

Forum:[Hack Forums](#)

Thread: [\[Stop infections on members\]Lets stop users from binding shit to our programs \[Protect your programs\]](#)

Orgy - July 16, 2010, 1:36 am

While thinking of shit to do for twBooter v3, I was worried the free version might get binded to some malware and then distributed by third parties trying to get infections.

Then I thought of a solution.

I thought that twBooter's initial security check could run an md5sum of itself, and if the md5sum doesn't match up, it could display a message such as:

THIS VERSION OF TWBOOTER IS BACKDOORED.
PLEASE VISIT THE HJT SECTION OF HACKFORUMS AND POST YOUR HJT LOGS TO CLEAN YOUR SYSTEM.
THEN PLEASE VISIT THIS LINK TO DOWNLOAD A CLEAN VERSION: <http://linkhere>

Now what if we all started doing this with all of our programs?

EDIT: I just thought of this, but this would also make it more difficult to crack.

D??M! - July 16, 2010, 1:37 am

Hackforums would be a much better, and much cleaner, place.

Good idea.

Oreos - July 16, 2010, 1:38 am

That's actually kinda smart. There wouldn't be a way to bypass it without the source, right.? It would be pretty damn hard to do it by hex editing.

Mongrel - July 16, 2010, 1:41 am

I totally agree.. They'll do what-ever they can to out-smart us

Orgy - July 16, 2010, 1:45 am

You know, I didn't think of this before, but this would also make it more difficult to crack.

Oreos - July 16, 2010, 1:48 am

(Jul 16, 2010 01:45 AM)Orgy Wrote: [\[CITE\]](#) You know, I didn't think of this before, but this would also make it more difficult to crack.

That's true. A patch wouldn't work because it would change the code, and the md5, thus it would fail the md5 check.

Your coming up with a lot of great ideas today orgy=D

Robbie - July 16, 2010, 1:50 am

Great idea dude. You might have just saved many computers with this idea. ?

Orgy - July 16, 2010, 1:50 am

Hehe. Thanks :) I've finally had some time to myself to think after a few days.

MasterChafe - July 16, 2010, 1:52 am

This is a good idea but the skids dude.... make it 120 second boot every 2 days

Orgy - July 16, 2010, 1:54 am

(Jul 16, 2010 01:52 AM)MasterChafe Wrote: [\[CITE\]](#) This is a good idea but the skids dude.... make it 120 second boot every 2 days

Lol wrong thread buddy. You meant the other one.

botnous - July 16, 2010, 1:57 am

Woa man thats a pretty smart idea.Way to think outside the box.

pushl %ebp - July 16, 2010, 2:00 am

This is a really good idea. This function could be seperated by a class so that it can't run another function too.

But, what if someone cracks the source and then they could cancel that part out. What really needs to be done is more awareness spread about the real MD5 and then people could manually check it.

Orgy - July 16, 2010, 2:03 am

(Jul 16, 2010 02:00 AM)h4ckingURLife Wrote: [\[CITE\]](#) This is a really good idea. This function could be seperated by a class so that it can't run another function too.

But, what if someone cracks the source and then they could cancel that part out. What really needs to be done is more awareness spread about the real MD5 and then people could manually check it.

Well if you protect your program enough, you shouldn't have to worry about it being canceled. But if they DID cancel that part out somehow, they'd probably not tell their victims about the MD5. Or if they did, they'd give them the wrong MD5

`00Synch_ - July 16, 2010, 2:09 am

Great idea. It'd be nice if members weren't trying to cause harm to peers reaching towards a common goal.

Great Prosperity - July 16, 2010, 2:24 am

People can still replicate the md5 checksum.

I remember when getting hacks for Gunz I always used a program that made the checksum the exact same as the original file so that the hack will work.

Also instead of finding an idea of making real money. Ppl apparently like to cause others misery with lame ddos tools that don't even benefit yourself.

Orgy - July 16, 2010, 2:27 am

(Jul 16, 2010 02:24 AM)Spikeye Wrote: [\[CITE\]](#) People can still replicate the md5 checksum.

I remember when getting hacks for Gunz I always used a program that made the checksum the exact same as the original file so that the hack will work.

Also instead of finding an idea of making real money. Ppl apparently like to cause others misery with lame ddos tools that don't even benefit yourself.

Sure there are ways to circumvent it, but it would stop a LOT of users that don't know shit about that, that would just bind their plague bots or rxbots to it

Fallenbot - July 16, 2010, 2:32 am

Thats good idea.

I agree with you.
Better hackforums,more safer... :)

Orgy - July 16, 2010, 8:21 am

Bumping this up. Anyone else got an opinion?

RBH - July 16, 2010, 9:05 am

This is a really good idea,
i did created 2 functions to do this in vb.net
posted here:
<https://hackforums.net/showthread.php?tid=545912>
ofcourse with you credits ;)

Orgy - July 16, 2010, 9:23 am

(Jul 16, 2010 09:05 AM)I am a Pirate! Wrote: [\[CITE\]](#) This is a really good idea,
i did created 2 functions to do this in vb.net
posted here:
<https://hackforums.net/showthread.php?tid=545912>
ofcourse with you credits ;)
Now if only people would realize that its not just for application protection. It makes it harder to
crack, and makes it harder to bind shit to it

bblokar - July 16, 2010, 11:26 am

GENIUS. SIMPLY GENIAL IDEA.

DEN1AL - July 16, 2010, 11:36 am

thats a great idea!

no cracks,infections clean files:)

TeemoProd - July 16, 2010, 12:18 pm

Going to work on this for my Booter now, thanks Orgy!

fads23 - July 16, 2010, 12:44 pm

Can you explain the implementation? If I want to add this, how would I know what hash to but in the
source if I didn't compile the program yet? :O

Orgy - July 16, 2010, 12:57 pm

(Jul 16, 2010 12:44 PM)Chad.Gomes Wrote: [\[CITE\]](#) Can you explain the implementation? If I want to
add this, how would I know what hash to but in the source if I didn't compile the program yet? :O
Simple. You check it AFTER compilation, and then store it in a database or .txt file on your server
somewhere, and have it compare with that

Diabolic - July 16, 2010, 12:58 pm

Yeah, This is an awesome idea.. Well done!

dylanups - July 16, 2010, 1:03 pm

Awesome idea could save alot of people :)

[EPIC] LOL [EPIC] - July 16, 2010, 1:24 pm

Great idea tbh :D

And, free version of twBooter? Wut? :D

Orgy - July 16, 2010, 9:55 pm

Yeah, free version of twBooter ;)

jam3s - July 16, 2010, 10:42 pm

lol at all the kiddies thinking this is revolutionary/unique/THE FIRST EVER.

@Orgy: How much brain capacity did this idea require?

????????™ - July 16, 2010, 11:01 pm

very good idea in my opinion and if this could be applied to apps in future releases it will make alot of us feel safer

Contend - July 16, 2010, 11:26 pm

By the time they open it, they will already be infected.

Meep - July 16, 2010, 11:35 pm

This would be a such better idea, please keep infecting me when they say they're helping me out

Zach - July 17, 2010, 12:44 am

Orgy, you could simply make it a website based, and not program based.

South Park - July 17, 2010, 12:47 am

Woah, great idea, I think I'm going to implant this in the future versions of my products. Great idea.

Orgy - July 17, 2010, 12:55 am

(Jul 17, 2010 12:44 AM)Zach Wrote: [\[CITE\]](#) Orgy, you could simply make it a website based, and not program based.

Website based? What are you on about

Zach - July 17, 2010, 1:03 am

(Jul 17, 2010 12:55 AM)Orgy Wrote: [\[CITE\]](#) Website based? What are you on about

Buy hosting, open a website.

Give the users the url for a test, code it to blacklist IP's or some shit after 1 attempt to dos.

Basically, you know what a regular shell looks like? Create one and when someone dos's it commands the other 250 shells or however many you have.

Orgy - July 17, 2010, 1:09 am

(Jul 17, 2010 01:03 AM)Zach Wrote: [\[CITE\]](#) Buy hosting, open a website.

Give the users the url for a test, code it to blacklist IP's or some shit after 1 attempt to dos.

Basically, you know what a regular shell looks like? Create one and when someone dos's it commands the other 250 shells or however many you have.

What in the hell are you talking about?

Zach - July 17, 2010, 1:14 am

(Jul 17, 2010 01:09 AM)Orgy Wrote: [\[CITE\]](#) What in the hell are you talking about?

This is stressing me out.

Okay, Orgy, instead of making a client, why don't you consider coding a website that can command all of your shells you own.

Think of it like this.

I'm on a shell site, do you know what a shell site typically looks like?

So, create a shell site, this shell site Orgy will command all of the shells you list, for example, lets say you own 10 shells.

When the person clicks enter, it commands your shells to attack that site.

1 website that commands all of your shells to attack a IP, like a webpanel.

Remember when you made that webversion? The free thing would be just like that, but it commands all of your shells IP's.

You could code it to not allow the same IP to attack over and over.

Orgy - July 17, 2010, 1:22 am

That has nothing to do with this thread.

thedankestmeme - July 17, 2010, 2:37 am

[img]http://ex0.in/s/0bc781a34b63acd1c6414df2b0dd33e1.PNG[/img]

hyperstream - July 17, 2010, 2:41 am

Encrypt the MD5 string(s)

bblokar - July 17, 2010, 3:26 am

(Jul 17, 2010 02:37 AM)manipulate Wrote: [\[CITE\]](#)

[img]http://ex0.in/s/0bc781a34b63acd1c6414df2b0dd33e1.PNG[/img]

Implying an average hackforums user has enough mental capabilities to use a hex editor.

thedankestmeme - July 17, 2010, 3:31 am

(Jul 17, 2010 03:26 AM)bblokar Wrote: [\[CITE\]](#) Implying an average hackforums user has enough mental capabilities to use a hex editor.

Implying that, in reality, averages are the only thing that matter.

xvisceral - July 17, 2010, 4:51 am

(Jul 17, 2010 02:41 AM)hyperstream Wrote: [\[CITE\]](#) Encrypt the MD5 string(s)

Needs to be a strong encryption, or it's basically useless.

I think I may implement a MD5 check on Blackshades... I don't think it is necessary, but it's worth a try

Gpizzle - July 17, 2010, 6:19 am

Yes it is a great idea, but what makes you think it will stop people?

jam3s - July 17, 2010, 9:38 am

(Jul 16, 2010 11:26 PM)Contend Wrote: [\[CITE\]](#) By the time they open it, they will already be infected.
+1 ? Correct answer.

fads23 - July 17, 2010, 10:00 am

(Jul 16, 2010 12:57 PM)Orgy Wrote: [\[CITE\]](#) Simple. You check it AFTER compilation, and then store it in a database or .txt file on your server somewhere, and have it compare with that

If you store it in a server somewhere, it can be easily spoofed by tracking outgoing connections.

(Jul 16, 2010 11:26 PM)Contend Wrote: [\[CITE\]](#) By the time they open it, they will already be infected.

+1 surprised no one thought of it lol

Orgy - July 17, 2010, 10:50 am

(Jul 17, 2010 10:00 AM)Chad.Gomes Wrote: [\[CITE\]](#) If you store it in a server somewhere, it can be easily spoofed by tracking outgoing connections.

(Jul 16, 2010 11:26 PM)Contend Wrote: [\[CITE\]](#) By the time they open it, they will already be infected.+1 surprised no one thought of it lol
So encrypt the connection.

And I've already thought of that. Hence why the program would ask them to go to the HJT section.

Teh Wallhacks™ - July 17, 2010, 12:17 pm

This is a Great Idea
We should do it

Orgy - July 26, 2010, 1:29 am

(Jul 17, 2010 12:17 PM)Teh Wallhacks™ Wrote: [\[CITE\]](#) This is a Great Idea
We should do it
Yep. Planning to. We'll see how it goes

Sautéed - July 26, 2010, 6:37 am

I agree with this. But then it might be harder since you have to somehow put the MD5 into the source and then recompile the app without changing the MD5... That will be hard.

Orgy - July 26, 2010, 6:44 am

(Jul 26, 2010 06:37 AM)Hackzee Wrote: [\[CITE\]](#) I agree with this. But then it might be harder since you have to somehow put the MD5 into the source and then recompile the app without changing the MD5... That will be hard.

Simple. Make it retrieve the MD5 from a file on your server.

Sautéed - July 26, 2010, 7:16 am

But you have to incorporate it into the program itself right? Doesn't that mean that if you get the original file's MD5, and then you put it into your program, and then you compile the program, the MD5 will change? I think that everytime you compile it, it will change the MD5 of the file.

Orgy - July 26, 2010, 7:19 am

No listen.

You do something like

```
string programHash;  
programHash = (contents of http://website.com/md5.txt)
```

Then you dont have to recompile it. It's dynamic

Error 403 - forbidden - July 26, 2010, 7:52 am

very smart idea every1 should do this

I am fool - July 26, 2010, 9:14 am

Incorporating it into Carbon Booter as we speak.

Orgy - July 26, 2010, 9:15 am

(Jul 26, 2010 09:14 AM)Carbon Wrote: [\[CITE\]](#) Incorporating it into Carbon Booter as we speak. Afterwards, test it out, and tell me if it works properly

watinator - July 26, 2010, 9:37 am

this isn't anything new... however, it's nice to see HF has caught on

aadster - July 26, 2010, 9:55 am

Good idea, would be simple to incorporate. Only problem would be if it were unpacked and ran, the md5 might not change.

Server.cfg - July 26, 2010, 12:59 pm

Good ideal Orgy. This will stop alot of people from infecting other users.

Taserz - July 26, 2010, 1:00 pm

not rilly i can change an md5 to anything lol make a test app and tell me what to make the md5 after reading the thread you people are bassicly saying you cant change the md5 to what you want which is wrong i can do it easily

Bawss - July 26, 2010, 1:12 pm

lol orgys sig =] and yes cracking needs to stop

Taserz - July 29, 2010, 1:13 pm

but this is still fail method since it can easily be changed

_umadlol - July 29, 2010, 2:09 pm

And also, it doesn't stop them from executing it, it will still run the binded program. There is no way to stop the binded program from running.

-na.Talish - July 29, 2010, 2:15 pm

This is what PixelRat does to avoid cracking.

IllusionSlayer - July 29, 2010, 2:58 pm

All they'd have to do is bind it and then null our your error message.

Orgy - July 29, 2010, 4:39 pm

(Jul 29, 2010 02:58 PM)IllusionSlayer Wrote: [\[CITE\]](#) All they'd have to do is bind it and then null our your error message.

>Implying the basic downloaded binders would be able to do that

IllusionSlayer - July 29, 2010, 7:01 pm

>implying you would use a binder to null a message.

Orgy - July 29, 2010, 9:10 pm

>Implying the average skid would have the tools to null a message

Poppins - July 30, 2010, 5:11 am

Thats a good idea but:

How would you grab the premade MD5 checksum? As soon as you enter the current checksum it will change.

Orgy - July 30, 2010, 5:13 am

(Jul 30, 2010 05:11 AM)Poppins Wrote: [\[CITE\]](#) Thats a good idea but:
How would you grab the premade MD5 checksum? As soon as you enter the current checksum it will change.

Third time I'll answer this:

Store it on a .txt file on a server, and have it read from there

Sautéed - July 30, 2010, 5:23 am

(Jul 26, 2010 07:19 AM)Orgy Wrote: [\[CITE\]](#) No listen.

You do something like

```
string programHash;  
programHash = (contents of http://website.com/md5.txt)
```

Then you dont have to recompile it. It's dynamic
Oh ok haha. Good idea. But then people might try to crack it..

johnno2932 - July 30, 2010, 5:31 am

this is not even a new idea lol

never heard of crc-32 checksum checker?

most installers have this option :)

still can be cracked easy... no use

Poppins - July 30, 2010, 5:44 am

(Jul 30, 2010 05:13 AM)Orgy Wrote: [\[CITE\]](#) Third time I'll answer this:

Store it on a .txt file on a server, and have it read from there
Ahh okay gotcha. Sorry I didn't read through 8 pages. I just read the first post.

DigitalDesire - July 30, 2010, 12:54 pm

wow, this is a really good idea. It's surprising no one has thought of this before.
This would certainly help save a lot of reputations.

4ChanIsHere - February 20, 2015, 11:44 pm

Orgy is right!!
Please stop infecting our memebbers

Private Network - February 21, 2015, 3:57 am

(Feb 21, 2015 12:44 AM)4ChanIsHere Wrote: [\[CITE\]](#) Orgy is right!!
Please stop infecting our memebbers
-1 Prestige and gravedigging threads, love you
Not