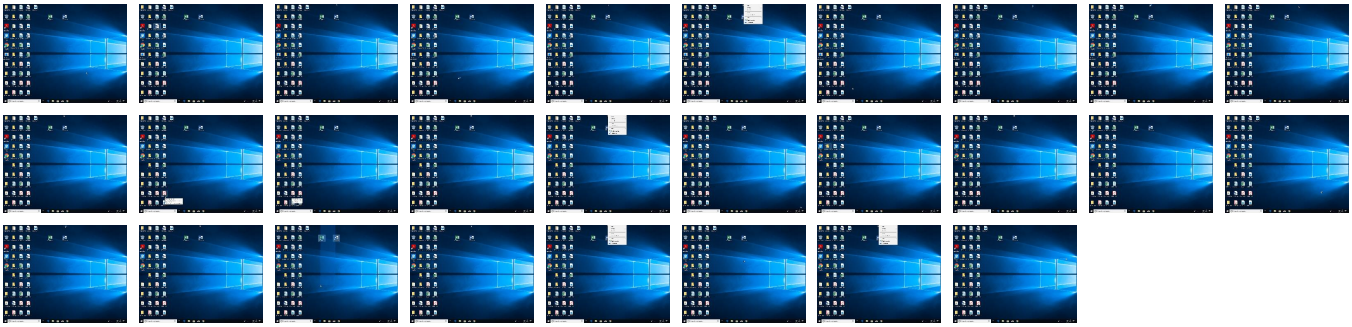
Behavior Graph



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
Notificaci#U00f3n de pago.exe	21%	Virustotal		Browse
Notificaci#U00f3n de pago.exe	41%	ReversingLabs	ByteCode-MSIL.Trojan.FormBook	
Notificaci#U00f3n de pago.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.0.Notificaci#U00f3n de pago.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
8.0.Notificaci#U00f3n de pago.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
8.0.Notificaci#U00f3n de pago.exe.400000.8.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
8.2.Notificaci#U00f3n de pago.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Copyright Joe Security LLC 2022

Domains

Source	Detection	Scanner	Label	Link
www.massage-rino.com	0%	Virustotal		Browse
theguiriguide.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.fontbureau.comlvfetDm	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.evertribute.com/d6fp/?7nxh=0IAMhpyfM6TyxYvNuQBLxFd+VBe1OVp7bFg/8SsVn3OL4Z0v7SAtnQzd8ZWN+7APMfoM&q6AlF=0txdQnwxgb	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.founder.com.cn/cnG	0%	URL Reputation	safe	
http://www.sajatypeworks.comG	0%	Avira URL Cloud	safe	
http://www.librevillegabon.com/d6fp/?7nxh=27dTALvGagYo6W4eiFO6YvZJ//Zn5pBdCa2l5DH7HNM2RGs4GWZbOB9vu5aCQaLmGkAl&q6AlF=0txdQnwxgb	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.galapagosdesign.com/n	0%	Avira URL Cloud	safe	
http://www.fontbureau.comB.TTF?m	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Y0?m	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/hm?	0%	Avira URL Cloud	safe	
http://www.fontbureau.comcom	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/6m	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sajatypeworks.come	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fontbureau.com.TTF	0%	URL Reputation	safe	
http://www.theguiriguide.com/d6fp/?7nxh=Vjw903Y9bM1AKbFW1pqe+tE50cefuwUzuT8QLR39Zk9vkX5o4NYForbp6qTr1jJAF4yG&q6AlF=0txdQnwxgb	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comt	0%	URL Reputation	safe	
http://www.sajatypeworks.comt-bh	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Zm	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.como)m	0%	Avira URL Cloud	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/)m	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
www.hkqhdq.com/d6fp/	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cnnt	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Dm	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/2	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/cm6	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/qm(	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cne-dio	0%	Avira URL Cloud	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/~mQ	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Mm	0%	Avira URL Cloud	safe	
http://www.fontbureau.comsief	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.triptoasiam.com	162.0.216.71	true	false		unknown
www.massage-rino.com	38.40.251.97	true	false	• 0%, Virustotal, Browse	unknown
theguiriguide.com	192.0.78.25	true	true	• 0%, Virustotal, Browse	unknown
parkingpage.namecheap.com	198.54.117.212	true	false		high
www.librevillegabon.com	104.195.7.239	true	true		unknown
www.theguiriguide.com	unknown	unknown	true		unknown
www.team-ctctitleco.com	unknown	unknown	true		unknown
www.evertribute.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.evertribute.com/d6fp/?7nxh=0IAMhpyfM6TyxYvNuQBLxFd+VBe1OVp7bFg/8SsVn3OL4Z0v7SAtnQzd8ZWN+7APMfoM&q6AlF=0txdQnwxgb	true	• Avira URL Cloud: safe	unknown
http://www.librevillegabon.com/d6fp/?7nxh=27dTALvGagYo6W4eiFO6YvZJ//Zn5pBdCa2l5DH7HNM2RGs4GWZbOB9vu5aCQaLmGkAl&q6AlF=0txdQnwxgb	true	• Avira URL Cloud: safe	unknown
http://www.theguiriguide.com/d6fp/?7nxh=Vjw903Y9bM1AKbFW1pqe+tE50cefuwUzuT8QLR39Zk9vkX5o4NYForbp6qTr1jJAF4yG&q6AlF=0txdQnwxgb	true	• Avira URL Cloud: safe	unknown
www.hkqhdq.com/d6fp/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	Notificaci#U00f3n de pago.exe, 00000000.00000002.313327402.0000000007222000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comlvfetDm	Notificaci#U00f3n de pago.exe, 00000000.00000003.283274028.0000000005F9A000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	Notificaci#U00f3n de pago.exe, 00000000.00000002.313327402.0000000007222000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Notificaci#U00f3n de pago.exe, 00000000.00000002.313327402.0000000007222000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.html0	Notificaci#U00f3n de pago.exe, 00000000.00000003.275317837.0000000005F97000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers?	Notificaci#U00f3n de pago.exe, 00000000.00000002.313327402.0000000007222000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.com	Notificaci#U00f3n de pago.exe, 00000000.00000002.313327402.0000000007222000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	Notificaci#U00f3n de pago.exe, 00000000.00000002.313327402.0000000007222000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	Notificaci#U00f3n de pago.exe, 00000000.00000002.313327402.0000000007222000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnG	Notificaci#U00f3n de pago.exe, 00000000.00000003.266184528.0000000005F97000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.comG	Notificaci#U00f3n de pago.exe, 00000000.00000003.267557028.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.265054289.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.267273158.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.264590356.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.264694065.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.268115380.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.267166340.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.264094876.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.266446750.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.266607005.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.265196390.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.265228038.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.264926337.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.265917644.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.264428081.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.263906770.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.264561984.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.268009733.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.264304896.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.267765595.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.267071973.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.com	Notificaci#U00f3n de pago.exe, 00000000.00000003.267557028.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.265054289.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.267273158.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.264590356.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.264694065.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.268115380.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.267166340.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.264094876.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.266446750.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.266607005.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.265196390.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.265228038.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.264926337.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.265917644.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.264428081.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.263906770.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.264561984.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.268009733.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.264304896.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.263447229.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.267765595.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	Notificaci#U00f3n de pago.exe, 00000000.00000002.313327402.0000000007222000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	Notificaci#U00f3n de pago.exe, 00000000.00000002.313327402.0000000007222000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Notificaci#U00f3n de pago.exe, 00000000.00000002.313327402.0000000007222000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	Notificaci#U00f3n de pago.exe, 00000000.00000002.313327402.0000000007222000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/n	Notificaci#U00f3n de pago.exe, 00000000.00000003.277842098.0000000005FC8000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comB.TTF?m	Notificaci#U00f3n de pago.exe, 00000000.00000003.283274028.0000000005F9A000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/Y0?m	Notificaci#U00f3n de pago.exe, 00000000.00000003.268786544.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.268937816.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/hm?	Notificaci#U00f3n de pago.exe, 00000000.00000003.268786544.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.268937816.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comcom	Notificaci#U00f3n de pago.exe, 00000000.00000003.275317837.0000000005F97000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.275623975.0000000005F98000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	Notificaci#U00f3n de pago.exe, 00000000.00000002.313327402.0000000007222000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/6m	Notificaci#U00f3n de pago.exe, 00000000.00000003.268786544.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.268937816.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/Y0	Notificaci#U00f3n de pago.exe, 00000000.00000003.268937816.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	Notificaci#U00f3n de pago.exe, 00000000.00000002.313327402.0000000007222000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	Notificaci#U00f3n de pago.exe, 00000000.00000002.313327402.0000000007222000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	Notificaci#U00f3n de pago.exe, 00000000.00000002.313327402.0000000007222000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	Notificaci#U00f3n de pago.exe, 00000000.00000002.313327402.0000000007222000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.come	Notificaci#U00f3n de pago.exe, 00000000.00000003.267557028.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.265054289.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.267273158.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.264590356.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.264694065.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.268115380.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.267166340.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.264094876.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.266446750.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.266607005.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.265196390.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.265228038.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.264926337.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.265917644.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.264428081.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.263906770.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.264561984.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.268009733.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.264304896.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.267765595.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.267071973.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	Notificaci#U00f3n de pago.exe, 00000000.00000002.313327402.0000000007222000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com.TTF	Notificaci#U00f3n de pago.exe, 00000000.00000003.275317837.0000000005F97000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.275623975.0000000005F98000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	Notificaci#U00f3n de pago.exe, 00000000.00000002.313327402.0000000007222000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	Notificaci#U00f3n de pago.exe, 00000000.00000003.275317837.0000000005F97000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.275623975.0000000005F98000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000002.313327402.0000000007222000.00000004.00000800.00020000.00000000.sdmp	false		high

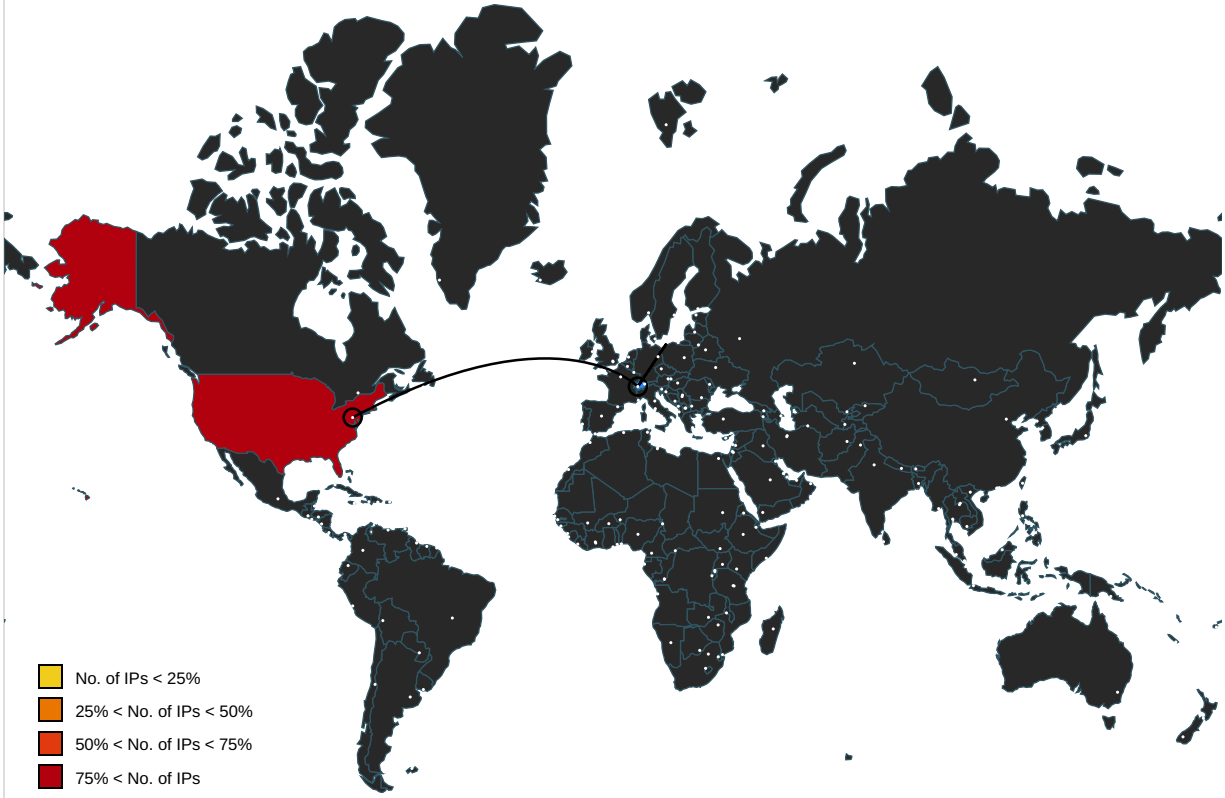
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.comt	Notificaci#U00f3n de pago.exe, 00000000.00000003.267557028.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.265054289.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.267273158.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.264590356.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.264694065.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.268115380.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.267166340.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.264094876.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.266446750.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.266607005.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.265196390.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.265228038.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.264926337.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.265917644.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.264428081.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.263906770.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.264561984.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.268009733.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.264304896.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.267765595.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.267071973.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.comt-bh	Notificaci#U00f3n de pago.exe, 00000000.00000003.267557028.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.265054289.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.267273158.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.264590356.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.264694065.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.268115380.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.267166340.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.264094876.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.266446750.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.266607005.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.265196390.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.265228038.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.264926337.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.265917644.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.264428081.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.263906770.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.264561984.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.268009733.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.264304896.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.263447229.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.267765595.0000000005FAB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/Zm	Notificaci#U00f3n de pago.exe, 00000000.00000003.268786544.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.268937816.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	Notificaci#U00f3n de pago.exe, 00000000.00000003.268786544.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.268937816.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.coma	Notificaci#U00f3n de pago.exe, 00000000.00000003.283274028.0000000005F9A000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000002.312759063.0000000005F90000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.307819527.0000000005F90000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.como)m	Notificaci#U00f3n de pago.exe, 00000000.00000003.283274028.0000000005F9A000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000002.312759063.0000005F90000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.307819527.0000000005F90000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.comd	Notificaci#U00f3n de pago.exe, 00000000.00000003.275317837.0000000005F97000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.275623975.0000005F98000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://en.w	Notificaci#U00f3n de pago.exe, 00000000.00000003.263896171.0000000005F96000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/)m	Notificaci#U00f3n de pago.exe, 00000000.00000003.268786544.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.268937816.0000005F9B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	Notificaci#U00f3n de pago.exe, 00000000.00000002.313327402.0000000007222000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Notificaci#U00f3n de pago.exe, 00000000.00000002.313327402.0000000007222000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn	Notificaci#U00f3n de pago.exe, 00000000.00000002.313327402.0000000007222000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.266184528.0000005F97000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.266049177.0000000005F98000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.265980144.0000000005F97000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	Notificaci#U00f3n de pago.exe, 00000000.00000002.313327402.0000000007222000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cnnt	Notificaci#U00f3n de pago.exe, 00000000.00000003.265980144.0000000005F97000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/Dm	Notificaci#U00f3n de pago.exe, 00000000.00000003.268786544.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.268937816.0000005F9B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/2	Notificaci#U00f3n de pago.exe, 00000000.00000003.277842098.0000000005FC8000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/cm6	Notificaci#U00f3n de pago.exe, 00000000.00000003.268786544.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.268937816.0000005F9B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/qm(	Notificaci#U00f3n de pago.exe, 00000000.00000003.268786544.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.268937816.0000005F9B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cne-dio	Notificaci#U00f3n de pago.exe, 00000000.00000003.266184528.0000000005F97000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comm	Notificaci#U00f3n de pago.exe, 00000000.00000003.275317837.0000000005F97000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.275623975.0000005F98000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	Notificaci#U00f3n de pago.exe, 00000000.00000003.268937816.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers8	Notificaci#U00f3n de pago.exe, 00000000.00000002.313327402.0000000007222000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/~mQ	Notificaci#U00f3n de pago.exe, 00000000.00000003.268786544.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.268937816.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/Mm	Notificaci#U00f3n de pago.exe, 00000000.00000003.268786544.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.268937816.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comsief	Notificaci#U00f3n de pago.exe, 00000000.00000003.275317837.0000000005F97000.00000004.00000800.00020000.00000000.sdmp, Notificaci#U00f3n de pago.exe, 00000000.00000003.275623975.0000000005F98000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.0.78.25	theguiriguide.com	United States		2635	AUTOMATTICUS	true
198.54.117.212	parkingpage.namecheap.com	United States		22612	NAMECHEAP-NETUS	false
104.195.7.239	www.librevillegabon.com	United States		22552	ESITEDUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626150
Start date and time: 13/05/202216:43:47	2022-05-13 16:43:47 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 52s

Copyright Joe Security LLC 2022

Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Notificaci#U00f3n de pago.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	24
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/1@6/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 22.1% (good quality ratio 19.8%) • Quality average: 70.8% • Quality standard deviation: 32.4%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 40.125.122.176, 52.152.110.14, 20.223.24.244, 52.242.101.226
- Excluded domains from analysis (whitelisted): fs.microsoft.com, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, store-images.s-microsoft.com, login.live.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com, displaycatalog-rp.md.mp.microsoft.com.akadns.net, glb.sls.prod.dcat.dsp.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
16:45:11	API Interceptor	1x Sleep call for process: Notificaci#U00f3n de pago.exe modified
16:47:10	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run D8ILG6RHT8 C:\Program Files (x86)\Qmx6\xhl42 jqfp00z.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Notificaci#U00f3n de pago.exe.log

Process:	C:\Users\user\Desktop\Notificaci#U00f3n de pago.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4FsXE8:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHJ
MD5:	EA78C102145ED608EF0E407B978AF339
SHA1:	66C9179ED9675B9271A97AB1FC878077E09AB731
SHA-256:	8BF01E0C445BD07C0B4EDC7199B7E17DAF1CA55CA52D4A6EAC4EF211C2B1A73E
SHA-512:	8C04139A1FC3C3BDACB680EC443615A43EB18E73B5A0CFCA644CB4A5E71746B275B3E238DD1A5A205405313E457BB75F9BBB93277C67AFA5D78DCFA30E5DA02B
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.9124952245387155
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	Notificaci#U00f3n de pago.exe
File size:	535552
MD5:	297e8b7f26a2eb1af366cac0202eca9a
SHA1:	4b3e36dcd7ea9785f93e43699e1224ad30626148
SHA256:	441ba10d2078c45be3d266523f77b59a1478f61ce09f2097ccc276d534c35855
SHA512:	bd53b63f91ecdc33e6dba2929dbe1039df08bc8a84950af9fb2b34fe803c3d61fc09c40ae8843d961e4107e6970690e2ff4d7436ff1d78b7e5aa0b4c87576942
SSDEEP:	12288:3GuFJoO8gHHV3PnS2l3wCGeoPzaHkkzXlWaVaGNtl7:rwyHHRS2tPweEkzXRVJ
TLSH:	4DB41256A267A933C14A9736CCD855CC5330CF06AC23DA4768E932CC2B73BC64E91B67
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...m.|b.....0.."..... ^A... ...`....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x48415e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x627CAF6D [Thu May 12 06:55:41 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x84110	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x86000	0x5e0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x88000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x840c3	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x82164	0x82200	False	0.939192333093	data	7.92135270708	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x86000	0x5e0	0x600	False	0.429036458333	data	4.15748129845	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x88000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x860a0	0x354	data		
RT_MANIFEST	0x863f4	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

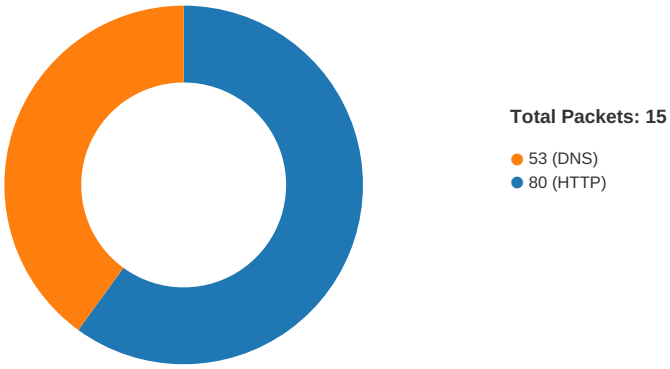
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2013
Assembly Version	0.0.1.0
InternalName	FormatExcept.exe
FileVersion	0.0.1.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	PagedOptionsDialog
ProductVersion	0.0.1.0
FileDescription	PagedOptionsDialog
OriginalFilename	FormatExcept.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2022 16:46:41.088460922 CEST	49760	80	192.168.2.3	198.54.117.212
May 13, 2022 16:46:41.261989117 CEST	80	49760	198.54.117.212	192.168.2.3
May 13, 2022 16:46:41.264811039 CEST	49760	80	192.168.2.3	198.54.117.212
May 13, 2022 16:46:41.271711111 CEST	49760	80	192.168.2.3	198.54.117.212
May 13, 2022 16:46:41.445027113 CEST	80	49760	198.54.117.212	192.168.2.3
May 13, 2022 16:46:41.445060015 CEST	80	49760	198.54.117.212	192.168.2.3
May 13, 2022 16:46:46.520431042 CEST	49761	80	192.168.2.3	192.0.78.25
May 13, 2022 16:46:46.539464951 CEST	80	49761	192.0.78.25	192.168.2.3
May 13, 2022 16:46:46.539556980 CEST	49761	80	192.168.2.3	192.0.78.25
May 13, 2022 16:46:46.539707899 CEST	49761	80	192.168.2.3	192.0.78.25
May 13, 2022 16:46:46.556318998 CEST	80	49761	192.0.78.25	192.168.2.3
May 13, 2022 16:46:46.708456039 CEST	80	49761	192.0.78.25	192.168.2.3
May 13, 2022 16:46:46.708498001 CEST	80	49761	192.0.78.25	192.168.2.3
May 13, 2022 16:46:46.708687067 CEST	49761	80	192.168.2.3	192.0.78.25
May 13, 2022 16:46:46.964236975 CEST	49761	80	192.168.2.3	192.0.78.25
May 13, 2022 16:46:46.980910063 CEST	80	49761	192.0.78.25	192.168.2.3
May 13, 2022 16:46:57.439934969 CEST	49764	80	192.168.2.3	104.195.7.239
May 13, 2022 16:46:57.627410889 CEST	80	49764	104.195.7.239	192.168.2.3
May 13, 2022 16:46:57.627687931 CEST	49764	80	192.168.2.3	104.195.7.239
May 13, 2022 16:46:57.630451918 CEST	49764	80	192.168.2.3	104.195.7.239
May 13, 2022 16:46:57.818396091 CEST	80	49764	104.195.7.239	192.168.2.3
May 13, 2022 16:46:57.818476915 CEST	80	49764	104.195.7.239	192.168.2.3
May 13, 2022 16:46:57.818505049 CEST	80	49764	104.195.7.239	192.168.2.3
May 13, 2022 16:46:57.818530083 CEST	80	49764	104.195.7.239	192.168.2.3
May 13, 2022 16:46:57.818550110 CEST	80	49764	104.195.7.239	192.168.2.3
May 13, 2022 16:46:57.818682909 CEST	49764	80	192.168.2.3	104.195.7.239
May 13, 2022 16:46:57.818797112 CEST	49764	80	192.168.2.3	104.195.7.239
May 13, 2022 16:46:58.006299973 CEST	80	49764	104.195.7.239	192.168.2.3
May 13, 2022 16:46:58.006746054 CEST	49764	80	192.168.2.3	104.195.7.239

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2022 16:46:41.058917999 CEST	53802	53	192.168.2.3	8.8.8.8
May 13, 2022 16:46:41.080055952 CEST	53	53802	8.8.8.8	192.168.2.3

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2022 16:46:46.489698887 CEST	65266	53	192.168.2.3	8.8.8.8
May 13, 2022 16:46:46.515434027 CEST	53	65266	8.8.8.8	192.168.2.3
May 13, 2022 16:46:51.974284887 CEST	63332	53	192.168.2.3	8.8.8.8
May 13, 2022 16:46:52.015516996 CEST	53	63332	8.8.8.8	192.168.2.3
May 13, 2022 16:46:57.120481968 CEST	63548	53	192.168.2.3	8.8.8.8
May 13, 2022 16:46:57.438465118 CEST	53	63548	8.8.8.8	192.168.2.3
May 13, 2022 16:47:02.828375101 CEST	49327	53	192.168.2.3	8.8.8.8
May 13, 2022 16:47:02.958780050 CEST	53	49327	8.8.8.8	192.168.2.3
May 13, 2022 16:47:10.203502893 CEST	61380	53	192.168.2.3	8.8.8.8
May 13, 2022 16:47:10.370362997 CEST	53	61380	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 13, 2022 16:46:41.058917999 CEST	192.168.2.3	8.8.8.8	0xfaa7	Standard query (0)	www.evertribute.com	A (IP address)	IN (0x0001)
May 13, 2022 16:46:46.489698887 CEST	192.168.2.3	8.8.8.8	0x7032	Standard query (0)	www.theguiriguide.com	A (IP address)	IN (0x0001)
May 13, 2022 16:46:51.974284887 CEST	192.168.2.3	8.8.8.8	0x6a9a	Standard query (0)	www.team-ctctitleco.com	A (IP address)	IN (0x0001)
May 13, 2022 16:46:57.120481968 CEST	192.168.2.3	8.8.8.8	0x1c73	Standard query (0)	www.librevillegabon.com	A (IP address)	IN (0x0001)
May 13, 2022 16:47:02.828375101 CEST	192.168.2.3	8.8.8.8	0xe13c	Standard query (0)	www.triptoasiam.com	A (IP address)	IN (0x0001)
May 13, 2022 16:47:10.203502893 CEST	192.168.2.3	8.8.8.8	0x1b3	Standard query (0)	www.massage-rino.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 13, 2022 16:46:41.080055952 CEST	8.8.8.8	192.168.2.3	0xfaa7	No error (0)	www.evertribute.com	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
May 13, 2022 16:46:41.080055952 CEST	8.8.8.8	192.168.2.3	0xfaa7	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
May 13, 2022 16:46:41.080055952 CEST	8.8.8.8	192.168.2.3	0xfaa7	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
May 13, 2022 16:46:41.080055952 CEST	8.8.8.8	192.168.2.3	0xfaa7	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
May 13, 2022 16:46:41.080055952 CEST	8.8.8.8	192.168.2.3	0xfaa7	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
May 13, 2022 16:46:41.080055952 CEST	8.8.8.8	192.168.2.3	0xfaa7	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
May 13, 2022 16:46:41.080055952 CEST	8.8.8.8	192.168.2.3	0xfaa7	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
May 13, 2022 16:46:41.080055952 CEST	8.8.8.8	192.168.2.3	0xfaa7	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
May 13, 2022 16:46:46.515434027 CEST	8.8.8.8	192.168.2.3	0x7032	No error (0)	www.theguiriguide.com	theguiriguide.com		CNAME (Canonical name)	IN (0x0001)
May 13, 2022 16:46:46.515434027 CEST	8.8.8.8	192.168.2.3	0x7032	No error (0)	theguiriguide.com		192.0.78.25	A (IP address)	IN (0x0001)
May 13, 2022 16:46:46.515434027 CEST	8.8.8.8	192.168.2.3	0x7032	No error (0)	theguiriguide.com		192.0.78.24	A (IP address)	IN (0x0001)
May 13, 2022 16:46:52.015516996 CEST	8.8.8.8	192.168.2.3	0x6a9a	Name error (3)	www.team-ctctitleco.com	none	none	A (IP address)	IN (0x0001)
May 13, 2022 16:46:57.438465118 CEST	8.8.8.8	192.168.2.3	0x1c73	No error (0)	www.librevillegabon.com		104.195.7.239	A (IP address)	IN (0x0001)
May 13, 2022 16:47:02.958780050 CEST	8.8.8.8	192.168.2.3	0xe13c	No error (0)	www.triptoasiam.com		162.0.216.71	A (IP address)	IN (0x0001)
May 13, 2022 16:47:10.370362997 CEST	8.8.8.8	192.168.2.3	0x1b3	No error (0)	www.massage-rino.com		38.40.251.97	A (IP address)	IN (0x0001)

Copyright Joe Security LLC 2022

HTTP Request Dependency Graph

- www.evertribute.com
- www.theguiriguide.com
- www.librevillegabon.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49760	198.54.117.212	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 13, 2022 16:46:41.271711111 CEST	8613	OUT	GET /d6fp/?7nxh=0lAMhpyfM6TyxYvNuQBLxFd+VBe1OVp7bFg/8SsVn3OL4Z0v7SAtnQzd8ZWN+7APMfoM&q6AlF=0txdQnwxgb HTTP/1.1 Host: www.evertribute.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49761	192.0.78.25	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 13, 2022 16:46:46.539707899 CEST	8614	OUT	GET /d6fp/?7nxh=Vjw903Y9bM1AKbFW1pqe+tE50cefuwUzuT8QLR39Zk9vkX5o4NYForbp6qTr1jJAF4yG&q6AlF=0txdQnwxgb HTTP/1.1 Host: www.theguiriguide.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 13, 2022 16:46:46.708456039 CEST	8614	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Fri, 13 May 2022 14:46:46 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://www.theguiriguide.com/d6fp/?7nxh=Vjw903Y9bM1AKbFW1pqe+tE50cefuwUzuT8QLR39Zk9vkX5o4NYForbp6qTr1jJAF4yG&q6AlF=0txdQnwxgb X-ac: 2.hhn _dfw Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx </body></html>

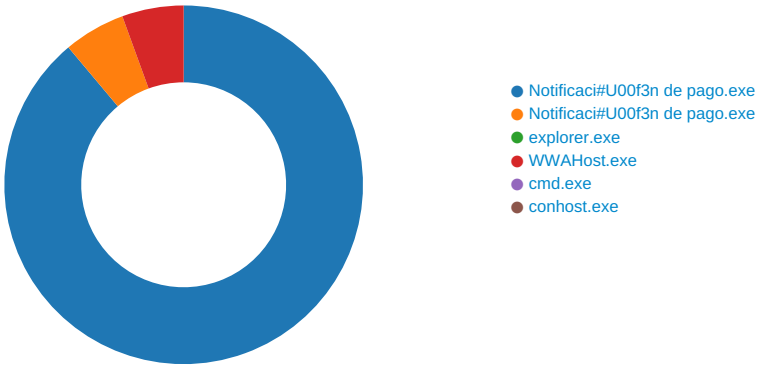
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49764	104.195.7.239	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 13, 2022 16:46:57.630451918 CEST	9314	OUT	GET /d6fp/?7nxh=27dTALvGagYo6W4eiFO6YvZJ//Zn5pBdCa2l5DH7HNM2RGs4GWZbOB9vu5aCQaLmGkAl&q6AlF=0txdQnwxgb HTTP/1.1 Host: www.librevillegabon.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 13, 2022 16:46:57.818396091 CEST	9314	IN	HTTP/1.1 200 OK Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Server: Nginx Microsoft-HTTPAPI/2.0 X-Powered-By: Nginx Date: Fri, 13 May 2022 14:46:58 GMT Connection: close Data Raw: 33 0d 0a ef bb bf 0d 0a Data Ascii: 3

Statistics

Behavior



System Behavior

Analysis Process: Notificaci#U00f3n de pago.exe PID: **6360**, Parent PID: **4108**

General

Target ID:	0
Start time:	16:44:56
Start date:	13/05/2022
Path:	C:\Users\user\Desktop\Notificaci#U00f3n de pago.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Notificaci#U00f3n de pago.exe"
Imagebase:	0xb90000
File size:	535552 bytes
MD5 hash:	297E8B7F26A2EB1AF366CAC0202ECA9A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.310859380.0000000003FFB000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.310859380.0000000003FFB000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.310859380.0000000003FFB000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.310331717.0000000002FB8000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.310059804.0000000002F31000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security

Reputation:	low

File Activities

Analysis Process: Notificaci#U00f3n de pago.exe PID: 6968, Parent PID: 6360

General

Target ID:	8
Start time:	16:45:17
Start date:	13/05/2022
Path:	C:\Users\user\Desktop\Notificaci#U00f3n de pago.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Notificaci#U00f3n de pago.exe
Imagebase:	0xe10000
File size:	535552 bytes
MD5 hash:	297E8B7F26A2EB1AF366CAC0202ECA9A
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: 00000008.00000002.383069133.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.383069133.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.383069133.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.383525954.0000000001410000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.383525954.0000000001410000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.383525954.0000000001410000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.383574580.0000000001440000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.383574580.0000000001440000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.383574580.0000000001440000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000000.306288871.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000000.306288871.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000000.306288871.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000000.305178001.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000000.305178001.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000000.305178001.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	41A407	NtReadFile

Analysis Process: explorer.exe PID: 3968, Parent PID: 6968

General

Target ID:	11
Start time:	16:45:22
Start date:	13/05/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6b8cf0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000000.366275281.0000000007136000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000000.366275281.0000000007136000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000000.366275281.0000000007136000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000000.349080967.0000000007136000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000000.349080967.0000000007136000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000000.349080967.0000000007136000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: WWAHost.exe PID: **6172**, Parent PID: **3968**

General

Target ID:	14
Start time:	16:45:52
Start date:	13/05/2022
Path:	C:\Windows\SysWOW64\WWAHost.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WWAHost.exe
Imagebase:	0x1120000
File size:	829856 bytes
MD5 hash:	370C260333EB3149EF4E49C8F64652A0
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.537261435.0000000003680000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.537261435.0000000003680000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.537261435.0000000003680000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.524275171.0000000000A60000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.524275171.0000000000A60000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.524275171.0000000000A60000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.529657171.0000000000FA0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.529657171.0000000000FA0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.529657171.0000000000FA0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	A7A407	NtReadFile

Analysis Process: cmd.exe PID: **6596**, Parent PID: **6172**

General

Target ID:	15
Start time:	16:45:57
Start date:	13/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\Desktop\Notificaci#U00f3n de pago.exe"
Imagebase:	0xc20000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **6568**, Parent PID: **6596**

General

Target ID:	16
Start time:	16:45:58
Start date:	13/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly