ID: 383936
Sample Name: RCS76393.exe
Cookbook: default.jbs
Time: 12:45:00
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

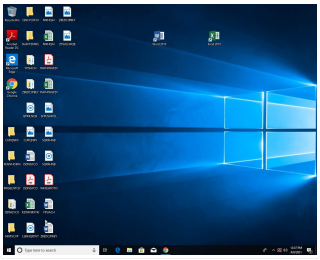
Analysis Report RCS76393.exe

Overview

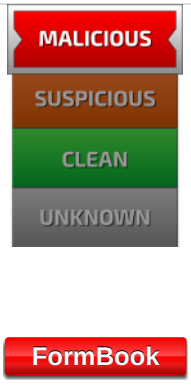
General Information

Sample Name:	RCS76393.exe
Analysis ID:	383936
MD5:	1ab1c3129fa0764.
SHA1:	ee8cd1946b5839..
SHA256:	5d1870672eff4e2..
Tags:	Formbook
Infos:	

Most interesting Screenshot:



Detection

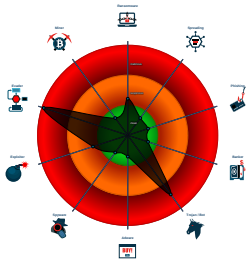


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Detected unpacking (changes PE se…
- Found malware configuration
- Malicious sample detected (through …
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Performs DNS queries to domains w…
- Queues an APC in another process …
- Sample uses process hollowing tech…

Classification



Startup

- **System is w10x64**
- RCS76393.exe (PID: 6500 cmdline: 'C:\Users\user\Desktop\RCS76393.exe' MD5: 1AB1C3129FA0764EA0702DA70F3EF569)
  - RCS76393.exe (PID: 6544 cmdline: 'C:\Users\user\Desktop\RCS76393.exe' MD5: 1AB1C3129FA0764EA0702DA70F3EF569)
    - explorer.exe (PID: 3440 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - msiexec.exe (PID: 6760 cmdline: C:\Windows\SysWOW64\msiexec.exe MD5: 12C17B5A5C2A7B97342C362CA467E9A2)
        - cmd.exe (PID: 6848 cmdline: /c del 'C:\Users\user\Desktop\RCS76393.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6864 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.batiktintaemas.com/goei/"
  ],
  "decoy": [
    "bet365o2.com",
    "gulf-landlord.info",
    "foodsystemsjusticeproject.com",
    "ronwongart.com",
    "fwgkdhg.icu",
    "armanrugservice.com",
    "mapadequito.com",
    "vbkulkarni.com",
    "ltsbinge.com",
    "creativem2.com",
    "mindflexlab.com",
    "ushealthvisa.com",
    "247carkeyslondon.com",
    "addthat.xyz",
    "zanzan8.com",
    "legendsalliance.net",
    "shopflyonline.com",
    "csgo-roll.net",
    "reutbergcapital.com",
    "mediaworkhouse.com",
    "office-tourism-tirana.com",
    "evecrude.xyz",
    "sportwillwin.com",
    "cluskmusk.com",
    "her2mymeme.com",
    "rsw3313.com",
    "digitalmarketingmoves.com",
    "seaworldminecraft.com",
    "onlinecollegetherapy.com",
    "ourmonaca.com",
    "generalflix.com",
    "limonproduce.com",
    "casalomasymphonyorchestra.com",
    "karyapertama.com",
    "massaponaxhighschool.com",
    "covidtracksb.com",
    "breathharbour.net",
    "italianrealestateagents.com",
    "xn--ga-c9a.com",
    "libreo.club",
    "leverhump.store",
    "kevinrsamuels.network",
    "pimpmyrecipe.com",
    "win-back.online",
    "kelasipo.com",
    "caross-china.com",
    "ly-iot.com",
    "nolimitsynthetics.net",
    "epicfriend.club",
    "19come.com",
    "lcjzjt.com",
    "lxpvccard.com",
    "distributorfocuson.com",
    "looneytunesrun.com",
    "mariebiernacki.com",
    "maquinaclub.com",
    "randalldavisauthor.com",
    "niggeruprising.com",
    "theexpatweightcoach.com",
    "mex33.info",
    "imbravura.com",
    "baldosasanjose.com",
    "akindousa.com",
    "ourmunera.net"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000001.324919242.0000000000400000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000003.00000001.324919242.0000000000400000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000003.00000001.324919242.0000000000400000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166b9:$sqlite3step: 68 34 1C 7B E1 • 0x167cc:$sqlite3step: 68 34 1C 7B E1 • 0x166e8:$sqlite3text: 68 38 2A 90 C5 • 0x1680d:$sqlite3text: 68 38 2A 90 C5 • 0x166fb:$sqlite3blob: 68 53 D8 7F 8C • 0x16823:$sqlite3blob: 68 53 D8 7F 8C
00000007.00000002.587150105.0000000000480000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000007.00000002.587150105.0000000000480000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 19 entries				

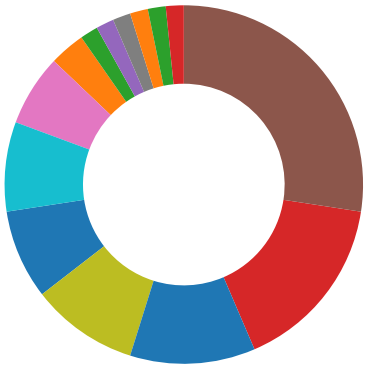
Unpacked PEs

Source	Rule	Description	Author	Strings
3.1.RCS76393.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.1.RCS76393.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13895:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13381:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13997:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b0f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x859a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9312:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18987:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
3.1.RCS76393.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x158b9:$sqlite3step: 68 34 1C 7B E1 • 0x159cc:$sqlite3step: 68 34 1C 7B E1 • 0x158e8:$sqlite3text: 68 38 2A 90 C5 • 0x15a0d:$sqlite3text: 68 38 2A 90 C5 • 0x158fb:$sqlite3blob: 68 53 D8 7F 8C • 0x15a23:$sqlite3blob: 68 53 D8 7F 8C
3.2.RCS76393.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.2.RCS76393.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13895:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13381:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13997:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b0f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x859a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9312:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18987:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 7 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Found malware configuration

Yara detected FormBook

Machine Learning detection for sample

Networking:

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

C2 URLs / IPs found in malware configuration

Performs DNS queries to domains with low reputation

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

Detected unpacking (changes PE section rights)

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

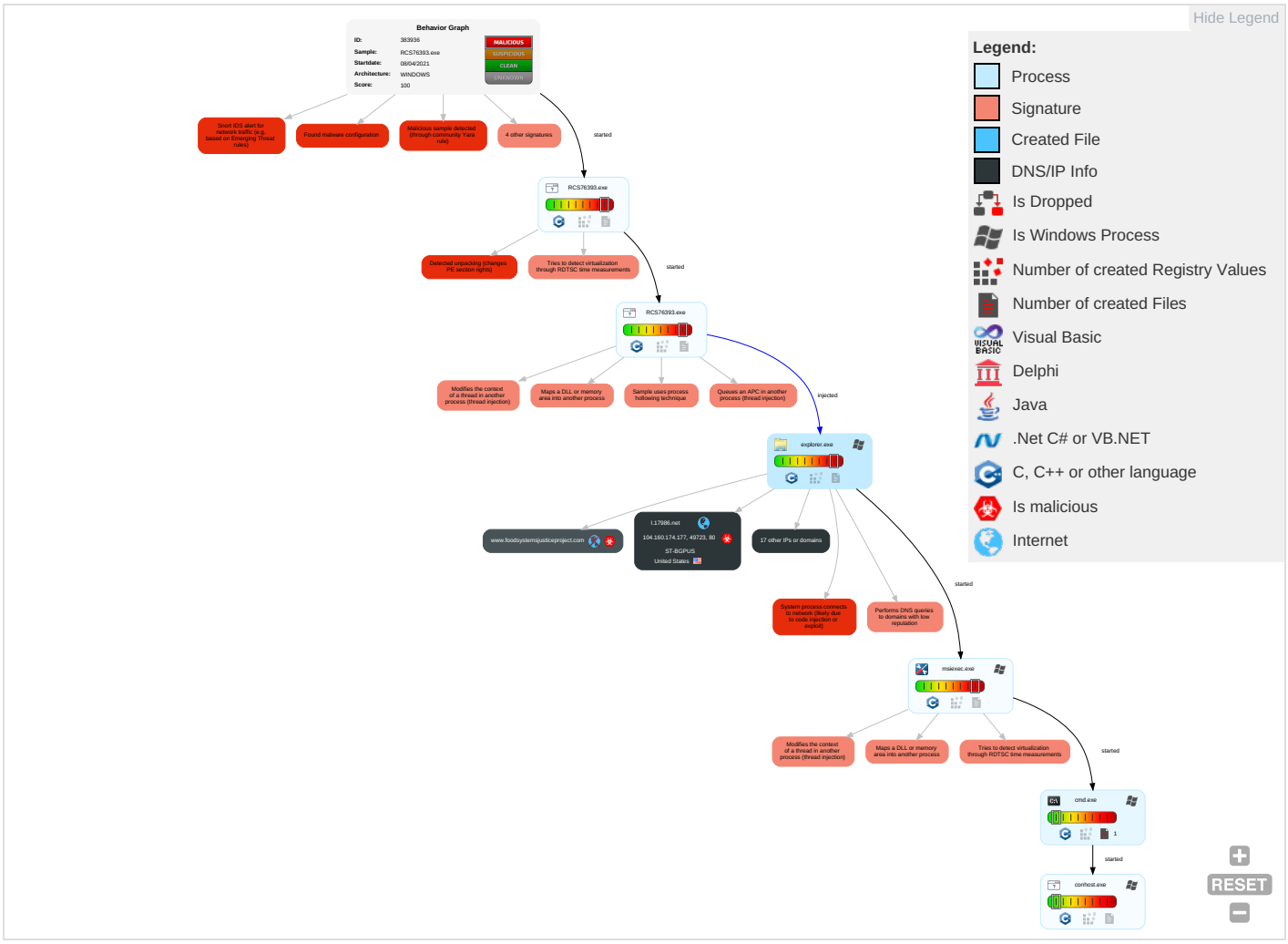
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Shared Modules 1	DLL Side-Loading 1	Process Injection 5 1 2	Virtualization/Sandbox Evasion 2	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatic
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Process Injection 5 1 2	LSASS Memory	Security Software Discovery 1 2 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 to Redirect Phor Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	Security Account Manager	Virtualization/Sandbox Evasion 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 4	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 3	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	System Information Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

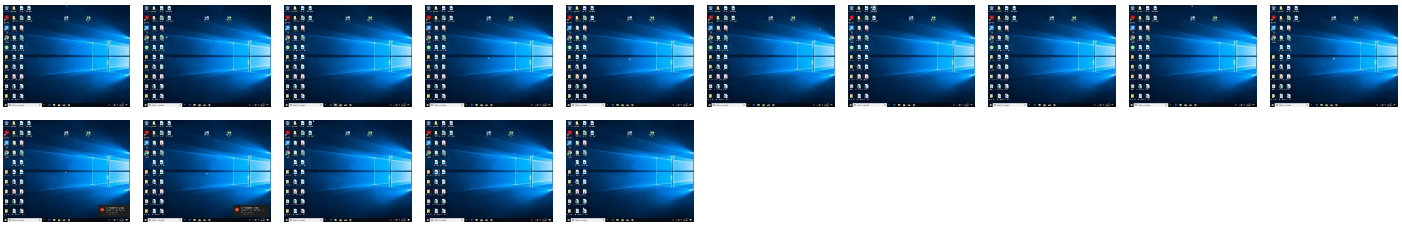
Behavior Graph



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
RCS76393.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.1.RCS76393.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
7.2.msiexec.exe.4be7960.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.RCS76393.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
www.batiktintaemas.com/goei/	100%	Avira URL Cloud	malware	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
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	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.addthat.xyz	199.59.242.153	true	true		unknown
l.17986.net	104.160.174.177	true	true		unknown
batiktintaemas.com	193.168.194.206	true	true		unknown
www.ronwongart.com	104.161.84.100	true	true		unknown
ext-cust.squarespace.com	198.185.159.144	true	false		high
generalflix.com	94.46.9.37	true	true		unknown
natroredirect.natrocdn.com	85.159.66.93	true	true		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
foodsystemsjusticeproject.com	34.102.136.180	true	false		unknown
www.foodsystemsjusticeproject.com	unknown	unknown	true		unknown
www.batiktintaemas.com	unknown	unknown	true		unknown
www.libreo.club	unknown	unknown	true		unknown
www.breathharbour.net	unknown	unknown	true		unknown
www.generalflix.com	unknown	unknown	true		unknown
www.vbkulkarni.com	unknown	unknown	true		unknown
www.pimpmyrecipe.com	unknown	unknown	true		unknown
www.csgo-roll.net	unknown	unknown	true		unknown
www.evecrude.xyz	unknown	unknown	true		unknown
www.ly-iot.com	unknown	unknown	true		unknown

Contacted URLs

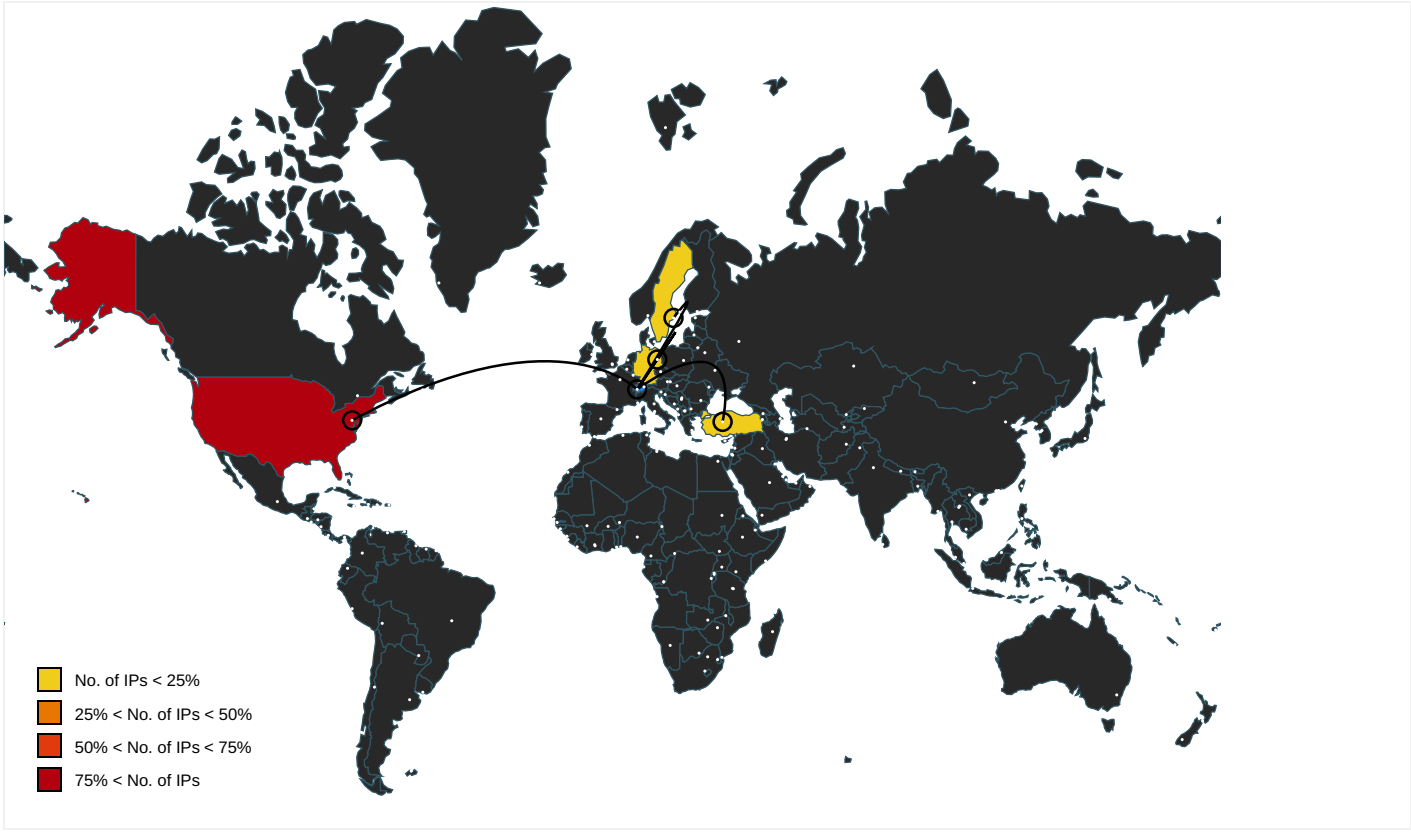
Name	Malicious	Antivirus Detection	Reputation
www.batiktintaemas.com/goei/	true	• Avira URL Cloud: malware	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000005.0000000 0.329599785.000000000095C000.0 0000004.00000020.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000005.0000000 0.347164157.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000005.0000000 0.347164157.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000005.0000000 0.347164157.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000005.0000000 0.347164157.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000005.0000000 0.347164157.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000005.0000000 0.347164157.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000005.0000000 0.347164157.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000005.0000000 0.347164157.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000005.0000000 0.347164157.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	explorer.exe, 00000005.0000000 0.347164157.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000005.0000000 0.347164157.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000005.0000000 0.347164157.000000000B1A6000.0 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 0.347164157.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000005.0000000 0.347164157.000000000B1A6000.0 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 0.347164157.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000005.0000000 0.347164157.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000005.0000000 0.347164157.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 00000005.0000000 0.347164157.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000005.0000000 0.347164157.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000005.0000000 0.347164157.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000005.0000000 0.347164157.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.fonts.com	explorer.exe, 00000005.0000000 0.347164157.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000005.0000000 0.347164157.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000005.0000000 0.347164157.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000005.0000000 0.347164157.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	explorer.exe, 00000005.0000000 0.347164157.000000000B1A6000.0 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
104.161.84.100	www.ronwongart.com	United States		53755	IOFLOODUS	true
94.46.9.37	generalflix.com	Sweden		200719	MISSDOMAINSE	true
199.59.242.153	www.addthat.xyz	United States		395082	BODIS-NJUS	true
198.185.159.144	ext-cust.squarespace.com	United States		53831	SQUARESPACEUS	false
34.102.136.180	foodsystemsjusticeproject.com	United States		15169	GOOGLEUS	false
193.168.194.206	batiktintaemas.com	Germany		47583	AS-HOSTINGERLT	true
85.159.66.93	natroredirect.natrocdn.com	Turkey		34619	CIZGITR	true
104.160.174.177	l.17986.net	United States		46844	ST-BGPUS	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383936
Start date:	08.04.2021
Start time:	12:45:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 18s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	RCS76393.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:	26
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@7/0@12/8
EGA Information:	Failed
HDC Information:	• Successful, ratio: 30.7% (good quality ratio 27.9%) • Quality average: 71.8% • Quality standard deviation: 31.6%
HCA Information:	• Successful, ratio: 94% • 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): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 20.82.210.154, 13.64.90.137, 204.79.197.200, 13.107.21.200, 23.54.113.53, 40.88.32.150, 104.43.139.144, 52.255.188.83, 20.50.102.62, 23.10.249.43, 23.10.249.26, 23.0.174.200, 23.0.174.185, 52.155.217.156, 20.54.26.129, 95.100.54.203 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, consumerrp-displaycatalog-aks2eap.md.mp.microsoft.com.akadns.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, dual-a-0001.a-msedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • VT rate limit hit for: /opt/package/joesandbox/database/analysis/383936/sample/RCS76393.exe

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
94.46.9.37	46578-TR.exe	Get hash	malicious	Browse	• www.generalflix.com/goei/?jBZx=D8b4q&kfOdRJ=J0lLVS/Rsi+YHyEfH1lEi6uDJp6jlcrDbJWYwp45E+lX6ClWTYpIvdMi/PcVRsXJUcC9
199.59.242.153	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=7CjyIVchQZXwoSp1jc0tC17NVLbOMIIdjZIIPcHCPGe34LEeqGe9fWkqZA8O62TU4Lu3&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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Order.exe	Get hash	malicious	Browse	• www.getbacklink.net/cugi/?BlL=15D5Rlw69THVEJtjRVEnjixvCWz0IM/dTd5neGnMhVDDO36KfpjGt1+SA4NLCUy6JvG/&EZXpx6=tXExBh8PdJwpH
	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=iL30VIAxs&8pntMJ6P=IosHUe5U7sgPlvQ08qcmYS3dN02u+cj8WLYYiVwUOXtKG3qUsmBBVHLqlghXUv6T7qPq
	onbgX3WswF.exe	Get hash	malicious	Browse	• www.sgdivergence.com/c22b/?w6=cbaAnqZg13PDvDAp4rbrvZjl753VAJ/hVAzUOls5TeU5Jx4pkABxsKYQ72QgGrkYw3xe&1b=W6O4DXSP5

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ARBmDNJS7m.exe	Get hash	malicious	Browse	• www.bootstrapexpress.com/aqu2/?rPj0Qr6=nYriP3GcRBwukkcsj3Cw6qOI4UbADI9fnlgfdFCApi4mXX+dpAaC8djN6XYIns7fxRpg&tXrx=gdkpfvSpm
	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+olXeWq&llsp=gTULpTwpERQd0J
	9tRIEZUd1j.exe	Get hash	malicious	Browse	• www.bootstrapexpress.com/aqu2/?5j=nYriP3GcRBwukkcsj3Cw6qOI4UbADI9fnlgfdFCApi4mXX+dpAaC8djN6XYi4cLf1Thg&_P=2dhtaH9

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
l.17986.net	Spare Parts Request MV Accord 8.13.20_pdf.exe	Get hash	malicious	Browse	• 64.32.28.253
natroredirect.natrocdn.com	newordermx.exe	Get hash	malicious	Browse	• 85.159.66.93
	Swift001_jpg.exe	Get hash	malicious	Browse	• 85.159.66.93
	t3R3C0QGKU.exe	Get hash	malicious	Browse	• 85.159.66.93
	PO_210301.exe.exe	Get hash	malicious	Browse	• 85.159.66.93
	PO_210224.exe	Get hash	malicious	Browse	• 85.159.66.93
	VESSEL SPECIFICATION 2021.exe	Get hash	malicious	Browse	• 85.159.66.93
	SAMSUNG C&T UPCOMING PROJECTS19-027-MP-0 10203.exe.exe	Get hash	malicious	Browse	• 85.159.66.93
	Y75vU558UfuGbzM.exe	Get hash	malicious	Browse	• 85.159.66.93
	Doc_74657456348374.xlsx.exe	Get hash	malicious	Browse	• 85.159.66.93
	REQUEST FOR QUOTATION.exe	Get hash	malicious	Browse	• 85.159.66.93
	D0ck7nuQyqLXPRQ.exe	Get hash	malicious	Browse	• 85.159.66.93
	RFQ.exe	Get hash	malicious	Browse	• 85.159.66.93
	bz3xMPgqmD5nAxW.exe	Get hash	malicious	Browse	• 85.159.66.93
	kaExkIZiT6.exe	Get hash	malicious	Browse	• 85.159.66.93
ext-cust.squarespace.com	PO4308.exe	Get hash	malicious	Browse	• 198.185.15 9.144
	PO#41000055885.exe	Get hash	malicious	Browse	• 198.49.23.144
	SHIPPING DOCUMENTS.exe	Get hash	malicious	Browse	• 198.185.15 9.144
	invoice bank.xlsx	Get hash	malicious	Browse	• 198.185.15 9.144
	Y79FTQtEqG.exe	Get hash	malicious	Browse	• 198.185.15 9.144
	UAE MINISTRY OF HEALTH MEDICAL EQUIPMENT SUPPLY TENDER.exe	Get hash	malicious	Browse	• 198.49.23.144
	Scan copy 24032021_jpeg.exe	Get hash	malicious	Browse	• 198.185.15 9.144
	PO032321.exe	Get hash	malicious	Browse	• 198.185.15 9.144
	Copia De Pago_pdf.exe	Get hash	malicious	Browse	• 198.49.23.145
	V90Y4n0acH.exe	Get hash	malicious	Browse	• 198.185.15 9.145
	Dgm2Yseey2.exe	Get hash	malicious	Browse	• 198.185.15 9.144
	winlog.exe	Get hash	malicious	Browse	• 198.185.15 9.144
	payment slip_pdf.exe	Get hash	malicious	Browse	• 198.185.15 9.144
	wFzMy6hehS.exe	Get hash	malicious	Browse	• 198.49.23.145
	INCHAP_Invoice_21.xlsx	Get hash	malicious	Browse	• 198.49.23.145
	ffOWE185KP.exe	Get hash	malicious	Browse	• 198.49.23.145
	q9xB9DE3RA.exe	Get hash	malicious	Browse	• 198.49.23.144
	NdxPGuzTB9.exe	Get hash	malicious	Browse	• 198.185.15 9.145
	pfjgWtj6ms.exe	Get hash	malicious	Browse	• 198.49.23.144
	Order 8953-PDF.exe	Get hash	malicious	Browse	• 198.49.23.144

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
IOFLOODUS	Betaling_advies.exe	Get hash	malicious	Browse	• 107.178.109.19
	Statement of Account.xlsx	Get hash	malicious	Browse	• 23.226.65.187
	Invoice.xlsx	Get hash	malicious	Browse	• 23.226.65.187
	MACHINE SPECIFICATION.exe	Get hash	malicious	Browse	• 104.161.56.143
	New Order.xlsx	Get hash	malicious	Browse	• 104.161.29.174
	AAXIFJn78w.exe	Get hash	malicious	Browse	• 23.226.65.187
	Debt-Details-1078370504-03052021.xls	Get hash	malicious	Browse	• 107.178.10 1.181
	Debt-Details-1078370504-03052021.xls	Get hash	malicious	Browse	• 107.178.10 1.181
	6a0000.exe	Get hash	malicious	Browse	• 162.213.211.87
	Payment.xlsx	Get hash	malicious	Browse	• 104.161.84.118
	Scan #84462.xlsm	Get hash	malicious	Browse	• 107.178.10 1.185

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	9VZe9OnL4V.exe	Get hash	malicious	Browse	• 104.161.84.118
	PO 9494843.xlsx	Get hash	malicious	Browse	• 104.161.84.118
	shipment document pdf.exe	Get hash	malicious	Browse	• 23.226.65.211
	Swift_Payment_jpeg.exe	Get hash	malicious	Browse	• 107.189.162.104
	ORDER pdf.exe	Get hash	malicious	Browse	• 23.226.65.211
	Detailed #460988.xlsm	Get hash	malicious	Browse	• 107.178.101.250
	Detailed #460988.xlsm	Get hash	malicious	Browse	• 107.178.101.250
	Detailed #460988.xlsm	Get hash	malicious	Browse	• 107.178.101.250
	Invoice pdf.exe	Get hash	malicious	Browse	• 23.226.65.211
MISSDOMAINSE	46578-TR.exe	Get hash	malicious	Browse	• 94.46.9.37
	MV Sky Marine.xlsx	Get hash	malicious	Browse	• 94.46.58.25
	4TYyYEdhtj.exe	Get hash	malicious	Browse	• 94.46.58.25
	MV Sky Marine_pdf.exe	Get hash	malicious	Browse	• 94.46.58.25
	z2xQEFs54b.exe	Get hash	malicious	Browse	• 185.76.64.223
	3yhnaDfaxn.exe	Get hash	malicious	Browse	• 185.76.64.223
BODIS-NJUS	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
	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
	9tRIEZUd1j.exe	Get hash	malicious	Browse	• 199.59.242.153

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.958502033101644

General

TrID:	• Win32 Executable (generic) a (10002005/4) 99.94% • Clipper DOS Executable (2020/12) 0.02% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • VXD Driver (31/22) 0.00%
File name:	RCS76393.exe
File size:	386560
MD5:	1ab1c3129fa0764ea0702da70f3ef569
SHA1:	ee8cd1946b58390f4599056df1472d01cf85a543
SHA256:	5d1870672eff4e2ec6d699d654d5268051f7a56f8ca991fefa538eeef380a89c
SHA512:	58bb904dc8d4435e232936f2972037dbf8b214559d0156d5d5275fdc3547a25e7ce92910459cd7f5c737641df74078e7060f0825df79b99203c2fb5033a0501c
SSDEEP:	6144:jK3TcyLImYxn3QDQEachg1e4VqOWB4hqynGEpNA:jK3Td093QDQEachGeZ8Gs2
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... ....PE..L..."Z.^.....

File Icon

Icon Hash:	8692f0c4c4ccb2ce

Static PE Info

General

Entrypoint:	0x4041a3
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x5EE25A22 [Thu Jun 11 16:21:54 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	9c90aa63bb435d1aab6db36d5bf4ee01

Entrypoint Preview

Instruction
call 00007F1EB8BC4ECDh
jmp 00007F1EB8BBD9BEh
int3
int3
int3
mov ecx, dword ptr [esp+04h]
test ecx, 00000003h
je 00007F1EB8BBDB66h
mov al, byte ptr [ecx]
add ecx, 01h
test al, al
je 00007F1EB8BBDB90h
test ecx, 00000003h
jne 00007F1EB8BBDB31h
add eax, 00000000h

Instruction
lea esp, dword ptr [esp+00000000h]
lea esp, dword ptr [esp+00000000h]
mov eax, dword ptr [ecx]
mov edx, 7EFEFEFFh
add edx, eax
xor eax, FFFFFFFFh
xor eax, edx
add ecx, 04h
test eax, 81010100h
je 00007F1EB8BBDB2Ah
mov eax, dword ptr [ecx-04h]
test al, al
je 00007F1EB8BBDB74h
test ah, ah
je 00007F1EB8BBDB66h
test eax, 00FF0000h
je 00007F1EB8BBDB55h
test eax, FF000000h
je 00007F1EB8BBDB44h
jmp 00007F1EB8BBDB0Fh
lea eax, dword ptr [ecx-01h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-02h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-03h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-04h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
mov edi, edi
push ebp
mov ebp, esp
sub esp, 20h
mov eax, dword ptr [ebp+08h]
push esi
push edi
push 00000008h
pop ecx
mov esi, 03DAD300h
lea edi, dword ptr [ebp-20h]
rep movsd
mov dword ptr [ebp-08h], eax
mov eax, dword ptr [ebp+0Ch]
pop edi
mov dword ptr [ebp-04h], eax
pop esi
test eax, eax
je 00007F1EB8BBDB4Eh
test byte ptr [eax], 00000008h
je 00007F1EB8BBDB49h
mov dword ptr [ebp+00h], 00000000h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x39b18a0	0x67	.new
IMAGE_DIRECTORY_ENTRY_IMPORT	0x39b0d84	0x3c	.new

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x39b2000	0x2ca0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x39b5000	0x1a9c	.reloc
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	0x39afa58	0x40	.new
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x39ad000	0x1e8	.new
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	0x4ab43	0x4ac00	False	0.740110263378	data	7.49545295007	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x4c000	0x395d288	0x1c00	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.jidiy	0x39aa000	0x1	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.wahe	0x39ab000	0x1179	0x400	False	0.0166015625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.new	0x39ad000	0x4907	0x4a00	False	0.372096706081	data	5.4613035653	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x39b2000	0x2ca0	0x2e00	False	0.558848505435	data	5.00204478072	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x39b5000	0x9918	0x9a00	False	0.146027800325	data	1.75035156037	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0x39b3498	0x134	data		
RT_ICON	0x39b23a0	0x10a8	data		
RT_STRING	0x39b37b8	0x148	data		
RT_STRING	0x39b3900	0x304	data		
RT_STRING	0x39b3c08	0x510	data		
RT_STRING	0x39b4118	0x502	data		
RT_STRING	0x39b4620	0x424	data		
RT_STRING	0x39b4a48	0xe6	data		
RT_STRING	0x39b4b30	0x16e	data		
RT_ACCELERATOR	0x39b3460	0x18	data		
RT_GROUP_CURSOR	0x39b35d0	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_ICON	0x39b3448	0x14	data		
RT_VERSION	0x39b35e8	0x1d0	data		
None	0x39b3478	0xa	data		
None	0x39b3488	0xa	data		

Imports

DLL	Import

DLL	Import
KERNEL32.dll	HeapReAlloc, RemoveVectoredExceptionHandler, EnumDateFormatsExW, FindResourceExW, WriteConsoleOutputCharacterA, LoadResource, SetWaitableTimer, GetCurrentProcess, HeapFree, GetModuleHandleExW, GlobalLock, CancelWaitableTimer, LockFile, SetTapeParameters, GetModuleHandleW, EnumCalendarInfoExW, TzSpecificLocalTimeToSystemTime, GetLocaleInfoW, GetSystemTimeAdjustment, InterlockedPopEntrySList, GetFileAttributesA, GetCompressedFileSizeA, GetTimeZoneInformation, GetEnvironmentVariableA, DisconnectNamedPipe, VirtualUnlock, GetConsoleAliasesW, GetProcAddress, GetAtomNameA, LocalAlloc, AddAtomA, GlobalFindAtomW, GlobalUnWire, lstrcatW, FatalExit, GetFileTime, GetConsoleCursorInfo, LocalFree, LCMapStringW, SetEnvironmentVariableA, CompareStringW, TerminateProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, GetStartupInfoW, RaiseException, RtlUnwind, HeapAlloc, GetLastError, EnterCriticalSection, LeaveCriticalSection, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, InterlockedIncrement, SetLastError, GetCurrentThreadId, InterlockedDecrement, GetCurrentThread, Sleep, ExitProcess, WriteFile, GetStdHandle, GetModuleFileNameA, GetModuleFileNameW, FreeEnvironmentStringsW, GetEnvironmentStringsW, GetCommandLineW, SetHandleCount, GetFileType, GetStartupInfoA, DeleteCriticalSection, HeapCreate, HeapDestroy, VirtualFree, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, SetFilePointer, WideCharToMultiByte, GetConsoleCP, GetConsoleMode, GetCPInfo, GetACP, GetOEMCP, IsValidCodePage, FatalAppExitA, VirtualAlloc, MultiByteToWideChar, CloseHandle, CreateFileA, InitializeCriticalSectionAndSpinCount, HeapSize, SetConsoleCtrlHandler, FreeLibrary, InterlockedExchange, LoadLibraryA, SetStdHandle, WriteConsoleA, GetConsoleOutputCP, WriteConsoleW, LCMapStringA, GetStringTypeA, GetStringTypeW, GetTimeFormatA, GetDateFormatA, GetUserDefaultLCID, GetLocaleInfoA, EnumSystemLocalesA, IsValidLocale, FlushFileBuffers, ReadFile, SetEndOfFile, GetProcessHeap, CompareStringA, GetModuleHandleA
USER32.dll	GetProcessDefaultLayout

Exports

Name	Ordinal	Address
Lolipops	1	0x4448a0
NoMore	2	0x444880
Robin	3	0x444890

Version Infos

Description	Data
InternalName	calimatimodunads.exe
FileVersions	7.0.2.54
LegalCopyrights	Vsekda
ProductVersions	7.0.21.45
Translation	0x0129 0x062b

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/08/21-12:46:58.836959	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49741	80	192.168.2.6	198.185.159.144
04/08/21-12:46:58.836959	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49741	80	192.168.2.6	198.185.159.144
04/08/21-12:46:58.836959	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49741	80	192.168.2.6	198.185.159.144
04/08/21-12:47:09.209527	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49742	34.102.136.180	192.168.2.6

Network Port Distribution

Total Packets: 95

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:46:38.828039885 CEST	49723	80	192.168.2.6	104.160.174.177
Apr 8, 2021 12:46:41.838196039 CEST	49723	80	192.168.2.6	104.160.174.177
Apr 8, 2021 12:46:42.010420084 CEST	80	49723	104.160.174.177	192.168.2.6
Apr 8, 2021 12:46:42.011430979 CEST	49723	80	192.168.2.6	104.160.174.177
Apr 8, 2021 12:46:42.498070002 CEST	49723	80	192.168.2.6	104.160.174.177
Apr 8, 2021 12:46:42.671731949 CEST	80	49723	104.160.174.177	192.168.2.6
Apr 8, 2021 12:46:43.010082960 CEST	49723	80	192.168.2.6	104.160.174.177
Apr 8, 2021 12:46:43.221426964 CEST	80	49723	104.160.174.177	192.168.2.6
Apr 8, 2021 12:46:43.287656069 CEST	80	49723	104.160.174.177	192.168.2.6
Apr 8, 2021 12:46:43.287707090 CEST	80	49723	104.160.174.177	192.168.2.6
Apr 8, 2021 12:46:43.287720919 CEST	80	49723	104.160.174.177	192.168.2.6
Apr 8, 2021 12:46:43.287738085 CEST	80	49723	104.160.174.177	192.168.2.6
Apr 8, 2021 12:46:43.287756920 CEST	80	49723	104.160.174.177	192.168.2.6
Apr 8, 2021 12:46:43.287769079 CEST	80	49723	104.160.174.177	192.168.2.6
Apr 8, 2021 12:46:43.287785053 CEST	80	49723	104.160.174.177	192.168.2.6
Apr 8, 2021 12:46:43.287884951 CEST	49723	80	192.168.2.6	104.160.174.177
Apr 8, 2021 12:46:43.287955999 CEST	49723	80	192.168.2.6	104.160.174.177
Apr 8, 2021 12:46:43.287972927 CEST	49723	80	192.168.2.6	104.160.174.177
Apr 8, 2021 12:46:48.174196005 CEST	49726	80	192.168.2.6	104.161.84.100
Apr 8, 2021 12:46:48.335020065 CEST	80	49726	104.161.84.100	192.168.2.6
Apr 8, 2021 12:46:48.335206032 CEST	49726	80	192.168.2.6	104.161.84.100
Apr 8, 2021 12:46:48.335388899 CEST	49726	80	192.168.2.6	104.161.84.100
Apr 8, 2021 12:46:48.495990038 CEST	80	49726	104.161.84.100	192.168.2.6
Apr 8, 2021 12:46:48.497931004 CEST	80	49726	104.161.84.100	192.168.2.6
Apr 8, 2021 12:46:48.497960091 CEST	80	49726	104.161.84.100	192.168.2.6
Apr 8, 2021 12:46:48.498164892 CEST	49726	80	192.168.2.6	104.161.84.100
Apr 8, 2021 12:46:48.498274088 CEST	49726	80	192.168.2.6	104.161.84.100
Apr 8, 2021 12:46:48.658807993 CEST	80	49726	104.161.84.100	192.168.2.6
Apr 8, 2021 12:46:58.729919910 CEST	49741	80	192.168.2.6	198.185.159.144
Apr 8, 2021 12:46:58.836591959 CEST	80	49741	198.185.159.144	192.168.2.6
Apr 8, 2021 12:46:58.836755037 CEST	49741	80	192.168.2.6	198.185.159.144
Apr 8, 2021 12:46:58.836958885 CEST	49741	80	192.168.2.6	198.185.159.144
Apr 8, 2021 12:46:58.943339109 CEST	80	49741	198.185.159.144	192.168.2.6
Apr 8, 2021 12:46:58.951539993 CEST	80	49741	198.185.159.144	192.168.2.6
Apr 8, 2021 12:46:58.951575041 CEST	80	49741	198.185.159.144	192.168.2.6
Apr 8, 2021 12:46:58.951591969 CEST	80	49741	198.185.159.144	192.168.2.6
Apr 8, 2021 12:46:58.951605082 CEST	80	49741	198.185.159.144	192.168.2.6
Apr 8, 2021 12:46:58.951620102 CEST	80	49741	198.185.159.144	192.168.2.6
Apr 8, 2021 12:46:58.951636076 CEST	80	49741	198.185.159.144	192.168.2.6
Apr 8, 2021 12:46:58.951647997 CEST	80	49741	198.185.159.144	192.168.2.6
Apr 8, 2021 12:46:58.951667070 CEST	80	49741	198.185.159.144	192.168.2.6
Apr 8, 2021 12:46:58.951689959 CEST	80	49741	198.185.159.144	192.168.2.6
Apr 8, 2021 12:46:58.951697111 CEST	80	49741	198.185.159.144	192.168.2.6
Apr 8, 2021 12:46:58.951709986 CEST	49741	80	192.168.2.6	198.185.159.144

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:46:58.951854944 CEST	49741	80	192.168.2.6	198.185.159.144
Apr 8, 2021 12:46:58.951930046 CEST	49741	80	192.168.2.6	198.185.159.144
Apr 8, 2021 12:46:59.058216095 CEST	80	49741	198.185.159.144	192.168.2.6
Apr 8, 2021 12:46:59.058240891 CEST	80	49741	198.185.159.144	192.168.2.6
Apr 8, 2021 12:46:59.058259964 CEST	80	49741	198.185.159.144	192.168.2.6
Apr 8, 2021 12:46:59.058274984 CEST	80	49741	198.185.159.144	192.168.2.6
Apr 8, 2021 12:46:59.058293104 CEST	80	49741	198.185.159.144	192.168.2.6
Apr 8, 2021 12:46:59.058310032 CEST	49741	80	192.168.2.6	198.185.159.144
Apr 8, 2021 12:46:59.058310986 CEST	80	49741	198.185.159.144	192.168.2.6
Apr 8, 2021 12:46:59.058326006 CEST	80	49741	198.185.159.144	192.168.2.6
Apr 8, 2021 12:46:59.058422089 CEST	80	49741	198.185.159.144	192.168.2.6
Apr 8, 2021 12:46:59.058439016 CEST	49741	80	192.168.2.6	198.185.159.144
Apr 8, 2021 12:46:59.058764935 CEST	49741	80	192.168.2.6	198.185.159.144
Apr 8, 2021 12:47:09.080147982 CEST	49742	80	192.168.2.6	34.102.136.180
Apr 8, 2021 12:47:09.092434883 CEST	80	49742	34.102.136.180	192.168.2.6
Apr 8, 2021 12:47:09.092621088 CEST	49742	80	192.168.2.6	34.102.136.180
Apr 8, 2021 12:47:09.092782021 CEST	49742	80	192.168.2.6	34.102.136.180
Apr 8, 2021 12:47:09.104984999 CEST	80	49742	34.102.136.180	192.168.2.6
Apr 8, 2021 12:47:09.209527016 CEST	80	49742	34.102.136.180	192.168.2.6
Apr 8, 2021 12:47:09.209676981 CEST	80	49742	34.102.136.180	192.168.2.6
Apr 8, 2021 12:47:09.209800959 CEST	49742	80	192.168.2.6	34.102.136.180
Apr 8, 2021 12:47:09.209867001 CEST	49742	80	192.168.2.6	34.102.136.180
Apr 8, 2021 12:47:09.222744942 CEST	80	49742	34.102.136.180	192.168.2.6
Apr 8, 2021 12:47:14.550185919 CEST	49743	80	192.168.2.6	193.168.194.206
Apr 8, 2021 12:47:17.559937954 CEST	49743	80	192.168.2.6	193.168.194.206
Apr 8, 2021 12:47:17.752141953 CEST	80	49743	193.168.194.206	192.168.2.6
Apr 8, 2021 12:47:17.752445936 CEST	49743	80	192.168.2.6	193.168.194.206
Apr 8, 2021 12:47:17.752739906 CEST	49743	80	192.168.2.6	193.168.194.206
Apr 8, 2021 12:47:17.944873095 CEST	80	49743	193.168.194.206	192.168.2.6
Apr 8, 2021 12:47:18.263333082 CEST	49743	80	192.168.2.6	193.168.194.206
Apr 8, 2021 12:47:18.495343924 CEST	80	49743	193.168.194.206	192.168.2.6
Apr 8, 2021 12:47:24.087763071 CEST	80	49743	193.168.194.206	192.168.2.6
Apr 8, 2021 12:47:24.087795973 CEST	80	49743	193.168.194.206	192.168.2.6
Apr 8, 2021 12:47:24.087848902 CEST	49743	80	192.168.2.6	193.168.194.206
Apr 8, 2021 12:47:24.087867975 CEST	49743	80	192.168.2.6	193.168.194.206
Apr 8, 2021 12:47:33.582299948 CEST	49749	80	192.168.2.6	199.59.242.153
Apr 8, 2021 12:47:33.692231894 CEST	80	49749	199.59.242.153	192.168.2.6
Apr 8, 2021 12:47:33.692333937 CEST	49749	80	192.168.2.6	199.59.242.153
Apr 8, 2021 12:47:33.692498922 CEST	49749	80	192.168.2.6	199.59.242.153
Apr 8, 2021 12:47:33.802305937 CEST	80	49749	199.59.242.153	192.168.2.6
Apr 8, 2021 12:47:33.802937031 CEST	80	49749	199.59.242.153	192.168.2.6
Apr 8, 2021 12:47:33.803009987 CEST	80	49749	199.59.242.153	192.168.2.6
Apr 8, 2021 12:47:33.803033113 CEST	80	49749	199.59.242.153	192.168.2.6
Apr 8, 2021 12:47:33.803052902 CEST	80	49749	199.59.242.153	192.168.2.6
Apr 8, 2021 12:47:33.803070068 CEST	80	49749	199.59.242.153	192.168.2.6
Apr 8, 2021 12:47:33.803193092 CEST	49749	80	192.168.2.6	199.59.242.153
Apr 8, 2021 12:47:33.803306103 CEST	49749	80	192.168.2.6	199.59.242.153
Apr 8, 2021 12:47:38.885835886 CEST	49750	80	192.168.2.6	85.159.66.93
Apr 8, 2021 12:47:38.937621117 CEST	80	49750	85.159.66.93	192.168.2.6
Apr 8, 2021 12:47:38.938090086 CEST	49750	80	192.168.2.6	85.159.66.93
Apr 8, 2021 12:47:38.938357115 CEST	49750	80	192.168.2.6	85.159.66.93
Apr 8, 2021 12:47:38.990061045 CEST	80	49750	85.159.66.93	192.168.2.6
Apr 8, 2021 12:47:38.990087032 CEST	80	49750	85.159.66.93	192.168.2.6
Apr 8, 2021 12:47:38.990317106 CEST	49750	80	192.168.2.6	85.159.66.93
Apr 8, 2021 12:47:38.990350962 CEST	49750	80	192.168.2.6	85.159.66.93
Apr 8, 2021 12:47:39.041932106 CEST	80	49750	85.159.66.93	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:45:40.491200924 CEST	58377	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:45:40.503812075 CEST	53	58377	8.8.8.8	192.168.2.6
Apr 8, 2021 12:45:40.519510031 CEST	55074	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:45:40.531883955 CEST	53	55074	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:45:40.561065912 CEST	54513	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:45:40.574002981 CEST	53	54513	8.8.8.8	192.168.2.6
Apr 8, 2021 12:45:41.460359097 CEST	62044	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:45:41.473582029 CEST	53	62044	8.8.8.8	192.168.2.6
Apr 8, 2021 12:45:42.396193981 CEST	63791	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:45:42.415102959 CEST	53	63791	8.8.8.8	192.168.2.6
Apr 8, 2021 12:45:46.134046078 CEST	64267	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:45:46.146598101 CEST	53	64267	8.8.8.8	192.168.2.6
Apr 8, 2021 12:45:46.986300945 CEST	49448	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:45:46.998900890 CEST	53	49448	8.8.8.8	192.168.2.6
Apr 8, 2021 12:45:52.766400099 CEST	60342	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:45:52.779835939 CEST	53	60342	8.8.8.8	192.168.2.6
Apr 8, 2021 12:46:02.372802019 CEST	61346	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:46:02.385209084 CEST	53	61346	8.8.8.8	192.168.2.6
Apr 8, 2021 12:46:04.517719984 CEST	51774	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:46:04.529655933 CEST	53	51774	8.8.8.8	192.168.2.6
Apr 8, 2021 12:46:06.922087908 CEST	56023	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:46:06.934973001 CEST	53	56023	8.8.8.8	192.168.2.6
Apr 8, 2021 12:46:08.683914900 CEST	58384	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:46:08.697056055 CEST	53	58384	8.8.8.8	192.168.2.6
Apr 8, 2021 12:46:11.894196033 CEST	60261	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:46:11.907191992 CEST	53	60261	8.8.8.8	192.168.2.6
Apr 8, 2021 12:46:12.857455969 CEST	56061	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:46:12.869524956 CEST	53	56061	8.8.8.8	192.168.2.6
Apr 8, 2021 12:46:13.544354916 CEST	58336	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:46:13.557018995 CEST	53	58336	8.8.8.8	192.168.2.6
Apr 8, 2021 12:46:14.242495060 CEST	53781	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:46:14.256418943 CEST	53	53781	8.8.8.8	192.168.2.6
Apr 8, 2021 12:46:15.592278957 CEST	54064	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:46:15.604839087 CEST	53	54064	8.8.8.8	192.168.2.6
Apr 8, 2021 12:46:16.340641975 CEST	52811	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:46:16.354026079 CEST	53	52811	8.8.8.8	192.168.2.6
Apr 8, 2021 12:46:17.016047001 CEST	55299	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:46:17.029288054 CEST	53	55299	8.8.8.8	192.168.2.6
Apr 8, 2021 12:46:17.737343073 CEST	63745	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:46:17.750946999 CEST	53	63745	8.8.8.8	192.168.2.6
Apr 8, 2021 12:46:18.768487930 CEST	50055	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:46:18.781229973 CEST	53	50055	8.8.8.8	192.168.2.6
Apr 8, 2021 12:46:19.469026089 CEST	61374	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:46:19.481959105 CEST	53	61374	8.8.8.8	192.168.2.6
Apr 8, 2021 12:46:29.406141043 CEST	50339	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:46:29.423815012 CEST	53	50339	8.8.8.8	192.168.2.6
Apr 8, 2021 12:46:36.685190916 CEST	63307	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:46:36.704133034 CEST	53	63307	8.8.8.8	192.168.2.6
Apr 8, 2021 12:46:38.335319042 CEST	49694	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:46:38.818474054 CEST	53	49694	8.8.8.8	192.168.2.6
Apr 8, 2021 12:46:46.989202976 CEST	54982	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:46:47.105591059 CEST	53	54982	8.8.8.8	192.168.2.6
Apr 8, 2021 12:46:47.799890041 CEST	50010	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:46:48.030651093 CEST	63718	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:46:48.069102049 CEST	53	50010	8.8.8.8	192.168.2.6
Apr 8, 2021 12:46:48.173165083 CEST	53	63718	8.8.8.8	192.168.2.6
Apr 8, 2021 12:46:48.494082928 CEST	62116	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:46:48.506784916 CEST	53	62116	8.8.8.8	192.168.2.6
Apr 8, 2021 12:46:48.805192947 CEST	63816	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:46:48.818182945 CEST	53	63816	8.8.8.8	192.168.2.6
Apr 8, 2021 12:46:49.010258913 CEST	55014	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:46:49.045222998 CEST	53	55014	8.8.8.8	192.168.2.6
Apr 8, 2021 12:46:49.234910011 CEST	62208	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:46:49.324081898 CEST	53	62208	8.8.8.8	192.168.2.6
Apr 8, 2021 12:46:49.741507053 CEST	57574	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:46:49.755121946 CEST	53	57574	8.8.8.8	192.168.2.6
Apr 8, 2021 12:46:50.091692924 CEST	51818	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:46:50.104129076 CEST	53	51818	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:46:50.764836073 CEST	56628	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:46:50.832796097 CEST	53	56628	8.8.8.8	192.168.2.6
Apr 8, 2021 12:46:51.420423031 CEST	60778	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:46:51.433657885 CEST	53	60778	8.8.8.8	192.168.2.6
Apr 8, 2021 12:46:51.829622984 CEST	53799	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:46:51.842360020 CEST	53	53799	8.8.8.8	192.168.2.6
Apr 8, 2021 12:46:53.534490108 CEST	54683	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:46:53.672425032 CEST	53	54683	8.8.8.8	192.168.2.6
Apr 8, 2021 12:46:56.255649090 CEST	59329	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:46:56.274786949 CEST	53	59329	8.8.8.8	192.168.2.6
Apr 8, 2021 12:46:58.687747002 CEST	64021	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:46:58.728197098 CEST	53	64021	8.8.8.8	192.168.2.6
Apr 8, 2021 12:47:03.972100973 CEST	56129	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:47:03.995660067 CEST	53	56129	8.8.8.8	192.168.2.6
Apr 8, 2021 12:47:09.055725098 CEST	58177	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:47:09.078679085 CEST	53	58177	8.8.8.8	192.168.2.6
Apr 8, 2021 12:47:14.224930048 CEST	50700	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:47:14.548867941 CEST	53	50700	8.8.8.8	192.168.2.6
Apr 8, 2021 12:47:21.684954882 CEST	54069	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:47:21.743495941 CEST	53	54069	8.8.8.8	192.168.2.6
Apr 8, 2021 12:47:23.284853935 CEST	61178	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:47:23.360908031 CEST	53	61178	8.8.8.8	192.168.2.6
Apr 8, 2021 12:47:27.867861986 CEST	57017	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:47:27.880448103 CEST	53	57017	8.8.8.8	192.168.2.6
Apr 8, 2021 12:47:28.412189960 CEST	56327	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:47:28.458304882 CEST	53	56327	8.8.8.8	192.168.2.6
Apr 8, 2021 12:47:30.204473972 CEST	50243	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:47:30.231271982 CEST	53	50243	8.8.8.8	192.168.2.6
Apr 8, 2021 12:47:33.472132921 CEST	62055	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:47:33.581131935 CEST	53	62055	8.8.8.8	192.168.2.6
Apr 8, 2021 12:47:38.813100100 CEST	61249	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:47:38.883302927 CEST	53	61249	8.8.8.8	192.168.2.6
Apr 8, 2021 12:47:44.016849041 CEST	65252	53	192.168.2.6	8.8.8.8
Apr 8, 2021 12:47:44.147923946 CEST	53	65252	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2021 12:46:38.335319042 CEST	192.168.2.6	8.8.8.8	0xd2c6	Standard query (0)	www.ly-iot.com	A (IP address)	IN (0x0001)
Apr 8, 2021 12:46:48.030651093 CEST	192.168.2.6	8.8.8.8	0x5e24	Standard query (0)	www.ronwongart.com	A (IP address)	IN (0x0001)
Apr 8, 2021 12:46:53.534490108 CEST	192.168.2.6	8.8.8.8	0xb23	Standard query (0)	www.vbkulkarni.com	A (IP address)	IN (0x0001)
Apr 8, 2021 12:46:58.687747002 CEST	192.168.2.6	8.8.8.8	0x75b4	Standard query (0)	www.pimpmyrecipe.com	A (IP address)	IN (0x0001)
Apr 8, 2021 12:47:03.972100973 CEST	192.168.2.6	8.8.8.8	0xda46	Standard query (0)	www.csgo-roll.net	A (IP address)	IN (0x0001)
Apr 8, 2021 12:47:09.055725098 CEST	192.168.2.6	8.8.8.8	0x43ea	Standard query (0)	www.foodsystemsjusticeproject.com	A (IP address)	IN (0x0001)
Apr 8, 2021 12:47:14.224930048 CEST	192.168.2.6	8.8.8.8	0x2ff5	Standard query (0)	www.batiktintaemas.com	A (IP address)	IN (0x0001)
Apr 8, 2021 12:47:23.284853935 CEST	192.168.2.6	8.8.8.8	0x5600	Standard query (0)	www.breathharbour.net	A (IP address)	IN (0x0001)
Apr 8, 2021 12:47:28.412189960 CEST	192.168.2.6	8.8.8.8	0x1d35	Standard query (0)	www.libreo.club	A (IP address)	IN (0x0001)
Apr 8, 2021 12:47:33.472132921 CEST	192.168.2.6	8.8.8.8	0x3f25	Standard query (0)	www.addthat.xyz	A (IP address)	IN (0x0001)
Apr 8, 2021 12:47:38.813100100 CEST	192.168.2.6	8.8.8.8	0x439	Standard query (0)	www.evecrude.xyz	A (IP address)	IN (0x0001)
Apr 8, 2021 12:47:44.016849041 CEST	192.168.2.6	8.8.8.8	0xb854	Standard query (0)	www.generaflix.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 12:46:38.818474054 CEST	8.8.8.8	192.168.2.6	0xd2c6	No error (0)	www.ly-iot.com	l.17986.net		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 12:46:38.818474054 CEST	8.8.8.8	192.168.2.6	0xd2c6	No error (0)	l.17986.net		104.160.174.177	A (IP address)	IN (0x0001)
Apr 8, 2021 12:46:48.173165083 CEST	8.8.8.8	192.168.2.6	0x5e24	No error (0)	www.ronwongart.com		104.161.84.100	A (IP address)	IN (0x0001)
Apr 8, 2021 12:46:53.672425032 CEST	8.8.8.8	192.168.2.6	0xb23	Name error (3)	www.vbkulkarni.com	none	none	A (IP address)	IN (0x0001)
Apr 8, 2021 12:46:58.728197098 CEST	8.8.8.8	192.168.2.6	0x75b4	No error (0)	www.pimpmyrecipe.com	ext-cust.squarespace.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 12:46:58.728197098 CEST	8.8.8.8	192.168.2.6	0x75b4	No error (0)	ext-cust.squarespace.com		198.185.159.144	A (IP address)	IN (0x0001)
Apr 8, 2021 12:46:58.728197098 CEST	8.8.8.8	192.168.2.6	0x75b4	No error (0)	ext-cust.squarespace.com		198.49.23.144	A (IP address)	IN (0x0001)
Apr 8, 2021 12:46:58.728197098 CEST	8.8.8.8	192.168.2.6	0x75b4	No error (0)	ext-cust.squarespace.com		198.49.23.145	A (IP address)	IN (0x0001)
Apr 8, 2021 12:46:58.728197098 CEST	8.8.8.8	192.168.2.6	0x75b4	No error (0)	ext-cust.squarespace.com		198.185.159.145	A (IP address)	IN (0x0001)
Apr 8, 2021 12:47:09.078679085 CEST	8.8.8.8	192.168.2.6	0x43ea	No error (0)	www.foodsystemsjusticeproject.com	foodsystemsjusticeproject.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 12:47:09.078679085 CEST	8.8.8.8	192.168.2.6	0x43ea	No error (0)	foodsystemsjusticeproject.com		34.102.136.180	A (IP address)	IN (0x0001)
Apr 8, 2021 12:47:14.548867941 CEST	8.8.8.8	192.168.2.6	0x2ff5	No error (0)	www.batiktintaemas.com	batiktintaemas.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 12:47:14.548867941 CEST	8.8.8.8	192.168.2.6	0x2ff5	No error (0)	batiktintaemas.com		193.168.194.206	A (IP address)	IN (0x0001)
Apr 8, 2021 12:47:23.360908031 CEST	8.8.8.8	192.168.2.6	0x5600	Server failure (2)	www.breathharbour.net	none	none	A (IP address)	IN (0x0001)
Apr 8, 2021 12:47:28.458304882 CEST	8.8.8.8	192.168.2.6	0x1d35	Name error (3)	www.libreo.club	none	none	A (IP address)	IN (0x0001)
Apr 8, 2021 12:47:33.581131935 CEST	8.8.8.8	192.168.2.6	0x3f25	No error (0)	www.addthat.xyz		199.59.242.153	A (IP address)	IN (0x0001)
Apr 8, 2021 12:47:38.883302927 CEST	8.8.8.8	192.168.2.6	0x439	No error (0)	www.evecrude.xyz	redirect.natrocdn.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 12:47:38.883302927 CEST	8.8.8.8	192.168.2.6	0x439	No error (0)	redirect.natrocdn.com	natroredirect.natrocdn.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 12:47:38.883302927 CEST	8.8.8.8	192.168.2.6	0x439	No error (0)	natroredirect.natrocdn.com		85.159.66.93	A (IP address)	IN (0x0001)
Apr 8, 2021 12:47:44.147923946 CEST	8.8.8.8	192.168.2.6	0xb854	No error (0)	www.generalflix.com	generalflix.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 12:47:44.147923946 CEST	8.8.8.8	192.168.2.6	0xb854	No error (0)	generalflix.com		94.46.9.37	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.ly-iot.com
- www.ronwongart.com
- www.pimpmyrecipe.com
- www.foodsystemsjusticeproject.com
- www.batiktintaemas.com
- www.addthat.xyz
- www.evecrude.xyz

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49723	104.160.174.177	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:46:42.498070002 CEST	1250	OUT	GET /goei/?EzuXh6BP=B46qr3zTyBR1t+VKbrees7UR/FiD4WL3nz1lGh06nIBkEBDQrNA0bRgDDyF1Au9+nA9wWbL6eg==&RL0=rVvxj02xpd_lyz HTTP/1.1 Host: www.ly-iot.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 12:46:43.287656069 CEST	1252	IN	HTTP/1.1 200 OK Server: nginx/1.17.10 Date: Thu, 08 Apr 2021 10:46:43 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Powered-By: PHP/7.3.15 Data Raw: 31 39 65 33 0d 0a 3c 68 74 6d 6c 3e 0d 0a 20 20 20 20 3c 68 65 61 64 3e 0d 0a 20 20 20 20 20 20 20 20 3c 74 69 74 6c 65 3e 6c 79 2d 69 6f 74 2e 63 6f 6d 20 2d 20 54 68 65 20 64 6f 6d 61 69 6e 20 69 73 20 61 76 61 69 6c 61 62 6c 65 20 66 6f 72 20 70 75 72 63 68 61 73 65 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 2e 30 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 6e 6f 22 2f 3e 3c 73 63 72 69 70 74 20 73 72 63 3d 22 68 74 74 70 3a 2f 2f 6c 69 62 73 2e 62 61 69 64 75 2e 63 6f 6d 2f 6a 71 75 65 72 79 2f 31 2e 39 2e 30 2f 6a 71 75 65 72 79 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 3c 73 63 72 69 70 74 3e 24 28 64 6f 63 75 6d 65 6e 74 29 2e 72 65 61 64 79 28 66 75 6e 63 74 69 6f 6e 28 29 7b 69 66 28 77 69 6e 64 6f 77 2e 73 63 72 65 65 6e 2e 68 65 69 67 68 74 3c 37 30 30 29 7b 24 28 22 2a 22 29 2e 63 73 73 28 7b 22 77 69 64 74 68 22 3a 22 61 75 74 6f 22 2c 22 68 65 69 67 68 74 22 3a 22 61 75 74 6f 22 2c 22 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 22 3a 22 6e 6f 6e 65 22 2c 22 70 6f 73 69 74 69 6f 6e 22 3a 22 73 74 61 74 69 63 22 7d 29 3b 24 28 22 70 22 29 2e 63 73 73 28 22 63 6f 6c 6f 72 22 2c 22 62 6c 61 63 6b 22 29 3b 24 28 22 2e 73 74 65 6e 63 69 6c 2d 74 69 70 22 29 2e 63 73 73 28 22 6c 69 6e 65 2d 68 65 69 67 68 74 22 2c 22 33 30 70 78 22 29 3b 7d 7d 29 3b 3c 2f 73 63 72 69 70 74 3e 0d 0a 20 20 20 20 20 20 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 42 4f 44 59 20 7b 0d 0a 09 46 4f 4e 54 2d 53 49 5a 45 3a 20 31 32 70 78 3b 20 4d 41 52 47 49 4e 3a 20 31 38 70 78 20 30 70 78 20 30 70 78 3b 20 43 4f 4c 4f 52 3a 20 23 34 32 34 32 3b 20 42 41 43 4b 47 52 4f 55 4e 44 2d 43 4f 4c 4f 52 3a 20 23 66 66 66 3b 20 54 45 58 54 2d 41 4c 49 47 4e 3a 20 63 65 6e 74 65 72 0d 0a 7d 0d 0a 54 44 20 7b 0d 0a 09 46 4f 4e 54 2d 46 41 4d 49 4c 59 3a 20 41 72 69 61 6c 0d 0a 7d 0d 0a 50 20 7b 0d 0a 09 46 4f 4e 54 2d 46 41 4d 49 4c 59 3a 20 41 72 69 61 6c 0d 0a 7d 0d 0a 44 49 56 20 7b 0d 0a 09 46 4f 4e 54 2d 46 41 4d 49 4c 59 3a 20 41 72 69 61 6c 0d 0a 7d 0d 0a 49 4e 50 55 54 20 7b 0d 0a 09 46 4f 4e 54 2d 46 41 4d 49 4c 59 3a 20 41 72 69 61 6c 0d 0a 7d 0d 0a 49 4d 47 20 7b 0d 0a 09 42 4f 52 44 45 52 2d 52 49 47 48 54 3a 20 30 70 78 3b 20 42 4f 52 44 45 52 2d 54 4f 50 3a 20 30 70 78 3b 20 42 4f 52 44 45 52 2d 4c 45 46 54 3a 20 30 70 78 3b 20 42 4f 52 44 45 52 2d 42 4f 54 54 4f 4d 3a 20 30 70 78 0d 0a 7d 0d 0a 54 44 20 7b 0d 0a 09 46 4f 4e 54 2d 53 49 5a 45 3a 20 31 32 70 78 3b 20 4c 49 4e 45 2d 48 45 49 47 48 54 3a 20 31 35 30 25 0d 0a 7d 0d 0a 54 48 20 7b 0d 0a 09 46 4f 4e 54 2d 53 49 5a 45 3a 20 31 32 70 78 3b 20 4c 49 4e 45 2d 48 45 49 47 48 54 3a 20 31 35 30 25 0d 0a 7d 0d 0a 23 66 20 7b 0d 0a 09 4d 41 52 47 49 4e 3a 20 30 70 78 3b 20 50 41 44 44 49 4e 47 2d 54 4f 50 3a 20 34 70 78 0d 0a 7d 0d 0a 23 42 20 7b 0d 0a 09 57 49 44 54 48 3a 20 38 30 30 70 78 0d 0a 7d 0d 0a 2e 68 65 61 64 65 72 20 7b 0d 0a 09 42 4f 52 44 45 52 2d 42 4f 54 54 4f 4d 3a 20 23 62 32 64 30 65 61 20 31 70 78 20 73 6f Data Ascii: 19e3<html> <head> <title>ly-iot.com - The domain is available for purchase</title><meta name="viewport" content="width=device-width, initial-scale=1.0, minimum-scale=1.0, maximum-scale=1.0, user-scalable=no"/><script src="http://libs.baidu.com/jquery/1.9.0/jquery.js"></script><script>$(document).ready(function(){if(window.screen.height<700){$("*").css({"width":"auto","height":"auto","background-image":"none","position":"static"});$("p").css("color","black");$(".stencil-tip").css("line-height","30px");}});</script> <style type="text/css">BODY {FONT-SIZE: 12px; MARGIN: 18px 0px 0px; COLOR: #424242; BACKGROUND-COLOR: #fff; TEXT-ALIGN: center}TD {FONT-FAMILY: Arial}P {FONT-FAMILY: Arial}DIV {FONT-FAMILY: Arial}INPUT {FONT-FAMILY: Arial}IMG {BORDER-RIGHT: 0px; BORDER-TOP: 0px; BORDER-LEFT: 0px; BORDER-BOTTOM: 0px}TD {FONT-SIZE: 12px; LINE-HEIGHT: 150%}TH {FONT-SIZE: 12px; LINE-HEIGHT: 150%}#f {MARGIN: 0px; PADDING-TOP: 4px}#B {WIDTH: 800px}.header {BORDER-BOTTOM: #b2d0ea 1px so

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49726	104.161.84.100	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:46:48.335388899 CEST	1385	OUT	GET /goei/?EzuXh6BP=GY2gQUF0Rr/aPbkdLLDyshZLrmGphrTrFvzfodUnQAaoW3qjeuccMn3ranK+t6GyiOOsZqKqHA==&RL0=rVvxj02xpd_lyz HTTP/1.1 Host: www.ronwongart.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 12:46:48.497931004 CEST	1403	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 08 Apr 2021 10:47:07 GMT Content-Type: text/html; charset=GBK Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Data Raw: 32 33 63 0d 0a 0d 0a 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 20 62 67 63 6f 6c 6f 72 3d 22 77 68 69 74 65 22 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 2f 31 2e 34 2e 33 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 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 2 0 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 23c<html><head><title>403 Forbidden</title></head><body bgcolor="white"><center> 403 Forbidden </center><hr><center>nginx/1.4.3</center></body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49741	198.185.159.144	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:46:58.836958885 CEST	5606	OUT	GET /goei/?EzuXh6BP=TTuxDc9EejbduYk8ZHEjlKcpN/O2EpBILXUKac8y6lhY4fajDGEqKXEgdN9L03N9MJzUHOy50w==&RL0=rVvxj02xpd_lyz HTTP/1.1 Host: www.pimpmyrecipe.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:46:58.951539993 CEST	5609	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 10:46:58 UTC Expires: Thu, 01 Jan 1970 00:00:00 UTC Pragma: no-cache Server: Squarespace X-Contextid: rofEdlC9/lBVebWxJ Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 3c 74 69 74 6c 65 3e 34 30 30 20 42 61 64 20 52 65 71 75 65 73 74 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 0a 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 20 77 68 69 74 65 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 7b 0a 20 20 20 20 70 6f 73 69 74 69 6f 6e 3a 20 61 62 73 6f 6c 75 74 65 3b 0a 20 20 20 20 74 6f 70 3a 20 35 30 25 3b 0a 20 20 20 20 6c 65 66 74 3a 20 35 30 25 3b 0a 20 20 20 20 74 72 61 6e 73 66 6f 72 6d 3a 20 74 72 61 6e 73 6c 61 74 65 28 2d 35 30 25 2c 20 2d 35 30 25 29 3b 0a 20 20 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 20 20 20 20 6d 69 6e 2d 77 69 64 74 68 3a 20 39 35 76 77 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 68 31 20 7b 0a 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 33 30 30 3b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 34 2e 36 65 6d 3b 0a 20 20 20 20 63 6f 6c 6f 72 3a 20 23 31 39 31 39 31 39 3b 0a 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 20 30 20 31 31 70 78 20 30 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 70 20 7b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 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 6f 6e 74 2d 77 65 69 67 68 74 3a 20 33 30 30 3b 0a 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 32 65 6d 3b 0a 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 70 20 61 20 7b 0a 20 20 20 20 63 6f 6c 6f 72 3a 20 23 33 61 33 61 33 61 3b 0a 20 20 20 20 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 20 6e 6f 6e 65 3b 0a 20 20 20 20 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 20 73 6f 6c 69 64 20 31 70 78 20 23 33 61 33 61 33 61 3b 0a 20 20 7d 0a 0a 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 22 43 6c 61 72 6b 73 6f 6e 22 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 32 70 78 3b 0a 20 20 7d 0a 0a 20 20 23 73 74 61 74 75 73 2d 70 61 67 65 20 7b 0a 20 20 20 20 64 69 73 70 6c 61 79 3a 20 6e 6f 6e 65 3b 0a 20 20 7d 0a 0a 20 20 66 6f 6f 74 65 72 20 7b 0a 20 20 20 20 70 6f 73 69 74 69 6f 6e 3a 20 61 62 73 6f 6c 75 74 65 3b 0a 20 20 20 20 62 6f 74 74 6f 6d 3a 20 32 32 70 78 3b 0a 20 20 20 20 6c 65 66 74 3a 20 30 3b 0a 20 20 20 20 77 69 64 74 68 3a 20 31 30 30 25 3b 0a 20 20 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 32 65 6d 3b 0a 20 20 7d 0a 0a 20 20 66 6f 6f 74 65 72 20 73 70 61 6e 3b 0a 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 20 31 31 70 78 3b 0a 20 20 20 20 66 6f 6f 74 65 72 20 73 70 61 6e 3a 20 31 65 6d 3b 0a 20 20 20 20 Data Ascii: <!DOCTYPE html><head> <title>400 Bad Request</title> <meta name="viewport" content="width=device-width, initial-scale=1"> <style type="text/css"> body { background: white; } main { position: absolute; top: 50%; left: 50%; transform: translate(-50%, -50%); text-align: center; min-width: 95vw; } main h1 { font-weight: 300; font-size: 4.6em; color: #191919; margin: 0 0 11px 0; } main p { font-size: 1.4em; color: #3a3a3a; font-weight: 300; line-height: 2em; margin: 0; } main p a { color: #3a3a3a; text-decoration: none; border-bottom: solid 1px #3a3a3a; } body { font-family: "Clarkson", sans-serif; font-size: 12px; } #status-page { display: none; } footer { position: absolute; bottom: 22px; left: 0; width: 100%; text-align: center; line-height: 2em; } footer span { margin: 0 11px; font-size: 1em;

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.6	49742	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:47:09.092782021 CEST	6398	OUT	GET /goei/?EzuXh6BP=BdWs9+XwUamw8CUuz3E8yrboev7iCL3gb6z7OkS86X4CeTXY3ejv3dXKop2WOnP3DDbLLyGv2A==&RL0=rVvxj02xpd_lyz HTTP/1.1 Host: www.foodsystemsjusticeproject.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 12:47:09.209527016 CEST	6398	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 08 Apr 2021 10:47:09 GMT Content-Type: text/html Content-Length: 275 ETag: "606abe1d-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.6	49743	193.168.194.206	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:47:17.752739906 CEST	6399	OUT	GET /goei/?EzuXh6BP=iESvN3vx+46BgVwWtoPvPQmUnTMTtp1hHS9L6erIUoS4dJlpb0oL7GpX49j9BG002Zkja/L0IA==&RL0=rVvxj02xpd_lyz HTTP/1.1 Host: www.batiktintaemas.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 12:47:24.087763071 CEST	6409	IN	HTTP/1.1 301 Moved Permanently Connection: close X-Powered-By: PHP/7.2.34 Content-Type: text/html; charset=UTF-8 Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: http://batiktintaemas.com/goei/?EzuXh6BP=iESvN3vx+46BgVwWtoPvPQmUnTMTtp1hHS9L6erIUoS4dJlpb0oL7GpX49j9BG002Zkja/L0IA==&RL0=rVvxj02xpd_lyz Content-Length: 0 Date: Thu, 08 Apr 2021 10:47:23 GMT Server: LiteSpeed Vary: User-Agent

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.6	49749	199.59.242.153	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:47:33.692498922 CEST	6429	OUT	GET /goei/?EzuXh6BP=WHzdRAWCNmljEZUdYknMeV5zI3m+uLt35kXWxc+UN/aPGTi9DTFvtLFMQ5OC8xESdqE/mkifJw==&RL0=rVvxj02xpd_lyz HTTP/1.1 Host: www.addthat.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 12:47:33.802937031 CEST	6430	IN	HTTP/1.1 200 OK Server: openresty Date: Thu, 08 Apr 2021 10:47:33 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANDrp2lz7AOmADaN8tA50LsWcjLFyQFcb/P2Txc58oYOeILb3vBw7J6f4pamkAQVSQuqYsKx3YzdUHCvbVZvFUsCAwEAAQ==_a7msil34EyaoVjODEDUQ2ff4sUDhxeCYFMDh2tCvLxODdKADG02BsrkHtQfUPBUVH5YKtKdN4CUGklYGwKwPLA== 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 61 37 6d 73 69 6c 33 34 45 79 61 6f 56 6a 4f 44 45 44 55 51 32 66 66 34 73 55 44 68 78 65 43 59 46 4d 44 68 32 74 43 76 4c 78 4f 44 64 4b 41 44 47 30 32 42 73 72 6b 48 74 51 66 55 50 42 55 56 48 35 59 4b 74 4b 64 4e 34 43 55 47 6b 6c 59 47 77 4b 77 50 4c 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==_a7msil34EyaoVjODEDUQ2ff4sUDhxeCYFMDh2tCvLxODdKADG02BsrkHtQfUPBUVH5YKtKdN4CUGklYGwKwPLA==><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
6	192.168.2.6	49750	85.159.66.93	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:47:38.938357115 CEST	6435	OUT	GET /goei/?EzuXh6BP=1hbvBZ6scGrlPy0N1riO1jCdFmqX21DbBNOeXEZPJTZAL1bLTprMXMNvQ4/+FZIG6w0HvwIWjw==&RL0=rVvxj02xpd_lyz HTTP/1.1 Host: www.evecrude.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 12:47:38.990061045 CEST	6436	IN	HTTP/1.1 404 Not Found Content-Type: text/html Server: Microsoft-IIS/10.0 X-Powered-By: ASP.NET Date: Thu, 08 Apr 2021 10:47:16 GMT Connection: close Content-Length: 1245 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 53 74 72 69 63 74 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f 78 68 74 6d 6c 31 2d 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 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 69 73 6f 2d 38 38 35 39 2d 31 22 2f 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 2d 20 46 69 6c 65 20 6f 72 20 64 69 72 65 63 74 6f 72 79 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0d 0a 3c 21 2d 2d 0d 0a 62 6f 64 79 7b 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 2d 73 69 7a 65 3a 2e 37 65 6d 3b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 56 65 72 64 61 6e 61 2c 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 45 45 45 45 45 45 3b 7d 0d 0a 66 69 65 6c 64 73 65 74 7b 70 61 64 64 69 6e 67 3a 30 20 31 35 70 78 20 31 30 70 78 20 31 35 70 78 3b 7d 20 0d 0a 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 32 2e 34 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 63 6f 6c 6f 72 3a 23 46 46 46 3b 7d 0d 0a 68 32 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 37 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 63 6f 6c 6f 72 3a 23 43 43 30 30 30 30 3b 7d 20 0d 0a 68 33 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 32 65 6d 3b 6d 61 72 67 69 6e 3a 31 30 70 78 20 30 20 30 20 30 3b 63 6f 6c 6f 72 3a 23 30 30 30 30 30 30 3b 7d 20 0d 0a 23 68 65 61 64 65 72 7b 77 69 64 74 68 3a 39 36 25 3b 6d 61 72 67 69 6e 3a 30 20 30 20 30 20 30 3b 70 61 64 64 69 6e 67 3a 36 70 78 20 32 25 20 36 70 78 20 32 25 3b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 74 72 65 62 75 63 68 65 74 20 4d 53 22 2c 20 56 65 72 64 61 6e 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 63 6f 6c 6f 72 3a 23 46 46 46 3b 0d 0a 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 35 35 35 35 35 35 3b 7d 0d 0a 23 63 6f 6e 74 65 6e 74 7b 6d 61 72 67 69 6e 3a 30 20 30 20 30 20 32 25 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 7d 0d 0a 2e 63 6f 6e 74 65 6e 74 2d 63 6f 6e 74 61 69 6e 65 72 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 46 46 3b 77 69 64 74 68 3a 39 36 25 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 38 70 78 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 7d 0d 0a 2d 2d 3e 0d 0a 3c 2f 73 74 79 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 64 69 76 20 69 64 3d 22 68 65 61 64 65 72 22 3e 3c 68 31 3e 53 65 72 76 65 72 20 45 72 72 6f 72 3c 2f 68 31 3e 3c 2f 64 69 76 3e 0d 0a 3c 64 69 76 20 69 64 3d 22 63 6f 6e 74 65 6e 74 22 3e 0d 0a 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 63 6f 6e 74 65 6e 74 2d 63 6f 6e 74 61 69 6e 65 72 22 3e 3c 66 69 65 6c 64 73 65 74 3e 0d 0a 20 20 3c 68 32 3e 34 30 34 20 2d 20 46 69 6c 65 20 6f 72 20 64 69 72 65 63 74 6f 72 79 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 68 32 3e 0d 0a 20 20 3c 68 33 3e 54 68 65 20 72 65 73 6f 75 72 63 65 20 79 6f 75 20 61 72 65 20 6c 6f 6f 6b 69 6e 67 20 66 6f 72 20 6d 69 67 68 74 20 68 61 76 65 20 62 65 65 6e 20 72 65 6d 6f 76 65 64 2c 20 68 61 64 20 69 74 73 20 6e 61 6d 65 20 63 68 61 6e 67 Data Ascii: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"><html xmlns="http://www.w3.org/1999/xhtml"><head><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/><title>404 - File or directory not found.</title><style type="text/css">...body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}fieldset{padding:0 15px 10px 15px;} h1{font-size:2.4em;margin:0;color:#FFF;}h2{font-size:1.7em;margin:0;color:#CC0000;} h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;} #header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;background-color:#555555;}#content{margin:0 0 0 2%;position:relative;}.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}--></style></head><body> <h1>Server Error</h1> <fieldset> <h2>404 - File or directory not found.</h2> <h3>The resource you are looking for might have been removed, had its name chang

Code Manipulations

Statistics

Behavior

- RCS76393.exe
- RCS76393.exe
- explorer.exe
- msiexec.exe
- cmd.exe
- conhost.exe

Click to jump to process

System Behavior

Analysis Process: RCS76393.exe PID: 6500 Parent PID: 5936

General

Start time:	12:45:47
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\RCS76393.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\RCS76393.exe'
Imagebase:	0x400000
File size:	386560 bytes
MD5 hash:	1AB1C3129FA0764EA0702DA70F3EF569
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: 00000002.00000002.326066867.0000000003F40000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.326066867.0000000003F40000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.326066867.0000000003F40000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

Analysis Process: RCS76393.exe PID: 6544 Parent PID: 6500

General

Start time:	12:45:48
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\RCS76393.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\RCS76393.exe'
Imagebase:	0x400000
File size:	386560 bytes
MD5 hash:	1AB1C3129FA0764EA0702DA70F3EF569
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000001.324919242.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000001.324919242.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000001.324919242.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.362951284.0000000000D00000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.362951284.0000000000D00000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.362951284.0000000000D00000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.362449000.0000000000990000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.362449000.0000000000990000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.362449000.0000000000990000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.362232664.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.362232664.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.362232664.0000000000400000.00000040.00000001.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	4182B7	NtReadFile

Analysis Process: explorer.exe PID: 3440 Parent PID: 6544

General

Start time:	12:45:51
Start date:	08/04/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6f22f0000
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: msiexec.exe PID: 6760 Parent PID: 3440

General

Start time:	12:46:03
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\msiexec.exe
Imagebase:	0x1a0000
File size:	59904 bytes
MD5 hash:	12C17B5A5C2A7B97342C362CA467E9A2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.587150105.0000000000480000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.587150105.0000000000480000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.587150105.0000000000480000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.587988322.00000000030A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.587988322.00000000030A0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.587988322.00000000030A0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.590270038.0000000004890000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.590270038.0000000004890000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.590270038.0000000004890000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	30B82B7	NtReadFile

Analysis Process: cmd.exe PID: 6848 Parent PID: 6760

General

Start time:	12:46:08
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\RCS76393.exe'
Imagebase:	0x2a0000
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: 6864 Parent PID: 6848

General

Start time:	12:46:12
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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