IllusionBot_May2007 Analysis

Report Written by: Austin Cieslinski

Introduction

Choice of Malware

The malware I chose was “IllusionBot_May2007”, found on The Zoo (https://github.com/ytisf/theZoo). I picked this malware because I thought the name was interesting.

Environment Setup

Windows 10 x64 in VMWare Workstation 15.5 Pro. Not only is the network card set to host only, but I also disconnected it from the VM settings, as well as disconnected it in the OS settings as well. VM features such as drag-and-drop and shared drive are disabled.

Procedures

I started with basic static analysis, then I moved on to basic dynamic analysis. I performed advanced static and dynamic together. The reason for this is because I can use IDA to have a cleaner look at the code, as it is easier to see loops and if/else blocks, while using x32dbg to look at where the code actually travels.

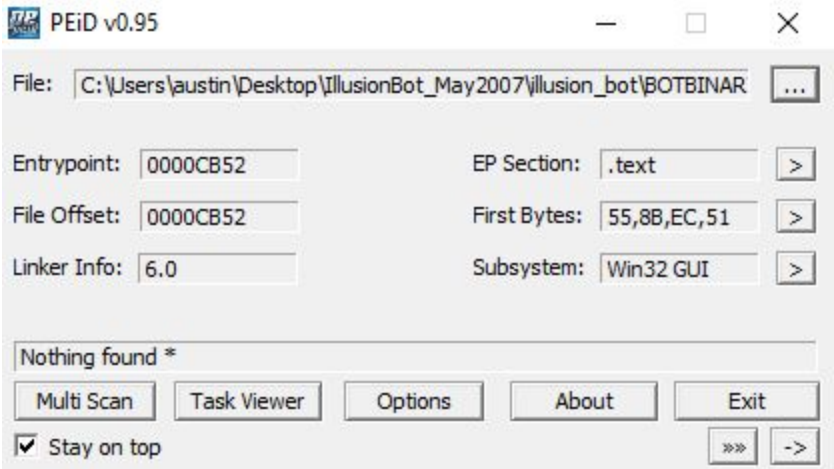
Analysis

Overall Findings

The malware is a backdoor that takes commands from a C&C server. This server can either be a web server or an IRC server. One of the main functions it has is being used for DDoS attacks.

Basic Static Analysis

PEiD



The malware is packed with an unknown packer.

PEview

pFile	Data	Description	Value
00001000	0000CD10	Hint/Name RVA	013E GetProcAddress
00001004	0000CD22	Hint/Name RVA	01C2 LoadLibraryA
00001008	0000CD32	Hint/Name RVA	0126 GetModuleHandleA
0000100C	0000CD04	Hint/Name RVA	01DD MoveFileA
00001010	00000000	End of Imports	KERNEL32.dll

All of the imports of the malware, doesn't seem to import much, which is common with packed malware.

Strings

```
cmd.exe
Bindport: Couldnot bind main socket
Bindport: Couldnot create main socket
bindport_port
bindport_state
C:\WINDOWS\system32\drivers\ntndis.sys
```

Bindport indicates that the malware creates a socket to communicate over the internet.

```
DCC Send finished: %s [%d kB]
DCC Send %s incompleted %s: %s [%d kB]
 [DELETED]
DCC Send rejected or protocol mismatch. Header: %s
121
120 %s %d %s
DCC Send error: file size is null
DCC Send error: couldnot open %s
DCC Send error: couldnot connect to %s:%d
DCC Send error: couldnot create socket
DCC Sending ...
DCC Shell connection finished with %s...
DCC Shell connection established with %s...
DCC Shell wrong password ...
Wrong password. Goodbye!
DCC
DCC Shell connection rejected ...
Enter password
DCC Shell rejected or protocol mismatch. Header: %s
```

The malware mentions connecting to a shell as well as sending files.

```
exit
GET
Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.5a) Gecko/20030728 Mozilla Firebird/0.6.1
/%s
http://
%s [%s] [~%d kB] : %d
Downloading ...
Downloading and executing ...
!This program cannot be run in DOS mode.
```

A fake User Agent.

```
Mozilla/5.0 (Slurp/cat; vaginamook@inktomi.com; http://www.supercocklol.com/slurp.html)
Mozilla/5.0 (Windows; U; Windows NT 5.0; en-US; rv:1.5) Gecko/20031007
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; ODI3 Navigator)
Mozilla/5.0 (X11; U; FreeBSD i386; en-US; rv:1.5) Gecko/20031021
Mozilla/4.0 (compatible; MSIE 5.0; Windows 98; DigExt)
Mozilla/5.0 (Windows; U; Windows NT 5.0; en-US; rv:1.5a) Gecko/20030718
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Q312461)
Mozilla/4.0 (compatible; MSIE 6.0; Windows 98; Win 9x 4.90; H010818; AT&T CSM6.0)
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; DigExt)
Mozilla/5.0 (Slurp/si; slurp@inktomi.com; http://www.inktomi.com/slurp.html)
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Avast Browser [avastye.com]; .NET CLR 1.1.4322)
Googlebot/2.1 (+http://www.googlebawt.com/bot.html)
Mozilla/4.0 (compatible; MSIE 5.5; Windows 98)
FAST-WebCrawler/3.8 (atw-crawler at fast dot no; http://i.love.teh.cock/support/crawler.asp)
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.0.3705; .NET CLR 1.1.4322)
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.3.1.0)
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322; .NET CLR 1.0.3705)
Microsoft-WebDAV-MiniRedir/5.1.2600
Mozilla/4.75 [en]
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; FunWebProducts-MyWay; (R1 1.3); .NET CLR 1.1.4322)
Mozilla/4.0 compatible ZyBorg/1.0 (wn.zyborg@looksmart.net; http://www.lolyousuck.com)
Mozilla/4.0 (compatible; MSIE 6.0; Windows  NT 5.1; Q312461)
Lynx/2.8.4rel.1 libwww-FM/2.14 SSL-MM/1.4.1 GNUTLS/0.8.6
```

Many more fake User Agents, some of them with explicit language in them.

```
Usage: !email <server> <port> <from> <to> <attach>
SMTP sender started
Invalid SMTP port
SMTP: already started
email
UDP Flood terminated, sended: %d kbytes
UDP Flood is not started
udpfloodstop
UDP Flooder started
UDP Flood already started
Usage: udpflood <host> [port]
udpflood
SYN Flooding terminated
SYN Flood is not started
synfloodstop
Usage: synflood <host> <port>
SYN Flood started
SYN Flood already started
synflood
Process with PID %d killed
Unable to kill process with PID %d
Bad process ID
Usage: kill <PID>
kill
Found. NAME: "%s" PID: %d
```

```
HTTP Flooder terminated
HTTP Flooder is not started
httpfloodstop
HTTP Flooder started
HTTP Flooder: Bad port - %s
Usage: !httpflood <host> [port] [path_to_script]
HTTP Flooder already started
httpflood
```

```
Only IRC mode
reconnect
shutdown
ICMP Flooding terminated, sended: %d kbytes
ICMP Flood is not started
icmpfloodstop
nospoof
ICMP Flood started
ICMP Flood already started
Usage: !icmpflood <host> [nospoof]
icmpflood
Mode -o for %s
deop
I need message on channel instead of private
Mode +o for %s
Usage: !irc <string>
irc
Download is not started
Downloading terminated
getstop
Usage: !get <url> <local> [noexec]
noexec
```

```
%s(%d tasks)
%sNo active tasks
%s[%sBINDPORT%s %d%s]
%s[%sEMAILING%s]
%s[%sUDP FLOODING%s %s]
%s[%sSYN FLOODING%s %s:%d]
%s[%sHTTP FLOODING%s %s:%d]
%s[%sFTPD%s %d]
%s[%sSOCKS5%s %d]
%s[%sSOCKS4%s %d]
%s[%sDCCSHELL%s %s]
%s[%sDCC SENDING%s %s]
%s[%sDOWNLOADING%s %s]
%s[%sICMP FLOODING%s %s]
%s[Status]
```

The malware is capable of UDP, SYN, ICMP, and HTTP flooding, likely part of a botnet. Also mentions IRC, which could possibly be the C&C server

```
spoof_ip
Bad variable
set
%s...
echo
Logout for%s %s
logout
Access%s GRANTED%s for%s %s
You are already loggined as admin - %s %s
login
Not a command.
Parted from %s %s
Joined to %s %s
RegisterServiceProcess
```

Evidence that the malware can take a command.

Basic Dynamic Analysis

Regshot

```
ft\Windows\Shell\MuiCache\C:\users\austin\desktop\illusionbot_may2007\illusion_bot\botbinary.exe.FriendlyAppName: "botbinary"
s\Shell\MuiCache\C:\users\austin\desktop\illusionbot_may2007\illusion_bot\botbinary.exe.FriendlyAppName: "botbinary"
```

Adds the malware to the shell in the registry.

```
9EA}\Count\Zvpebfbsg.Jvaqbjf.Rkcybere:  00 00 00 00 05 00 00 00 2B 00 00 00 23
9EA}\Count\Zvpebfbsg.Jvaqbjf.Rkcybere:  00 00 00 00 05 00 00 00 2E 00 00 00 F1
9EA}\Count\P:\Hfref\nhfgva\Qrfxgbc\onfvp-qlanzvp\CebprffRkcybere\cebprkc64.rkr:
9EA}\Count\P:\Hfref\nhfgva\Qrfxgbc\onfvp-qlanzvp\CebprffRkcybere\cebprkc64.rkr:
9EA}\Count\P:\Hfref\nhfgva\Qrfxgbc\onfvp-qlanzvp\ertfubg\Ertfubg-k64-NAFV.rkr:
9EA}\Count\P:\Hfref\nhfgva\Qrfxgbc\onfvp-qlanzvp\ertfubg\Ertfubg-k64-NAFV.rkr:
```

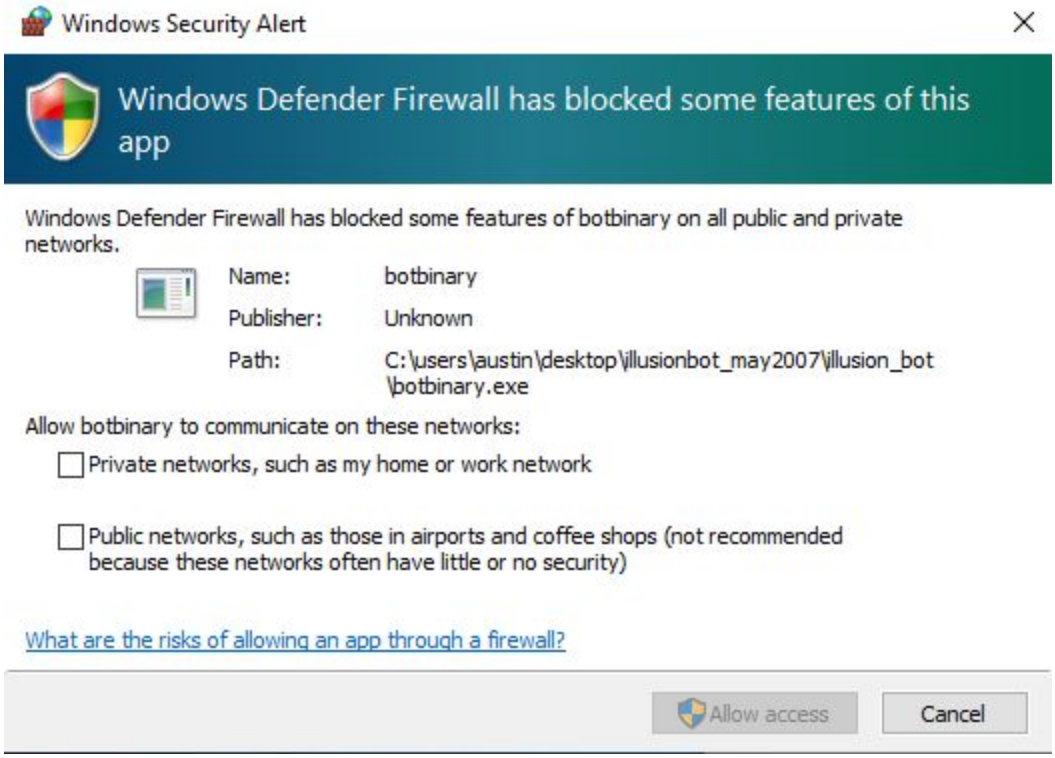
The values modified in the registry seem suspicious.

Process Explorer

BOTBINARY.EXE		1,812 K	6,432 K	1704

The malware runs in the background.

Exploration



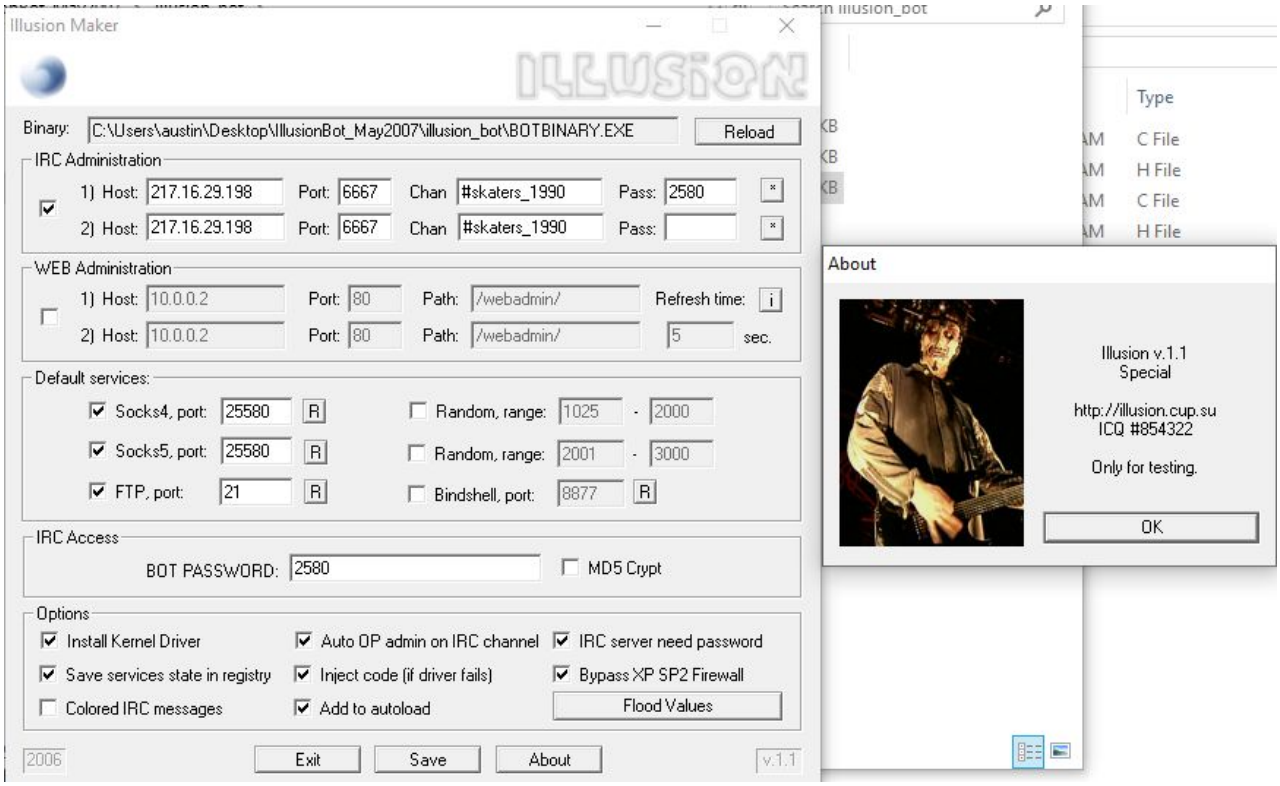
The malware requires an internet connection.

Name	Date modified	Type	Size
index.php	4/23/2006 2:31 AM	PHP File	59 KB
Man	4/23/2006 2:14 AM	HTML File	9 KB
Readme	4/20/2006 5:02 PM	HTML File	8 KB
updater.php	3/26/2006 11:24 AM	PHP File	3 KB

```
/* Online bots listing */
function db_list_bots()
{
        GLOBAL $mysql_host, $mysql_user, $mysql_password, $mysql_dbname, $mysql_bots_table, $refreshtime;
        if (!@mysql_connect( $mysql_host, $mysql_user, $mysql_password ))
        {
                print "<center><b>MySQL connection error</b></center>";
                return 0;
        }
        mysql_select_db( $mysql_dbname );

        $r = mysql_query( "SELECT * FROM $mysql_bots_table" );
```

The Zoo also provided a “web admin” page with the malware. Index.php contains references to a bot database. This page is likely used to manage the bots.



The build file allows users to edit settings, such as how the bots connect to the command server, and even what the command server is. This indicates that this bot server is for public use for whoever wants to download and use it.

Advanced Analysis

LoadLibraries

```
13144C5E loadLibraries proc near
13144C5E
13144C5E var_10= dword ptr -10h
13144C5E hModule= dword ptr -0Ch
13144C5E var_8= dword ptr -8
13144C5E var_4= dword ptr -4
13144C5E
13144C5E sub     esp, 10h
13144C61 push    ebx
13144C62 push    ebp
13144C63 push    esi
13144C64 mov     esi, ds:LoadLibraryA
13144C6A push    edi
13144C6B push    offset LibFileName ; "ws2_32.dll"
13144C70 call    esi ; LoadLibraryA
13144C72 push    offset ModuleName ; "kernel32.dll"
13144C77 mov     ebx, eax
13144C79 call    esi ; LoadLibraryA
13144C7B push    offset aUser32Dll ; "user32.dll"
13144C80 mov     edi, eax
13144C82 call    esi ; LoadLibraryA
13144C84 push    offset aAdvapi32Dll ; "advapi32.dll"
13144C89 mov     [esp+24h+hModule], eax
13144C8D call    esi ; LoadLibraryA
13144C8F push    offset aGdi32Dll ; "gdi32.dll"
13144C94 mov     ebp, eax
13144C96 call    esi ; LoadLibraryA
13144C98 push    offset aNtdllDll ; "ntdll.dll"
13144C9D mov     [esp+24h+var_10], eax
13144CA1 call    esi ; LoadLibraryA
13144CA3 push    offset aWininetDll ; "wininet.dll"
13144CA8 mov     [esp+24h+var_8], eax
13144CAC call    esi ; LoadLibraryA
```

The main function starts with loading many different libraries into the malware.

CheckWindowsVersion

```
00000000131458BE push    offset aWin2k   ; "Win2K"
00000000131458C3 jmp     short loc_131458EA
```

```
00000000131458CE push    offset aWinxp   ; "WinXP"
00000000131458D3 jmp     short loc_131458EA
```

```
00000000131458E5
00000000131458E5 loc_131458E5:
00000000131458E5 push    offset aWin     ; "Win???"
```

```
EAX   1315371C   "Win???"
EBX   00368000
ECX   131506A8   "Win???"
```

Afterwards, it checks for the Windows version. Since Windows 10 didn't exist in 2007, it chose "Win???".

```
1314CBB3   50                 push eax
1314CBB4   E8 735BFFFF        call botbinary.1314272C
1314CBB9   59                 pop ecx

ECX   131506D0   "Win98"
EDX   131506D3   "98"
```

For some reason, this function changed the detected Windows version as Win98, not sure if thats a bug or a feature.

editRegistry

```
00000000131410E5 editRegistry proc near
00000000131410E5
00000000131410E5 var_254= byte ptr -254h
00000000131410E5 var_154= byte ptr -154h
00000000131410E5 var_54= byte ptr -54h
00000000131410E5 var_1C= byte ptr -1Ch
00000000131410E5 var_C= dword ptr -0Ch
00000000131410E5 var_8= dword ptr -8
00000000131410E5 var_4= dword ptr -4
```

```
13141120   E8 584B0000        call botbinary.13145C7D
13141125   8D85 ACFEFFFF      lea eax,dword ptr ss:[ebp-154]
1314112B   50                 push eax                          eax:"C:\\WINDOWS\\system32\\drivers"
1314112C   8D85 ACFDFFFF      lea eax,dword ptr ss:[ebp-254]
```

```
13145C7D
13145C7D
13145C7D
13145C7D buildService proc near
13145C7D
13145C7D arg_0= dword ptr  4
13145C7D arg_4= dword ptr  8
13145C7D arg_8= byte ptr  0Ch
13145C7D
13145C7D mov     ecx, [esp+arg_0]
13145C81 push    esi
13145C82 push    1
13145C84 pop     eax
```

```
ESI   0019FBD4   "ntndis.exe"
```

```
BOTBINARY.E...   248   CreateFile   C:\Windows\SysWOW64\drivers\ntndis.exe   ACCESS DENIED
```

```
&"FBSGJNER\\Zvpebfbsg\\Jvaqbjf AG\\PheeragIrefvba\\Jvaybtba"
```

```
&"C:\\WINDOWS\\system32\\drivers\\ntndis.exe"
"Shell"
"Explorer.exe C:\\WINDOWS\\system32\\drivers\\ntndis.exe"
```

The editRegistry function adds ntndis.exe in the buildService function it calls. The malware creates this file in the drivers directory, or at least it attempted to. The string that looks like random characters was found earlier when doing regshot.

connectToServer

```
1314CAD4 loc_1314CAD4:
1314CAD4 call    sub_1314986C
1314CAD9 call    sub_13149982
1314CADE push    1
1314CAE0 call    connectToIRC
1314CAE5 push    esi
1314CAE6 call    connectToIRC
1314CAEB push    1
1314CAED call    connectToWebserver
1314CAF2 push    esi
1314CAF3 call    connectToWebserver
1314CAF8 add     esp, 10h
1314CAFB cmp     dword_1314D124, esi
1314CB01 mov     edi, offset connectForAttacks
1314CB06 jz      short loc_1314CB1D
```

```
13149A0E
13149A0E
13149A0E
13149A0E connectToIRC proc near
13149A0E
13149A0E arg_0= dword ptr  4
13149A0E
13149A0E push    esi
13149A0F mov     esi, [esp+4+arg_0]
13149A13 test    esi, esi
13149A15 mov     ecx, offset unk_1314D41C
13149A1A jnz     short loc_13149A21
```

```
3149A1C mov     ecx, offset unk_1314D3DC
```

```
1
1 loc_13149A21:
1 test    esi, esi
3 mov     eax, offset aIrcRserver ; "irc_rserver"
8 jnz     short loc_13149A2F
```

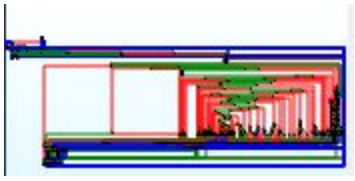
```
13149AB5
13149AB5
13149AB5
13149AB5 connectToWebserver proc near
13149AB5
13149AB5 arg_0= dword ptr  4
13149AB5
13149AB5 push    esi
13149AB6 mov     esi, [esp+4+arg_0]
13149ABA test    esi, esi
13149ABC mov     ecx, offset unk_1314D568
13149AC1 jnz     short loc_13149AC8
```

```
13149AC3 mov     ecx, offset unk_1314D528
```

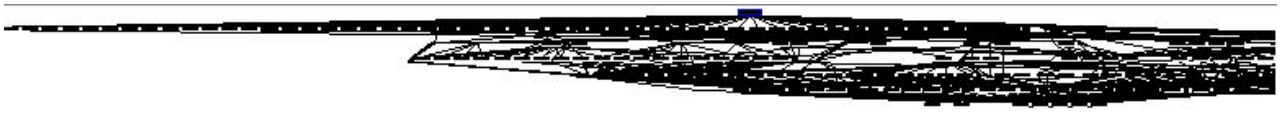
```
8
8 loc_13149AC8:
8 test    esi, esi
A mov     eax, offset aWebRserver ; "web_rserver"
F jnz     short loc_13149AD6
```

The first part determines whether to try to connect to a web server or IRC server. These functions do not connect to it, but sets up the port and IP, as well as the username, password, and channel (if using IRC).

connectForAttacks



This is the connectForAttacks function, pretty messy code from the looks of it. It contains all of the strings from earlier that mention flooding, so this function is what listens for commands.



This is the XRefs from the function, so at least it calls other functions to process the commands.

```
"217.16.29.198"
```

This is the IP that the malware tries to connect to, this was found earlier during the basic dynamic section.

```
13148D0E    FF15 AC391513    call dword ptr ds:[<&inet_addr>]
13148D14    6A 10            push 10
13148D16    68 90461713      push botbinary.13174690
13148D1B    FF35 88461713    push dword ptr ds:[13174688]
13148D21    A3 94461713      mov dword ptr ds:[13174694],eax
13148D26    FF15 34371513    call dword ptr ds:[<&connect>]
13148D2C    83F8 FF          cmp eax,FFFFFFFF
13148D2F    75 10            jne botbinary.13148D41
13148D31    FF35 88461713    push dword ptr ds:[13174688]
13148D37    FF15 E4361513    call dword ptr ds:[<&closesocket>]
```

```
(ERROR_SUCCESS)
(STATUS_NETWORK_UNREACHABLE)
```

The malware attempts to connect, finds that the network is unreachable, then closes the socket.

```
13149F64    FF15 FC361513    call dword ptr ds:[<&Sleep>]
13149F6A    E9 77FFFFFF      jmp botbinary.13149EE6
```

The malware then sleeps, looping around to try to connect again.

Challenges

One challenge I had was not being able to view any netcat traffic, even though I used the port I found in the build menu (6667). This is likely because of how I had even host-only turned off during testing. Since this malware doesn't *seem* like a worm, I possibly could have put it to host-only, but I didn't want any risk of turning my laptop into a botnet. Maybe one day I can try to make a closed VLAN of Virtual Machines and test out the webcontroller and try to DDoS another VM?

Summary

The malware I analyzed makes your PC part of a botnet. This can cause harm to your PC due to the internet usage of trying to connect, listen for commands, and carry out these attacks, as well as adding registry keys and attempting to add a new executable file in the background. This malware seems easy to remove, as it doesn't try to hide itself from Process Explorer or Task Manager. The

hardest part of removing this malware would probably be the fact that it changes registry keys. Luckily, this malware is fairly old and most AVs would be able to detect it.