

Hotline

---

contents

---

A-Applescript Trojans <lames...surrounding me...\$#@>

B-Social Engineering

D-The Hotline Socket

E-Making ToolBars

A

Trojans are probably the most boring, and easy to get caught may of hacking hotline. In result, it is the most popular. Most are made up of apple script, and given a name and an icon <i.e. the icon of a simple text document and named "my upload list">. The code of the script is pretty simple, and moves a user from the upoads folder into the users folder.

I have written a little bit of code to get you started.

Tell application "finder"

move file "guest " of folder "uploads" of folder "Files" of folder

"server folder"of folder "Hotline Server" of startup disk to

folder "Users" of folder "Server folder" of folder "Hotline Server"

of startup disk  
End tell

That will put the user data <that you created with "hotline user data editor", or any one program of that kind, and uploaded into the uploads folder>, and move it to the users folder. That user will be activated. The reason why you should call it "guest " is so that when the admin gets info on you, it will look like you're a guest <remember you put a space after guest>.

B

Social engineering is a lot of fun, especially when it's with clueless people. On hotline, they're easy to find. When you find your target server <most likely "Coolhakerz Super-De-Duper MacWarez Filez!!AOL RULES!!">, change your name and icon to something different than what you usually use. Go in, but be sure not to message anyone. Just look around. Is it a mac server? who hosts it? Is it not as lame as you expected? how old is it? Is a full priviled admin stupid? Read the news. Is it a banner server? All of those will help you out when talking to the admin.

Now, relogin with a new name and icon. Not the one you had before. Talk to the admin. This is the typical conversation I have when doing this:

You-"I think I can help out this server."

Him-"really? how???"

You-"Your security seems pretty weak. If I wanted to,

I could upload a self executable trojan to this server, and as we speak,

delete all your files from your hard disk, or make an admin account."

Him-"woa!!...what would you use?"

You-"Interware's new file-delete/creation system. It's pretty new, but I have

a bot that can detect it."

Him-"Can you u/l it???"

You-"No...it's still in beta. I will run it off my computer for you, though.

I would need an admin account to log it in with..."

Him-"Cool!!!l/p???"

You-<the l/p of your choice>

<after he completes the account, say thanks, then wait. After about two minutes,

talk to him again:>

You-The bot won't logon because it needs more privs. It needs a full admin."

Him-"oh..ok...sorry. Hold on"

<if he says no, and thinks some things up, do this:

You-"I can still run the bot, but you will have to do on-spot verification"

Him-"what's that?"

You-"I'll show you"

(now login with a new copy of HL Client. Have a simple Text document with answers to paste with i.e "Please enter a login and password under your command."

"That was an invalid command". Tell him to message your "bot" and test him out.

on the first message he sends, send him back the message "Please enter a login and password under your command.". On the second one, when he sends it, give him "That was an invalid command". If you get it, don't leave abruptly. Keep playing along. Tell him that you need to work on the bot and will be back in a while>

<if he does give you the login and pass, bring on the "bot" (another copy of HL

Client), and have a few messages ready to be copy/pasted out of simple text. Let him play with it a while. In a few minutes, quit that copy of HL Client. Tell him there was an error type one with the bot, and you need about a half an hour to go back over the code.>

Both outcomes

Go back on in a while with a guest user, and a new name and icon. If the admin is idle or gone, login with the admin l/p, and make an account "guest " <WITH THE SPACE>. Don't make him red or unkickable, but all other privs are there. If there is another admin there, login with the admin account/password, and change your name to the admin's. Tell him that he needs to leave "your" server alone, and delete his account. Then ban him. <only do that last part if ya want to get caught :P>

C

The hotline protocol's socket is fairly easily made in RB. I have supplied some code for a connect button. It is all the code you need to make the person running the HL Server get a "ba-bing" <the hit sound>. Play with it. All you need is a pushbutton, an editfield, and a socket.

```
if <ip address editfield>.text <> "" then
```

```
if inStr(<ip address editfield>.text,":")<> 0 then
```

```
<socket's name>.Address = nthField(<ip address editfield>.text,":",1)
```

```
<socket's name>.Port = val( nthField(<ip address editfield>.text,":",2) )
```

```
else
```

```
<socket's name>.Address = <ip address editfield>.text
```

```
<socket's name>.Port = 5500
```

```
end
```

```
end
```

```
<socket's name>.Connect
```

D

To make a tool bar, you need to make a new document in resedit. Make a pict and a HPTB 128 resource. You need to also open Hotline with resedit while you have the toolbar open and copy the TMPL resource. It is easier to start with a pre-made tool bar, and customize it to how you want it, but I will include the info if you want to start from scratch.

<copied from an unnamed text file I found>

"HPTB"

Set this field to "HPTB".

Version1

Set this field to 1.

sideTitleBar

If this is set to 1, the titlebar on the toolbar window will appear vertically on the left side of the window. If it is set to 0, it will appear at the top as normal. A side titlebar is good for a window that is wider than it is high.

toggleWinVis

If this is set to 1, the behavior for "showing" a window gets changed. If the window is hidden, it is shown in front of all others. If the window is visible, it is brought to the front. If it was already at the front, it gets hidden (normally it stays visible).

(reserved)

It is important that you leave these set to 0.

connectPict

The ID of the PICT to draw when Hotline is connected (or 0 for none).

connectPictR

The rectangle (top,left,bottom,right) in pixels to draw the "connectPict" at.

height

The height of the window in pixels.

width

The width of the window in pixels.

bkgndPict

The ID of the PICT to draw as the background into the window. This is the main picture — how the toolbar looks normally.

item bounds

The rectangle (top,left,bottom,right) in pixels that encloses this item. This rectangle is used to determine if the mouse is within the item, and is used to draw the "mDownPict" in the correct location.

item mDownPict

The ID of the PICT to draw while mouse is down in this item (while the button on the mouse is pressed and located within the bounds of this item).

item mWithinPict

The ID of the PICT to draw while mouse is in/over this item (while the mouse is located within the bounds of this item).

item mDownAction

The action to perform when the mouse goes down in this item (when the button on the mouse is pressed and located within the bounds of this item). See "Action Numbers" following for valid values.

item mUpAction

The action to perform when the mouse is released in this item (when the button on the mouse was pressed and has just been released within the bounds of this item). See "Action Numbers" following for valid values.

#### item mDownSound

When the button on the mouse is pressed over this item, play the sound ("snd ") of this ID. Note that if you add your own "snd " resources, the IDs must be in the range 1000 to 2000.

#### item mUpSound

When the button on the mouse is released over this item, play the sound ("snd ") of this ID. Note that if you add your own "snd " resources, the IDs must be in the range 1000 to 2000.

#### item showPicInWin

The ID of the PICT to show in a window with an OK button when this item is clicked. Good for credits etc.

#### mDownPictRct

Normally, the "mDownPict" gets drawn in the item bounds. You can optionally specify a different rectangle here.

#### mWithinPictR

Normally, the "mWithinPict" gets drawn in the item bounds. You can optionally specify a different rectangle here.

#### Action Numbers

- 0 = do nothing
- 1 = show options window
- 2 = show connect window
- 3 = disconnect
- 4 = show news window
- 5 = show post window
- 6 = show chat window
- 7 = show files window
- 8 = show user list window
- 9 = show tasks window
- 10 = quit
- 11 = show about window
- 12 = show new user window
- 13 = show open user window
- 15 = show tracker window