

Forum:[Hack Forums](#)

Thread: [\[MASM\] ArxLoader 1.0 - Ring3 Rootkit - FTP Grabber - Form Grabber](#)

z0tpyrk - November 30, 2013, 4:34 am

<https://hackforums.net/showthread.php?tid=3903182>

D??M! - November 30, 2013, 5:36 am

Hmm, something about that panel seems similar.

Internap. - November 30, 2013, 5:41 am

(Nov 30, 2013 06:36 AM)DOOM! Wrote: [\[CITE\]](#) Hmm, something about that panel seems similar. Was thinking the exact same thing lol.

betamonkey - November 30, 2013, 8:36 am

Oh look, a form grabber. Better remove that because of the elite banking powers it bestows upon its owner.

But really you need more than a 32 bit UUID. I'd go with at least 24 - 128 bits.

Bat™ - November 30, 2013, 8:51 am

Hmm, you are not doing any good with editing the images lol

This

[img]<http://img534.imageshack.us/img534/9110/ns40.png>[/img]

And then this :

Looks legit :)

Breezo - November 30, 2013, 9:27 am

(Nov 30, 2013 09:51 AM)Bat™ Wrote: [\[CITE\]](#) Hmm, you are not doing any good with editing the images lol

This

[img]<http://img534.imageshack.us/img534/9110/ns40.png>[/img]

And then this :

Looks legit :)

It is not done yet, it is still in early stages of development so no need hate.

- Hugs

Bat™ - November 30, 2013, 9:30 am

(Nov 30, 2013 10:27 AM)Hugs Wrote: [\[CITE\]](#)

It is not done yet, it is still in early stages of development so no need hate.

- Hugs

I'm not hating just adding some light to the posts #2 and #3 :)

z0tpyrk - November 30, 2013, 9:33 am

(Nov 30, 2013 09:51 AM)Bat™ Wrote: [\[CITE\]](#) Hmm, you are not doing any good with editing the images lol

This

[img]http://img534.imageshack.us/img534/9110/ns40.png[/img]

And then this :

Looks legit :)

It's because i didn't finished the SQL Query yet on connections.

KFC Watermelon - November 30, 2013, 9:36 am

(Nov 30, 2013 06:36 AM)DOOM! Wrote: [\[CITE\]](#) Hmm, something about that panel seems similar. Another bootstrap based UI, right?

(Nov 30, 2013 09:36 AM)betamonkey Wrote: [\[CITE\]](#) Oh look, a form grabber. Better remove that because of the elite banking powers it bestows upon its owner.

But really you need more than a 32 bit UUID. I'd go with at least 24 - 128 bits.

Was thinking the same thing. Are you planning on selling a watered down version of Beta Bot or something any time?

betamonkey - November 30, 2013, 9:44 am

(Nov 30, 2013 10:36 AM)KFC Watermelon Wrote: [\[CITE\]](#) Another bootstrap based UI, right?

Was thinking the same thing. Are you planning on selling a watered down version of Beta Bot or something any time?

It doesn't matter. Omni said it's not allowed in any shape or form here. Evidently it has nothing to do with the form grabber. Basically if any shit here gets enough attention he will just ban it. You would think blackshades or basically -all- the booters would be banned under that principle but I imagine that has something to do with money.

Bat™ - November 30, 2013, 10:25 am

(Nov 30, 2013 10:44 AM)betamonkey Wrote: [\[CITE\]](#) It doesn't matter. Omni said it's not allowed in any shape or form here. Evidently it has nothing to do with the form grabber. Basically if any shit here gets enough attention he will just ban it. You would think blackshades or basically -all- the booters would be banned under that principle but I imagine that has something to do with money. Yes, its only the money which plays game here.

Don't you know how TOW's proof thread of blackshades being backdoored was closed? Money!!!

J?ck - November 30, 2013, 11:07 am

(Nov 30, 2013 09:36 AM)betamonkey Wrote: [\[CITE\]](#) Oh look, a form grabber. Better remove that

because of the elite banking powers it bestows upon its owner.

But really you need more than a 32 bit UUID. I'd go with at least 24 - 128 bits.
Oh you.

(Nov 30, 2013 06:36 AM)DOOM! Wrote: [\[CITE\]](#) Hmm, something about that panel seems similar. I know what you're saying, but usually design in products in malware isn't exactly looked upon. So it's going to look similar.

D??M! - November 30, 2013, 12:27 pm

Out of curiosity @OP and/or Hugs... Who here do you have that knows how to code all of this in ASM? I'm not fond of bots that have the potential to be game changing posting no information whatsoever. Right now, until you do, you're on the same level as the Batman Botnet (Dark Knight Bot or whatever that retard named it).

(Nov 30, 2013 11:25 AM)Bat™ Wrote: [\[CITE\]](#) Yes, its only the money which plays game here. Don't you know how TOW's proof thread of blackshades being backdoored was closed? Money!!! To be fair, I was running Blackshades at the time and even now, fighting with most anyone still involved there, I can say BS never paid anyone off on HF to do shit for us. I tried, I offered multiple staff members including Omni cash to do various things for us, and never did they accept my offers.

(Nov 30, 2013 12:07 PM)J?ck Wrote: [\[CITE\]](#) I know what you're saying, but usually design in products in malware isn't exactly looked upon. So it's going to look similar. I haven't use it in a while, but I wasn't fond with how similar looking it is to Beta Bot. I suppose you can only get so innovative with Bootstrap though.

betamonkey - November 30, 2013, 3:28 pm

(Nov 30, 2013 12:07 PM)J?ck Wrote: [\[CITE\]](#) I know what you're saying, but usually design in products in malware isn't exactly looked upon. So it's going to look similar. Well I didn't copy any designs for my bot's panel. As I always say, HF has a major creativity issue on just about every level.

At any rate, besides the UUID thing, these kinds of bots should really not be coded in Assembly. It's overly complex and much more likely to produce complications. Unless you are a professional with the time and know-how to invest, you're just asking for problems.

[H]ell - November 30, 2013, 3:32 pm

(Nov 30, 2013 06:36 AM)DOOM! Wrote: [\[CITE\]](#) Hmm, something about that panel seems similar. It's called bootstrap. Something used by thousands of sites because it makes cuts the design time down a ton. For a bot like this, you don't wanna spend time designing a panel.

m4dh4ck3r - November 30, 2013, 3:42 pm

(Nov 30, 2013 10:36 AM)KFC Watermelon Wrote: [\[CITE\]](#) Another bootstrap based UI, right?

Was thinking the same thing. Are you planning on selling a watered down version of Beta Bot or something any time?

Bootstrap based interfaces are way better than ripped off themeforest templates.

[H]ell - November 30, 2013, 3:51 pm

(Nov 30, 2013 04:28 PM)betamonkey Wrote: [\[CITE\]](#) Well I didn't copy any designs for my bot's panel. As I always say, HF has a major creativity issue on just about every level.

At any rate, besides the UUID thing, these kinds of bots should really not be coded in Assembly. It's

overly complex and much more likely to produce complications. Unless you are a professional with the time and know-how to invest, you're just asking for problems.

Saying bootstrap is copying code is the same as saying that using cakePHP or Symphony is for skiddies. It cuts time on basic development tasks.

Other than that, I completely agree on the fact that MASM is extremely inefficient for a project like this. We created higher level languages like C , C++ etc.. These languages all compile to binary code. Which is the same thing MASM does. There's nothing wrong with using C or C++. Only for optimization it's smart to use MASM.

J?ck - December 1, 2013, 4:08 am

(Nov 30, 2013 04:28 PM)betamonkey Wrote: [\[CITE\]](#) Well I didn't copy any designs for my bot's panel. As I always say, HF has a major creativity issue on just about every level.

At any rate, besides the UUID thing, these kinds of bots should really not be coded in Assembly. It's overly complex and much more likely to produce complications. Unless you are a professional with the time and know-how to invest, you're just asking for problems.

No you didn't copy anyone's panel, but there's only so many things you can do with bootstrap without getting heavily involved. Most of the time, panels have offline/online aspects of bots on the left. Table of bot information on the right covering most of the page, and navigation on the top.

I do agree though, HF members aren't always the most creative with their products.

WHBmen - December 1, 2013, 7:46 am

nice, add filesearch list in tasks.

z0tpyrk - December 2, 2013, 7:01 am

(Dec 1, 2013 08:46 AM)WHBmen Wrote: [\[CITE\]](#) nice, add filesearch list in tasks.

Tell me why this should come in handy for people?

Bull™ - December 2, 2013, 7:38 am

I have did some reserch and found the OP has multiple account on HF .

His Other profile is : <https://hackforums.net/member.php?action=profile&uid=1007026>

Just watch both profiles and you have got lot of simlarties.

Edit : I can bet he is using a window RDP with a static IP.

D??M! - December 2, 2013, 10:17 am

(Dec 2, 2013 08:38 AM)Bull™ Wrote: [\[CITE\]](#) I have did some reserch and found the OP has multiple account on HF .

His Other profile is : <https://hackforums.net/member.php?action=profile&uid=1007026>

Just watch both profiles and you have got lot of simlarties.

Edit : I can bet he is using a window RDP with a static IP.

If you're correct, it'll make a lot of sense.

J?ck - December 2, 2013, 10:18 am

Things have just got interesting...

z0tpyrk - *December 2, 2013, 10:23 am*

Fenix, is a dutch friend of mine.

We started this Project a long time ago if i still have the PM's from it but he never came online again.