

Forum:[Hack Forums](#)

Thread: [FAQ || READ THIS BEFORE POSTING](#)

0x03a8 - October 6, 2014, 5:25 am

[img]http://s28.postimg.org/xzd648w7h/HF_FAQ.png[/img]

This thread is still WIP

Feel like we're missing stuff?

Can you do better?

PM me about it, we will gladly add your parts!

Index:Post 1 -> Introduction (Why create it)

Post 1 -> Index

Post 2 -> [Hack forums and basic things to know](#)

Post 3 -> [Anonymity \(by Niely\)](#)

Post 4 -> [Password Security, Hashes & Hash Cracking](#)

Post 5 -> [DDoS](#)

Post 6 -> Rats, Bots, Worms - Uses and Removal

Post 6 -> Virus crypting

Post 7 -> [Coding](#)

Post 8 -> Link to useful threads, tutorials and more

Who Created This?[Niely](#)

Anonymity

[0x03a8](#)

Index

First paragraph of Anonymity

Password Security, Hashes & Hash Cracking

DDoS

Rats, Bots, Worms - Uses and Removal

[TeamScreamHD](#)

Helped Post

[Xehoil](#)

Created GFX

Why create this thread? Why oh why you might wonder. The answer is simple.
Because you are an idiot! There, I said it. I know it might sound rude but it's probably true.

The thing is that the same questions appear EVERYWHERE EVERY TIME!
A single tutorial won't help!
A Helpdesk won't help!

People will keep asking the same questions and I think it won't stop for a long time.
This is why I thought up this. To increase the quality of ALL HF users posting in the beginner hacking section.

<https://gyazo.com/2cb0bfc6b5cf81d9957acd6e7060b553.png>

These questions can be answered by just reading all of this!

So stupid, that's why I'm changing stuff by doing this.
THE QUALITY OF THE AVERAGE HF USER NEEDS TO INCREASE!!!
People should be linked to this thread when asking the stupid same questions every time.

Please post below what you thought, if you have questions, if things are unclear let me know.

?Pozdrav - October 6, 2014, 7:46 am

How to stay anonymous?

The most important topic we discuss is anonymity.

A basic thing about anonymity is making sure other's can't track you. This all starts with your username.

Make sure you only use that username for things related to hacking, make sure you don't post that username anywhere else.

People can use that to dox you and using that, retrieve information about you.

It's also important to watch out with usage of passwords with some things.

You can use the same password for hackforums, gmail, hotmail. All fine. But watch out with a

booter / stresser.

Chances are the owner will release the info or use it for malicious reasons. These chances exist, but it's more likely

that the booter / stresser get's hacked by a 3rd party. In that case, the database is dumped and your hashes are free to be cracked.

That's why we will discuss password security & Hash encryption / Decryption as well in this FAQ

The three top methods to stay anonymous are: Proxies, VPN, and Tor.

Proxies: You can configure your browser to use a proxy. A proxy is actually a computer (server) between you, and the website where you connect to.

A normal connection goes like this: you > ISP > Website; with a proxy: you > ISP > Proxy-server > Website.

That makes that the website sees the IP of the website, and not yours one.

Firefox > Preferences > Advanced > Network > Settings use proxy (to use a proxy in your browser).

People post daily proxies in this section:

[VPN, Proxies, and Socks](#)

VPN: A Virtual Private Network works kind of the same as a proxy, the only difference is that a proxy only covers the application using the proxy, and not all the other traffic. A VPN secures your whole traffic!

Often VPN also encrypts your traffic for your ISP.

[censored] is a good free VPN.

Tor: The Onion Router is in my opinion the best way to stay anonymous.

Unlike a proxy and VPN, it does originally don't keep logs.

Of course there are some servers who try to log your info and decrypt it, but it's unlikely that will work out for them.

Tor originally works like this(kiss)

You > ISP > Tor-server 1 > Tor-server 2 > Tor-server 3 > Tor-server ... > Website

Multiple encryptions, multiple servers between you and the website,...

Tor also has some extra features and things you should know.

Tor encrypts your traffic even before it reaches the ISP (like as by a VPN - sometimes), so no one can view it.

Best of all, almost every Tor user gets an unique algorithm/key for that encryption, so it's almost impossible to crack.

Tor often switches it's path (changes the server between the first and last node).

If people are able to crack the first server, they only know who has used it, but not what you've done. If they crack the last server (exit node) they know what you're doing, but not who's doing it.

This is a small compensation of a VPN and Tor:

Specs || VPN | Tor

Logs: || Yes | No

Speed: || Fast | Bit Slower

Safety: || Low | High

Encryption: || Yes | Yes, multiple

Servers: || 1 | multiple

Price: || most paid | Free

Why people think Tor isn't safe:

"NSA logs who download Tor" - Use a proxy while downloading.

"Tor servers keep logs" - Not true, only a few who are controlled by the NSA. And if they keep logs it's unlikely they can decrypt your data, if they can decrypt it they only know what you're doing (request you send to websites etc), not who it is doing (you're location is still safe).

"Tor browser is back-doored" - It's open-source, disable JavaScript + route your data through the original Firefox then.

"Tor can get cracked" - View all answers above + only version 2.2 was known to be able to get cracked.

How to search for answers?

This may seem an idiot question, but it isn't!

Some people really don't know how to use Google, or the search function on HackForums.

Let me first show you a bit on how to search on Google.

Google: First of all, don't use Google! It's a damn anti-privacy company.

We will use another Search Engine instead, Startpage.

Startpage gives the same results as Google (based on Google); but it has taken out the logs and track methods the original Google delivers.

<http://startpage.com>

Search results are based on keywords, keywords are small words who describe what you want; it's easier as you may think.

If I for example want to look-up how to do cookie-stealing, I just type:

Cookie-stealing

Or

How to do Cookie-stealing

If you want to get more info about cookie-stealing, Wikipedia is probably the website we want to be looking on.

An easy to get Wikipedia results is by just typing Wikipedia is keyword:

Cookie-stealing Wikipedia

And there your result comes up.

Another way is by using Dorks, with a dork you specify what result should come up, anything not matching that; should come up.

Example:

Cookie-stealing inurl:wikipedia.org

And you'll get a really specific result.

Another dork I want to show, is searching for free e-books!

It's one of my favourite ways.

Our search-query would look like this:

pdf: C++ fundamentals

pdf: malware removal guide

pdf: start with ethical hacking

pdf: How to do SQLi

...

And you get thousands, and thousands of free e-books!

On Hackforums:

<https://hackforums.net/search.php>

You have to work with very selective and descriptive keywords, for more specified results choose the section as well.

Here you can search for members:

<https://hackforums.net/memberlist.php>

Sort by: username

May be more interesting as joining date. :)

How to spoof or crypt a file?

If you want to spread malware, spoofing and crypting are essential parts. Let me first explain some terms:

Spoofing: Faking an extension from a file, but keep that file acting like it's original extension.

Converting: Making a file extension, act like another file extension, so it actually changes type.

Crypting: Making a file FUD/UD for protection tools (like: Anti-Viruses, Anti-Malware,...).

FUD: Fully UndetectAble - No protection tools don't detect the malware, not when downloading nor when running.

UD: Only a few protection tools don't detect it, and only in few cases.

Anyway, all of these processes can easily be done by using tools.

Search Hackforums for "Free spoofer" for example.

In the Cryptography section and Hacking Tools and Programs section you can also find thousands of these tools.

If these all are done right, your victim gets infected with your malware.

0x03a8 - October 6, 2014, 7:46 am

[img]http://s28.postimg.org/8kj8l87il/How_to_stay_anonymous.png[/img]

The most important topic we discuss is anonymity.

A basic thing about anonymity is making sure other's can't track you. This all starts with your username.

Make sure you only use that username for things related to hacking, make sure you don't post that username anywhere else.

People can use that to dox you and using that, retrieve information about you.

It's also important to watch out with usage of passwords with some things.

You can use the same password for hackforums, gmail, hotmail. All fine. But watch out with a booter / stresser.

Chances are the owner will release the info or use it for malicious reasons. These chances exist, but it's more likely

that the booter / stresser get's hacked by a 3rd party. In that case, the database is dumped and your hashes are free to be cracked.

That's why we will discuss password security & Hash encryption / Decryption as well in this FAQ

The three top methods to stay anonymous are: Proxies, VPN, and Tor.

Proxies: You can configure your browser to use a proxy. A proxy is actually a computer (server) between you, and the website where you connect to.

A normal connection goes like this: you > ISP > Website; with a proxy: you > ISP > Proxy-server > Website.

That makes that the website sees the IP of the website, and not yours one.

Firefox > Preferences > Advanced > Network > Settings use proxy (to use a proxy in your browser).

People post daily proxies in this section:

VPN, Proxies, and Socks

VPN: A Virtual Private Network works kind of the same as a proxy, the only difference is that a proxy only covers the application using the proxy, and not all the other traffic. A VPN secures your whole traffic!

Often VPN also encrypts your traffic for your ISP.

[censored] is a good free VPN.

Tor: The Onion Router is in my opinion the best way to stay anonymous.

Unlike a proxy and VPN, it does originally don't keep logs.

Of course there are some servers who try to log your info and decrypt it, but it's unlikely that will work out for them.

Tor originally works like this:*

You > ISP > Tor-server 1 > Tor-server 2 > Tor-server 3 > Tor-server ... > Website

Multiple encryptions, multiple servers between you and the website,...

Tor also has some extra features and things you should know.

Tor encrypts your traffic even before it reaches the ISP (like as by a VPN - sometimes), so no one can view it.

Best of all, almost every Tor user gets an unique algorithm/key for that encryption, so it's almost impossible to crack.

Tor often switches it's path (changes the server between the first and last node).

If people are able to crack the first server, they only know who has used it, but not what you've done. If they crack the last server (exit node) they know what you're doing, but not who's doing it.

This is a small compensation of a VPN and Tor:

Specs || VPN | Tor

Logs: || Yes | No

Speed: || Fast | Bit Slower

Safety: || Low | High

Encryption: || Yes | Yes, multiple

Servers: || 1 | multiple

Price: || most paid | Free

Why people think Tor isn't safe:

"NSA logs who download Tor" - Use a proxy while downloading.

"Tor servers keep logs" - Not true, only a few who are controlled by the NSA. And if they keep logs it's unlikely they can decrypt your data, if they can decrypt it they only know what you're doing (request you send to websites etc), not who it is doing (you're location is still safe).

"Tor browser is back-doored" - It's open-source, disable JavaScript + route your data through the original Firefox then.

"Tor can get cracked" - View all answers above + only version 2.2 was known to be able to get cracked.

[img]http://s28.postimg.org/4665vn7kd/How_to_search_for_answers.png[/img]

How to search for answers?

This may seem an idiot question, but it isn't!

Some people really don't know how to use Google, or the search function on HackForums.

Let me first show you a bit on how to search on Google.

Google: First of all, don't use Google! It's a damn anti-privacy company.

We will use another Search Engine instead, Startpage.

Startpage gives the same results as Google (based on Google); but it has taken out the logs and track methods the original Google delivers.

<http://startpage.com>

Search results are based on keywords, keywords are small words who describe what you want; it's easier as you may think.

If I for example want to look-up how to do cookie-stealing, I just type:

Cookie-stealing

Or

How to do Cookie-stealing

If you want to get more info about cookie-stealing, Wikipedia is probably the website we want to be looking on.

An easy to get Wikipedia results is by just typing Wikipedia is keyword:

Cookie-stealing Wikipedia

And there your result comes up.

Another way is by using Dorks, with a dork you specify what result should come up, anything not matching that; should come up.

Example:

Cookie-stealing inurl:wikipedia.org

And you'll get a really specific result.

Another dork I want to show, is searching for free e-books!

It's one of my favourite ways.

Our search-query would look like this:

pdf: C++ fundamentals

pdf: malware removal guide

pdf: start with ethical hacking

pdf: How to do SQLi

...

And you get thousands, and thousands of free e-books!

On Hackforums:

<https://hackforums.net/search.php>

You have to work with very selective and descriptive keywords, for more specified results choose the section as well.

Here you can search for members:

<https://hackforums.net/memberlist.php>

Sort by: username

May be more interesting as joining date. :)

[img]http://s28.postimg.org/4znd202z1/How_to_spoof_or_crypt_a_file.png[/img]

If you want to spread malware, spoofing and crypting are essential parts. Let me first explain some terms:

Spoofing: Faking an extension from a file, but keep that file acting like it's original extension.

Converting: Making a file extension, act like another file extension, so it actually changes type.

Crypting: Making a file FUD/UD for protection tools (like: Anti-Viruses, Anti-Malware,...).

FUD: Fully UndetectAble - No protection tools don't detect the malware, not when downloading nor when running.

UD: Only a few protection tools don't detect it, and only in few cases.

Anyway, all of these processes can easily be done by using tools.

Search Hackforums for "Free spoofer" for example.

In the Cryptography section and Hacking Tools and Programs section you can also find thousands of these tools.

If these all are done right, your victim gets infected with your malware.

?Pozdrav - October 6, 2014, 7:47 am

DDoS

Distributed Denial of Service or, DDoS for short is like you connecting to a server along with multiple (thousands/millions) others at the exact same time.

The server is then overloaded with requests to send data. It can't send them to all at the same time so real people can't connect anymore.

Of course, you aren't doing the DDoS yourself, Bots are. Bot's are a method of DDoS that send data packets (UDP, TCP) to a target.

Dos or Denial of service is the same as DDoS, only that one person attacks the server instead of a whole bunch.

Denial of Service, like the name implies it denies access to a service. For instance gaming servers, website or your own home connection.

For some services you want to use a different method then the default one. Each type of service has it's weakness.

For a website it is example mostly better to use a method like "SYN or XML-RPC" as it keeps open the connection or floods the server faster.

Of course, the default methods like a UDP flood still has it's effect on a target, but some methods hit way harder.

UDP is by far the most comon method of DoS.

Normal UDP flood are limited to the port speed of the attacking computer. This is why "Amplification Attacks" are used.

Amplification as the name implies allows us to make the attack way stronger, sometimes up to 500x (*depends on the method)

The most common method for UDP amplification is the "DNS Amplification".

This method of amplification uses the Domain Name System (DNS).

The attacker sends a spoofed request (spoofed so it will return the information to the target) to a DNS Server and the DNS server replies with more data.

Example of returned data.

[img]http://i.technet.microsoft.com/hh972393.dnssec_04(en-us,MSDN.10).jpg[/img]

This is then done at really high speeds with thousands of DNS servers at the same time.

Input -> Target

128Kb -> 128Kb

Input -> DNS Server -> Target

128Kb -> 128Kb -> 3Mb

Of course the numbers aren't perfect but you should get the general idea regarding this method of amplification.

This allows us to turn a 1Gbps attack into a 30-40Gbps attack.

Here is a list of methods found inside booters & Stressers and where they should be used on.
(spoofed) UDP (All)

SYN (Websites) (SSYN too)

Slowloris (websites)

Chargen (websites)

SSDP (All)

DNS (All)

NTP (All)

SNMP (All)

RUDY (websites)

XML-RPC (websites)

Here is a list of some amplification methods used and their effectivity

DNS 28 to 54

NTP 556.9

SNMPv2 6.3

SSDP 30.8

CharGEN 358.8

QOTD 140.3

Kad 16.3

Quake 63.9

XML-RPC

NTP and XML-RPC can be easily blocked and aren't as usefull as they used to be.
Why is NTP so strong? Because it returns the last 600 machines the server has intereacted with.
This causes the response to be WAY BIGGER then the usual amount.

Things that can be used for DDoS are: Dedicated servers, VPS's or Bots (botnet).

Ever heard of LOIC? HOIC? Wether you have or haven't, DO NOT USE THEM!
They have no power now and are worthless. They only slow down your own connection.
Just like "Ping Of Death" concept. (Ping -l 65500 -n -1 -a <target>)

Suggested & Featured Stressers:[vDos](#)

[PM me to get yours here]

0x03a8 - October 6, 2014, 7:47 am

[img]http://s28.postimg.org/z2xag7gul/DDo_S.png[/img]

Distributed Denial of Service or, DDoS for short is like you connecting to a server along with multiple (thousands/millions) others at the exact same time.
The server is then overloaded with requests to send data. It can't send them to all at the same time so real people can't connect anymore.
Of course, you aren't doing the DDoS yourself, Bots are. Bot's are a method of DDoS that send data packets (UDP, TCP) to a target.
Dos or Denial of service is the same as DDoS, only that one person attacks the server instead of a whole bunch.

Denial of Service, like the name implies it denies access to a service. For instance gaming servers, website or your own home connection.
For some services you want to use a different method then the default one. Each type of service has it's weakness.
For a website it is example mostly better to use a method like "SYN or XML-RPC" as it keeps open the connection or floods the server faster.
Of course, the default methods like a UDP flood still has it's effect on a target, but some methods hit way harder.
UDP is by far the most comon method of DoS.

Normal UDP flood are limited to the port speed of the attacking computer. This is why "Amplification Attacks" are used.
Amplification as the name implies allows us to make the attack way stronger, sometimes up to 500x (*depends on the method)
The most common method for UDP amplification is the "DNS Amplification".
This method of amplification uses the Domain Name System (DNS).

The attacker sends a spoofed request (spoofed so it will return the information to the target) to a DNS Server and the DNS server replies with more data.

Example of returned data.

[img][http://i.technet.microsoft.com/hh972393.dnssec_04\(en-us,MSDN.10\).jpg](http://i.technet.microsoft.com/hh972393.dnssec_04(en-us,MSDN.10).jpg)[/img]

This is then done at really high speeds with thousands of DNS servers at the same time.

Input -> Target

128Kb -> 128Kb

Input -> DNS Server -> Target

128Kb -> 128Kb -> 3Mb

Of course the numbers aren't perfect but you should get the general idea regarding this method of amplification.

This allows us to turn a 1Gbps attack into a 30-40Gbps attack.

Here is a list of methods found inside booters & Stressers and where they should be used on.
(spoofed) UDP (All)

SYN (Websites) (SSYN too)

Slowloris (websites)

Chargen (websites)

SSDP (All)

DNS (All)

NTP (All)

SNMP (All)

RUDY (websites)

XML-RPC (websites)

Here is a list of some amplification methods used and their effectivity
DNS 28 to 54

NTP 556.9

SNMPv2 6.3

SSDP 30.8

CharGEN 358.8

QOTD 140.3

Kad 16.3

Quake 63.9

XML-RPC

NTP and XML-RPC can be easily blocked and aren't as usefull as they used to be.
Why is NTP so strong? Because it returns the last 600 machines the server has intereacted with.
This causes the response to be WAY BIGGER then the usual amount.

Things that can be used for DDoS are: Dedicated servers, VPS's or Bots (botnet).

Ever heard of LOIC? HOIC? Wether you have or haven't, DO NOT USE THEM!
They have no power now and are worthless. They only slow down your own connection.
Just like "Ping Of Death" concept. (Ping -l 65500 -n -1 -a <target>)

Suggested & Featured Stressers:[vDos](#)

[PM me to get yours here]

?Pozdrav - October 6, 2014, 7:48 am

This is a placeholder for more conent on this FAQ. Please be patient.

0x03a8 - October 6, 2014, 7:49 am

Coding, one of the easiest & most legal way of getting money easily online.
On top of that, you can use it to get a better job in real life, and it can be used in daily life to make things easier.

For instance if you want to create a program to remove the last character of each line in a text file. If the file is 1000000 lines.

Imagine doing it by hand! You can just code a program in 5 minutes and run the program for 30 seconds, and you're done. Easy as that.

You can also use it to create a program that you can then sell, be it on HF or on another forum.
Some things you can create,
and in what languages you can create them (in order of recommendation):

Bot / Rat: C++, C, VB.NET, C#(Visual)

Keylogger: VB.NET, C#

Crypter: VB.NET, C#

Stresser / Booter: PHP, HTML, CSS, SQL

Website: PHP, HTML, CSS, SQL, JS

Coding languages explained

PHP:

Lorem ipsum dolor sit amet, consectetur adipiscing elit. In vulputate nisi scelerisque urna tempor, ullamcorper lacinia felis ultrices. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Mauris fringilla quis justo eu aliquam. Fusce mi elit, scelerisque at eleifend eu, laoreet non lorem. Donec mollis ultrices arcu, sed auctor ante blandit vitae. Ut sit amet hendrerit neque. Maecenas a purus vulputate, pharetra diam in, lacinia sem. Suspendisse eleifend fringilla sapien, eget commodo sapien feugiat at. Sed lacinia elementum scelerisque. Ut pharetra vitae tortor non faucibus. Curabitur non leo ut turpis feugiat maximus quis non nisi. Nam sagittis a ligula eget congue. Nullam et convallis magna. Praesent eget mattis orci. Fusce tempus, ligula sed accumsan tincidunt, ipsum elit ullamcorper enim, sed consectetur libero tortor id urna.

?Pozdrav - October 6, 2014, 7:49 am

This is a placeholder for more content on this FAQ. Please be patient.

0x03a8 - October 6, 2014, 7:50 am

This is a placeholder for more content on this FAQ. Please be patient. :)

?Pozdrav - October 6, 2014, 7:50 am

This is a placeholder for more content on this FAQ. Please be patient.

0x03a8 - October 6, 2014, 7:51 am

This is a placeholder for more content on this FAQ. Please be patient. Get ready

Niely - October 6, 2014, 8:48 am

This is a placeholder for more content on this FAQ. Please be patient.

RelationShit - October 6, 2014, 9:24 am

This is not a placeholder for more content on this FAQ. Please be patient.

Cyrus - October 6, 2014, 9:26 am

Guys, disable your signature's in the "place holder" it makes the thread so ugly.

0x03a8 - October 6, 2014, 9:44 am

(Oct 6, 2014 09:26 AM)Cyrus Wrote: [\[CITE\]](#) Guys, disable your signature's in the "place holder" it makes the thread so ugly.

Thanks Cyrus :)

I'm getting everyone to disable theirs now.

Feel free to leave suggestions on content to add

note: I'm adding GFX soon to make it look better

haximizer - October 6, 2014, 11:28 am

Good job with the faq until now.

Most of this subjects take ALOT of time to start learning right when people have not some mentor, or some directions from where to go, and the way u're doing u're stuff it's very well organized. Good for beginners.

Keep up the good job.

0x03a8 - October 6, 2014, 12:54 pm

(Oct 6, 2014 11:28 AM)haximizer Wrote: [\[CITE\]](#) Good job with the faq until now.

Most of this subjects take ALOT of time to start learning right when people have not some mentor, or some directions from where to go, and the way u're doing u're stuff it's very well organized. Good for beginners.

Keep up the good job.

Thanks, I'd like to request everyone to link people to this thread if their answer can be found here

Aura - October 6, 2014, 6:29 pm

Should had left the "How to remove a virus" part to someone who actually knows how it works but oh well ...

Good thread overall.

0x03a8 - October 6, 2014, 10:11 pm

(Oct 6, 2014 06:29 PM)Aur? Wrote: [\[CITE\]](#) Should had left the "How to remove a virus" part to someone who actually knows how it works but oh well ...

Good thread overall.

XD I was fully aware that I can't do it.

I wasn't able to directly find someone who's able to write this for the FAQ.

If you want to take this chance and write that part out, you are free to do so.

Just send me a PM and let me know.

Same goes for everyone else, if you feel like you can do better, think things are missing or anything else.

Send me a PM and we can add your section, paragraph(s).

Hassan Gazi - October 7, 2014, 10:06 am

Great thread ?

Don't forgot to add a tutorial on RAT and Keyloggers. Most of the newbies ask questions about these things.

Keep it up ?

0x03a8 - October 7, 2014, 11:59 pm

(Oct 7, 2014 10:06 AM)Hassan Gazi Wrote: [\[CITE\]](#) Great thread ?

Don't forgot to add a tutorial on RAT and Keyloggers. Most of the newbies ask questions about these things.

Keep it up ?

I'll add links and improve that section soon.

420 Blaze It - October 8, 2014, 12:00 am

Interesting, explains everything needed to known.

0x03a8 - October 8, 2014, 10:06 pm

(Oct 8, 2014 12:00 AM)420 Blaze It Wrote: [\[CITE\]](#) Interesting, explains everything needed to known.

Thanks, We're still adding content.

muzzy. - October 12, 2014, 9:56 am

Hey there. If you take a look at my post count, I have over 1000 posts in here.

Take a look at my [thread](#) from last year, from which Omni & a number of the staff / helpers posted in. This section has had literally hundreds of these mega threads, and they're buried in days. If people planned on reading before asking, they'd use the search feature. This section exists to function as a cess pit for the beginners and 1 account wonders to ask their questions.

Your effort is appreciated, but the people you want to read it aren't going to.

0x03a8 - October 12, 2014, 10:19 am

(Oct 12, 2014 09:56 AM)Muzzy Wrote: [\[CITE\]](#) Hey there. If you take a look at my post count, I have over 1000 posts in here.

Take a look at my [thread](#) from last year, from which Omni & a number of the staff / helpers posted in. This section has had literally hundreds of these mega threads, and they're buried in days. If people planned on reading before asking, they'd use the search feature. This section exists to function as a cess pit for the beginners and 1 account wonders to ask their questions.

Your effort is appreciated, but the people you want to read it aren't going to.

Omni should have stickied one of those damn threads and it would have been over & fixed

Niely - October 12, 2014, 10:20 am

^I've sent you more content for the FAQ through PM by the way. :)

PA666 - October 17, 2014, 2:42 pm

RIP HQ thread ;(

Guess this won't be updated anymore

Niely - October 17, 2014, 4:07 pm

What the hell happened to the OP?

Did he scammed someone? From what I knew it always was a HQ member?

Pilfering - November 13, 2014, 11:30 am

So much information, thanks for this!

CyberGuard - August 5, 2015, 11:08 pm

Perhaps someone should remake this thread.