

Forum:[Hack Forums](#)

Thread: [HF Served How?](#)

Omniscient - September 2, 2016, 11:35 am

For those wondering why they get slow HF loads or maybe just curious how HF is served...I made this new chart which represents most of how HF is served to you.

I'll try to explain the image and elaborate a bit.

We start at CF (Cloudflare) which has a WAF (Web Application Firewall) and a lot of rulesets. Once we go through HF security we have Sucuri which again has DDOS protection and assists in grabbing traffic that CF doesn't block. I don't always have Sucuri enabled as it tends to have a higher rate of false positives and their setup is sometimes buggy.

Next we hit a server which has an OS kernel based firewall which I personally manage. It's also a tunnel server. Packets that hit this server are then tunneled to the next server which runs Nginx.

Nginx has some modules for DDOS protection. Nginx serves all the static content. It then forwards any php requests to Apache. You may wonder why I don't use Nginx to forward to Apache but I have my reasons. I have some custom written modules for Apache that I can't replace with Nginx. These modules enhances HF security and ddos protection. They are irreplaceable. Once you pass Nginx though you do get forwarded to Apache which as I stated does have a lot of modules and is setup fairly well.

Apache will forward the PHP calls to the PHP CGI processor. That's when the nuts and bolts of the actual serving of the page truly begins. PHP grabs the database (different server) information and serves your browser the page.

And so that's why HF doesn't load in .5 seconds and miraculously does load in just 2-3 seconds (most pages anyways).

This setup has taken me years to mature into with layers being added as needed based on attacks, security requirements, technology changes, and the size of HF itself.

So when I get a PM saying a person is blocked or having slow page loads you must understand that it's not a 10 second (or even 10 minute) fix to figure out why one user is having a problem. Each layer has protections which could slow you down or even block you.

For those who doubt that we need all this....

That's the past month. It's nearly 3 BILLION requests and that's over 60 TB of traffic too. And yet our downtime is for the most part minimal in comparison to the sizes of the attacks.

Sometimes attacks are worse too. Cloudflare just lets me display past month.

And that's not everything either. It's just what I'm willing to post about. Do we go offline sometimes? Yes, we do. And I'm sure we'll continue to be attacked regularly. I never honestly care about who is attacking or why they are. My only concern is keeping HF online. At this point there is a lot of automation built into protection. Some protections are always enabled while others toggle on/off based on attack patterns. And there is always things I can do manually.

After the past 10 days of rather large attacks I went into a few of our layers and tightened them up. We should see even better uptime now. Doubt a day will ever come where we will see 100% uptime but I'm happy with even 98% considering the frequency of attacks.

Thank you.

Nachfolger - September 2, 2016, 11:36 am

Interesting explanation. Probably needed for those who hate on the loadtimes.

Thanks.

Jordana Brewster - September 2, 2016, 11:39 am

That is a ton of security, but... looks like it's needed

KFC Watermelon - September 2, 2016, 11:40 am

HackForums usually loads very quick for me. This page took 477ms to load according to Chrome's network debugger. Great work on the setup!

felicixus - September 2, 2016, 11:40 am

Nice system!

Do you think attackers can now use targeted attack after this lesson on how HF is served?

Fortunate - September 2, 2016, 11:41 am

This very cool and interesting, i have always wondered how HF runs, thanks.

Azylum - September 2, 2016, 11:42 am

Now that's what i call security.

Great job.

W?lf - September 2, 2016, 11:42 am

Behind the scenes on how protected hackforums really is and how many attacks it gets. Thanks for the info omni!

Neeeeeeeeeeel.- - September 2, 2016, 11:44 am

Wow, what a complex structure! I thought it was too much simple like CP -> Firewall -> HF Server

Omniscient - September 2, 2016, 11:46 am

(Sep 2, 2016 11:40 AM)felicixus Wrote: [\[CITE\]](#) Nice system!

Do you think attackers can now use targeted attack after this lesson on how HF is served?

We'll get attacked anyways. I'm sure this thread will inspire a moron or two to do so almost immediately. I've seen attacks sustained for 3 days that didn't do much more than 1 second page load delays. My guess is the butthurt ban evaders are the ones who most likely attack.

If we get attacked and go offline it's not something I whine about. I deal with it and move on. If we're offline 3 minutes or 3 hours then so be it. I just site here and work on it. Attacks are part of my daily routine and don't effect me personally.

Just be patience and HF will eventually come back. Follow the Twitter as I use it to announce long downtimes.

Headdy - September 2, 2016, 11:47 am

Now that was an interesting read!

I enjoy insight topics :)

webdev77 - September 2, 2016, 11:52 am

Pretty cool setup that exists here. I appreciate the time and effort that has been taken to keep us online here.

Rubixa - September 2, 2016, 11:52 am

Crazy setup but definitely needed.. almost 3 billion in the past month, that's insane. Thanks heaps for sharing how we access the site on the daily, was definitely an interesting read.

Bluffer - September 2, 2016, 11:54 am

I recall a few months ago when my site was constantly getting attacked and it really sucks.

It's cool that with your experience you are able to find so many ways to block the attacks or redirect them. Nice job!

Omniscient - September 2, 2016, 11:58 am

(Sep 2, 2016 11:54 AM)Bluffer Wrote: [\[CITE\]](#) I recall a few months ago when my site was constantly getting attacked and it really sucks.

It's cool that with your experience you are able to find so many ways to block the attacks or redirect them. Nice job!

I think if I didn't have HF I'd work in DDOS protection maybe. Not that it's my favorite thing to do but I've become adept at it simply out of necessity.

MasterCurser - September 2, 2016, 11:59 am

It really takes years to set up something like this. To know if it is needed and spend on it. That's something amazing right there. I'll now know what is going on when my thread is not loading but youtube is running crazy.

Tommy - September 2, 2016, 12:04 pm

Downtime doesn't seem like it's an issue anymore not as much as it used to a few years ago.

Zher0 - September 2, 2016, 12:14 pm

Very interesting, I'm surprised the load times are so quick with all those services and servers! Nice job.

minimalist - September 2, 2016, 12:25 pm

I hope this isn't an incredibly ill-informed question, but what goes on before CloudFlare...or is it hosted by CloudFlare?

Bibbly - September 2, 2016, 12:27 pm

(Sep 2, 2016 11:52 AM)Rubixa Wrote: [\[CITE\]](#) Crazy setup but definitely needed.. almost 3 billion in the past month, that's insane. Thanks heaps for sharing how we access the site on the daily, was definitely an interesting read.

crazy you see there is a point to where it used 1Billion on one attack
keep up the work omni

RelationShit - September 2, 2016, 12:28 pm

SUCURI doesn't like me

It would never allow me to use Hf on airports

M?xim - September 2, 2016, 12:29 pm

Hopefully people will stop crying over 2-5 seconds load time now.

Rubixa - September 2, 2016, 12:30 pm

(Sep 2, 2016 12:27 PM)Bibbly Wrote: [\[CITE\]](#) crazy you see there is a point to where it used 1Billion on one attack

keep up the work omni

The 1.10B attack at the end? Yeah, how nuts is that! Crazy to see how hard Omni works to keep us up.

(Sep 2, 2016 12:29 PM)That Guy Maxim Wrote: [\[CITE\]](#) Hopefully people will stop crying over 2-5 seconds load time now.

There will always be that one guy, always.

Princeton - September 2, 2016, 12:31 pm

Great system structure! This might be the secret of why HF is always running despite being targeted so many times.

Rubixa - September 2, 2016, 12:33 pm

(Sep 2, 2016 12:25 PM)Minimalist Wrote: [\[CITE\]](#) I hope this isn't an incredibly ill-informed question, but what goes on before CloudFlare...or is it hosted by CloudFlare?

"And that's not everything either. It's just what I'm willing to post about."

I probably wouldn't ask about anything more than what he has decided to show us, really none of our business. I asked about his setup once and got the reply I probably should have expected.

M?xim - September 2, 2016, 12:35 pm

(Sep 2, 2016 12:33 PM)Rubixa Wrote: [\[CITE\]](#) I asked about his setup once and got the reply I probably should have expected.

Please share with us lol.

LastSession - September 2, 2016, 12:36 pm

(Sep 2, 2016 12:35 PM)That Guy Maxim Wrote: [\[CITE\]](#) Please share with us lol.

You are not allowed to share PMs ? lol

minimalist - September 2, 2016, 12:36 pm

(Sep 2, 2016 12:33 PM)Rubixa Wrote: [\[CITE\]](#) "And that's not everything either. It's just what I'm willing to post about."

I probably wouldn't ask about anything more than what he has decided to show us, really none of our business. I asked about his setup once and got the reply I probably should have expected.

I'm just asking about the machine that processes all of our low quality posts. I think I remember him posting the specs to one of the servers but I can't find it anymore. Just curious is all ?.

Elitas - September 2, 2016, 12:37 pm

Very insightful! Thanks for showing us this Omni! :)

Rubixa - September 2, 2016, 12:38 pm

(Sep 2, 2016 12:35 PM)That Guy Maxim Wrote: [\[CITE\]](#) Please share with us lol.

No, it's just none of our business how HF is setup, let's leave it at that and be thankful he has shown us this much and how much work we now realize goes into keeping the site up.

All that matters.

LastSession - September 2, 2016, 12:39 pm

(Sep 2, 2016 12:37 PM)xHackerPr0 Wrote: [\[CITE\]](#) Very

insightful!

Do you really just avoided the 25 characters in Omniscient's thread? thug life

Varane - September 2, 2016, 12:39 pm

This is a very interesting chart, simple but it explains a lot.

Elitas - September 2, 2016, 12:40 pm

(Sep 2, 2016 12:39 PM)LastSession Wrote: [\[CITE\]](#) Do you really just avoided the 25 characters in Omniscient's thread? thug life

Done that by accident, is it a rule?

M?xim - September 2, 2016, 12:40 pm

(Sep 2, 2016 12:36 PM)LastSession Wrote: [\[CITE\]](#) You are not allowed to share PMs ? lol

Oh damn. Thought you could. Really wanted to know what he replied lol.

(Sep 2, 2016 12:38 PM)Rubixa Wrote: [\[CITE\]](#) No, it's just none of our business how HF is setup, let's leave it at that and be thankful he has shown us this much and how much work we now realize goes into keeping the site up.

All that matters.

Never said that I wanted to know about the "setup".

Rubixa - September 2, 2016, 12:48 pm

(Sep 2, 2016 12:40 PM)That Guy Maxim Wrote: [\[CITE\]](#) Oh damn. Thought you could. Really wanted to know what he replied lol.

Never said that I wanted to know about the "setup".

And I never said that you did? Basically nailed down that I asked him about it and that it wasn't mine or anyone's business.

Meow - September 2, 2016, 12:56 pm

So, you are doing your best at keeping HF online as much as possible (and it's doing great considering how many DDOS attacks you get), you check most of your PMs, you keep community clean (ban/close/rekill) and you get to have some free time with your family/friends/whoever?

And all that in 24 hours? holy shit

LastSession - September 2, 2016, 12:58 pm

(Sep 2, 2016 12:56 PM)Meow? Wrote: [\[CITE\]](#) So, you are doing your best at keeping HF online as much as possible (and it's doing great considering how many DDOS attacks you get), you check most of your PMs, you keep community clean (ban/close/rekill) and you get to have some free time with your family/friends/whoever?

And all that in 24 hours? holy shit

And additionally, I read that he owns even more forums. lol

J?son - September 2, 2016, 12:59 pm

Honestly, this websites loads fast for me and I'm on satellite internet.

The people who complain about this website loading slow must have dial-up.

Y?ung Thug - September 2, 2016, 1:00 pm

Its rare that the site takes more than .5 seconds to load each page for me

Omniscient - September 2, 2016, 1:03 pm

Quote:I hope this isn't an incredibly ill-informed question, but what goes on before CloudFlare...or is it hosted by CloudFlare?

Yes, that's ill-informed. Before a page is begun there is DNS which is also at Cloudflare. DNS is normally cached by ISP's with the TTL (time-to-live). Cloudflare DNS is very good and initially I only used CF strictly for DNS. They have a very good global network for delivery. Years ago many attacks were DNS based but nowadays that style of attack is much-less effective. Mainly it's layer-7 HTTP floods that get the farthest. Clever attackers definitely show some creativity and ingenuity when going after HF. I've seen just about every attack style imaginable.

SoulZeh - September 2, 2016, 1:25 pm

Omni are you some type of wizard?

However, 9/10 hackforums loads perfectly fine for me, Yea I get the odd slow moment from time to time, but a little refresh and my shits sorted.

samsepi01 - September 2, 2016, 1:34 pm

Thanks a ton for taking the time to write this out, Omni! It is always wonderful as a sysadmin to see how the pros do things!

Night Fury - September 2, 2016, 5:08 pm

That was a very informative thread. I also don't have much issue with HF's loading times, but I appreciate the opportunity to learn.

This makes me wonder about something: what differences would one see between a setup like this and one that a giant company like YouTube operates? Is it always generally a similar structure, but they have the fastest of everything because of their access to large amounts of capital? Being that they receive 18% of overall peak internet traffic, I'm sure their system is robust, but would you guess it is one of the most intricate systems on the internet as well?

Omniscient - September 2, 2016, 9:37 pm

Quote:what differences would one see between a setup like this and one that a giant company like YouTube operates?

I can't say for sure but definitely they spend more on infrastructure. They have many more servers than I do. I doubt they rely on something like Cloudflare but these massive companies normally use Akamai technology.

<https://www.akamai.com/>

Google is 100% custom kernels for their setups. Gotta be amazing to work in their backend datacenters.

<https://www.google.com/about/datacenters/>

Description - September 2, 2016, 10:02 pm

Woah this is really neat and lots of security

Will Grigg - September 2, 2016, 10:10 pm

Omni have you ever contacting the police about the massive attacks HF gets? like has it ever happened that you have done it? Since you have so great skills im pretty sure you can trace these attackers and hand them to the police.

fire_bender - September 2, 2016, 10:11 pm

Wow, just checked Sucuri's pricing and they are far lower than CloudFlare's. Is Sucuri better at mitigating DDoS attacks than CloudFlare? I'm asking cause I'm paying CloudFlare 200 a month (yeah they offer CDN but I don't use it, I use MaxCDN which works perfectly)...

Switching to Sucuri, if better than CloudFlare mitigating attacks then thats like 2K savings a year...

Ni??c??k - September 2, 2016, 10:18 pm

Do you spend a lot just on this security alone?

It's mind-boggling to know the measures we have to take to keep HF up.

KFC Watermelon - September 2, 2016, 10:18 pm

(Sep 2, 2016 10:11 PM)fire_bender Wrote: [\[CITE\]](#) Wow, just checked Sucuri's pricing and they are far lower than CloudFlare's. Is Sucuri better at mitigating DDoS attacks than CloudFlare? I'm asking cause I'm paying CloudFlare 200 a month (yeah they offer CDN but I don't use it, I use MaxCDN which works perfectly)...

Switching to Sucuri, if better than CloudFlare mitigating attacks then thats like 2K savings a year... In my experience, it's no where near as good. and Sucuri's captcha screen will scare off a lot of legitimate traffic.

I use CloudFlare pro with firewall rules and my backend filters all requests. Not sure what the CloudFlare \$200/month package offers over pro.

fire_bender - September 2, 2016, 10:21 pm

(Sep 2, 2016 10:18 PM)KFC Watermelon Wrote: [\[CITE\]](#) In my experience, it's no where near as good. and Sucuri's captcha screen will scare off a lot of legitimate traffic.

I use CloudFlare pro with custom firewall rules and my backend filters all requests. Not sure what the CloudFlare \$200/month package offers over pro.

I have CL business... some more crappy features, but the only "good one" I find is "Advanced DDoS" protection.

Does Sucuri always throw the captcha to first time visitors?

Night Fury - September 2, 2016, 10:54 pm

(Sep 2, 2016 09:37 PM)Omniscient Wrote: [\[CITE\]](#) I can't say for sure but definitely they spend more on infrastructure. They have many more servers than I do. I doubt they rely on something like Cloudflare but these massive companies normally use Akamai technology.

<https://www.akamai.com/>

Google is 100% custom kernels for their setups. Gotta be amazing to work in their backend datacenters.

<https://www.google.com/about/datacenters/>

Wow, that center is amazing. The alligators are a nice extra touch on security.

Akamai gives some interesting info on traffic and attacks. According to them, there were over three million attacks in the US today. Based on all your internet experience, are attacks a recent phenomenon, or have they always been a concern of yours? Akamai was founded in 1998, so was there not much need for worry prior to their founding?

There is a lot more going on behind the scenes than I ever imagined. I'm sure there's a lot more that I don't know about. Thanks for the response. Technology's awesome.

He B TeMy - September 3, 2016, 4:46 am

Yea, it was no news for me there were several steps before the requests hit your server, it's always that 2s wait then loads in half a second, that is a no brainer, sometimes the page does load in half a second after the request but the traffic must be huge sometimes.

Mr. Robot - September 3, 2016, 4:49 am

Quote:I never honestly care about who is attacking or why they are. My only concern is keeping HF online. At this point there is a lot of automation built into protection. Some protections are always enabled while others toggle on/off based on attack patterns. And there is always things I can do manually.

Respect for that right there. Keep it up, that's all we can ask of you mate. It's like, you get no recognition for the work in keeping it up when it's running fine but when it goes down - people bitch.

ps. I have the same keyboard - still don't know what f9, f10, f11 and f12 do.

Ventriloquism - September 3, 2016, 6:39 am

Very interesting :> Thanks for the explanation Omni

Refusal - September 3, 2016, 6:46 am

Lol you could never have too much security I guess lol.

The HF load times for me are fine.

Prince™ - September 3, 2016, 7:19 am

"3 BILLION requests and that's over 60 TB of traffic too."

Jesus Christ!

Happeh - September 3, 2016, 9:43 am

I don't mind - this is super pleasant to see and your efforts are clearly noticeable. Said this last thread but I'm from the generation where downtime could be hours and hours if you were sleeping so to see such a tight system is really cool. Especially when you can go on holiday and enjoy yourself and nothing much happening.

Granny Bacon - September 3, 2016, 9:53 am

I enjoy reading threads like these because I get to expand my knowledge in this field considering I'm gonna work servers/security.

I have a question though, I've heard some companies use Voxility and some use cloudflare, what's the difference between those two?

Omniscient - September 3, 2016, 9:56 am

(Sep 3, 2016 09:53 AM)Granny Bacon Wrote: [\[CITE\]](#) I enjoy reading threads like these because I get to expand my knowledge in this field considering I'm gonna work servers/security.

I have a question though, I've heard some companies use Voxility and some use cloudflare, what's the difference between those two?

I hear some good things about Voxility. Voxility isn't something I would use though. They don't list prices and have this weird website.

B?ker - September 3, 2016, 9:56 am

(Sep 3, 2016 09:53 AM)Granny Bacon Wrote: [\[CITE\]](#) I enjoy reading threads like these because I get to expand my knowledge in this field considering I'm gonna work servers/security.

I have a question though, I've heard some companies use Voxility and some use cloudflare, what's the difference between those two?Rumor is they have over 500GB of DDoS Protection, or so what I have read. But I agree I love reading these types of threads.

(Sep 3, 2016 09:56 AM)Omniscient Wrote: [\[CITE\]](#) I hear some good things about Voxility. Voxility isn't something I would use though. They don't list prices and have this weird website.
Completely Agree on this myself!

YinYang - September 3, 2016, 9:59 am

Hahaha thanks for giving me the key to hacking Hackforums!

For real though this was pretty interesting to read, and I don't mind the 'slow' loading time, because hackforums has an amazing uptime.

Omniscient - September 3, 2016, 10:02 am

(Sep 3, 2016 09:59 AM)YinYang Wrote: [\[CITE\]](#) Hahaha thanks for giving me the key to hacking Hackforums!

Giving you my address and where the front door is doesn't tell you where I'm sitting inside with my shotgun.

:)

TRH4CK - September 3, 2016, 10:05 am

Damn that looks complicated.... What are the specs of the main server (HF), if you don't mind ?

Cammy - September 3, 2016, 10:06 am

Man that looks awful difficult to maintain and keep running with (almost) no problems. Props

I have a question though

So for example if the Server Firewall goes offline for some reason (a power failure or whatever) does it just skip over that layer of security or does the whole site get inaccessible because of it? Sorry if that's already been asked

Granny Bacon - September 3, 2016, 10:07 am

(Sep 3, 2016 09:56 AM)Omniscient Wrote: [\[CITE\]](#) I hear some good things about Voxility. Voxility isn't something I would use though. They don't list prices and have this weird website.

I agree their website is really weird... I don't know if it is the right page but here are the prices for each plans if you want to just check it out:

<https://www.voxility.com/shop/security/anti-ddos/iaas/2013.05.20%20-%20Voxility%20Anti-DDoS%20for%20Hosted%20Infrastructure.%20Euro%20Price%20List.pdf>

And those prices are damn high...

Well, HF works 99% of the time when I browse so I don't really complain. xD

YinYang - September 3, 2016, 10:08 am

(Sep 3, 2016 10:02 AM)Omniscient Wrote: [\[CITE\]](#) Giving you my address and where the front door is doesn't tell you where I'm sitting inside with my shotgun.

:)

Fuck that's a good quote, ima use that one

What physical security do you have in your home may I ask?

Including pins, passwords etc

YayHar - September 3, 2016, 10:08 am

Load times don't affect me that much. I find it interesting how much security this site actually has.

Keep it going Omni.

Light - September 3, 2016, 10:09 am

(Sep 3, 2016 09:56 AM)Omniscient Wrote: [\[CITE\]](#) I hear some good things about Voxility. Voxility isn't something I would use though. They don't list prices and have this weird website.

Yeah, Voxillity they don't make it clear and simple to buy, you think a company would want to, but nah.

LastSession VII - September 3, 2016, 10:09 am

Hackforums.net is really fast for me, its down sometimes (like 10mins max).

May I ask how much you pay to host the site with all that shit (like cf, firewall ect)

or its private lol

Granny Bacon - September 3, 2016, 10:12 am

(Sep 3, 2016 10:09 AM)Productivity Wrote: [\[CITE\]](#) Yeah, Voxillity they don't make it clear and simple to buy, you think a company would want to, but nah.

Well their website looks very bad, I think they should work on it a little bit more to look more presentable, I just heard big companies are using it.

Tommy Chong - September 3, 2016, 10:15 am

I don't really have any problems with loading hackforums.

There's some downtime pretty much every day, but thats not longer than 10min max. Usually it takes like a minute. But that's no surprise with all these skids, kids and banned/closed kids who ddos because they're butthurt.

Sometimes it loads a bit slower, but i don't really mind.

I feel like Omni is doing a great job running this site. The downtime is minimal if you look at how big the userbase is.

Evanescence - September 3, 2016, 10:39 am

Great setup with awesome speed when taking into account the measures.

M?xim - September 3, 2016, 10:45 am

(Sep 3, 2016 10:02 AM)Omniscient Wrote: [\[CITE\]](#) Giving you my address and where the front door is

doesn't tell you where I'm sitting inside with my shotgun.

:)

Best thing i've read today.

Dark Smile - September 3, 2016, 10:48 am

Was someone get to successfully attack Cloud flare or is stucked on allways stuck on some firewall before?

Roy Wood\$ - September 3, 2016, 11:50 am

yo omni whats the biggest attack that hit u ?

TheRapist - September 3, 2016, 12:12 pm

That setup is impressive!

It's weird that people will spend their time and money just to make somebody's day harder..

'Ben - September 3, 2016, 12:25 pm

Other than the odd slow load time I have never really noticed anything worth complaining about.

J?son - September 3, 2016, 3:50 pm

Voxility is garbage and I wouldn't suggest using it.

I prefer using OVH.

Canonsx130 - September 3, 2016, 7:58 pm

So with all these multiple layers of security, how can someone still take HF down, at least theoretically? BTW great read, was very informative and now I have lots of stuffs to read and know more about :)

Omniscient - September 4, 2016, 11:13 am

Quote:So for example if the Server Firewall goes offline for some reason (a power failure or whatever) does it just skip over that layer of security or does the whole site get inaccessible because of it?

If one layer breaks the site is not accessible. At times some of the layers have problems at the datacenters but normally they are temporary.

Quote:May I ask how much you pay to host the site with all that shit (like cf, firewall ect)

Sorry, I don't like to discuss financials.

Quote:Do the attacks motivate you to 'build' a perfect system?

Yes. It's a very high priority to maintain uptime and site security. Much of the serious work I've done for HF over the years has been associated with stopping attack effectiveness.

Quote:yo omni whats the biggest attack that hit u ?

Glad you asked.

<https://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack/>

Quote:So with all these multiple layers of security, how can someone still take HF down, at least

theoretically?

Because there are people willing to go through great lengths to attack HF. Unsure if they are testing their abilities or just want to disrupt HF. And what worked 5 years ago to stop attacks may not work today. Attacks continue to evolve.

Cold Hearted - September 4, 2016, 11:15 am

Strange, Hackforums has loaded a ton faster for me the past 2-3 days.

Before then it took around 10 seconds+ a time, now it's loading in about 300ms.

shashwat97 - September 4, 2016, 11:28 am

Having a forum about hacking is bound to lead to attacks. Nice to know how much work goes into keeping the website almost DDOS proof.

USMC Chris - September 4, 2016, 11:48 am

I don't know too much about the actual coding and bypassing of layers of security, but in my mind, in theory, I would assume the easiest way to DDOS attack through all those layers of security would be to sign in on a regular account, run a program that would tell you what servers you are going to as you go through the layers of security, then find the IP/Server ID's for the main server once you bypass all the security measures.

But even then I'm sure you have something in place to ensure no one will be able to properly ID the DNS/IP of your main Server(s) for HF to run off of. Definitely an admirable system you run here to ensure the protection of your site.

Omniscient - September 4, 2016, 11:54 am

Quote:I don't know too much about the actual coding and bypassing of layers of security

That's the only correct thing you said. Everything else was wrong. The only real attacks we need to deal with are HTTP layer 7 floods. The rest are pretty much handled appropriately. And right now, my latest changes to security are working very well to stop those.

I do have at least 2 new options for DDOS protection technology that I haven't used but am prepared to setup. I always try to have someone available that's new so we're able to be a bit dynamic in mitigating attacks. If I were to do everything possible I fear a successful attack wouldn't be stopped. So I always keep an option open.

Also adding new layers does slow down HF serving and further complicates the backend.

?hoenix - September 4, 2016, 11:55 am

It's pretty neat seeing how you have Hack Forums routed, I was always curious why I would rarely get a sucuri captcha and sometimes a cloudflare captcha but not it makes sense.

LastSession - September 4, 2016, 11:58 am

I wonder what kind of people want to harm the site. Intelligent agencies? HF members who got closed? lol. I don't think they achieve that someone will leave the site due to these attacks or that Omniscinet will give up because of them.

It has a good side though:

There will always be haters. And the more you grow the more they hate; the more they hate the more you grow.

USMC Chris - September 4, 2016, 12:10 pm

(Sep 4, 2016 11:54 AM)Omniscient Wrote: [\[CITE\]](#) That's the only correct thing you said. Everything else was wrong. The only real attacks we need to deal with are HTTP layer 7 floods. The rest are pretty much handled appropriately. And right now, my latest changes to security are working very well to stop those.

I do have at least 2 new options for DDOS protection technology that I haven't used but am prepared to setup. I always try to have someone available that's new so we're able to be a bit dynamic in mitigating attacks. If I were to do everything possible I fear a successful attack wouldn't be stopped. So I always keep an option open.

Also adding new layers does slow down HF serving and further complicates the backend.
Thanks for the knowledge

What I was saying was for instance when you go to look for the IP of HF.net you will find 104.23.128.83, which is a cloudflare server. But if someone who is more hacking inclined than I with better tools, would they not be able to further find the IP's of the Sucuri server, then the Firewall server, then the Tunnel server, so on and so fourth until they reach the HF main server? You said HTTP Layer 7 is your only real threat, which I assume is because by it's own nature it is more capable of being seen as harmless traffic than any other type of flood. So if instead of attempting a flood you only pinged one seemingly harmless packet through all of the layers, would you not be able to return the IP of the main server upon reaching it? If the main servers are used and accessible by any member, there must be some way to access the address.

???? - September 4, 2016, 12:12 pm

This is a surprising amount of tunneling & protection for a site that loads so fast for me (~0.5-1s).

How do you deal with DDoS attacks when they happen? As when HF is down it is never longer than a few minutes. Does some firewall kick in?

ps-
Spoiler [\(Click to View\)](#)
open my pm ?

Omniscient - September 4, 2016, 12:23 pm

Quote: But if someone who is more hacking inclined than I with better tools, would they not be able to further find the IP's of the Sucuri server, then the Firewall server, then the Tunnel server, so on and so fourth until they reach the HF main server?

No tools would be able to penetrate all those layers in that way.

Quote: So if instead of attempting a flood you only pinged one seemingly harmless packet through all of the layers, would you not be able to return the IP of the main server upon reaching it?

Not how the serving technology works.

One layer calls the next layer which then calls the next layer. Each layer is essentially invisible to that 3rd layer. So yes, if you do by chance get past Cloudflare you'd see the next layer but that wouldn't tell you what's next. Highly unlikely all the layers would get penetrated. And even if they were. Would take me about 15 minutes to change the setup, which is part of my design as well. I can change at least 3 layers IPs on a whim, just in case. And sometimes I do change our IPs a matter of added security, which is why DNS sometimes gets screwy for members. Tunnels and IPs

are very easy to change.

Quote:How do you deal with DDoS attacks when they happen?

First post explains that. Each of these layers is a form of ddos protection. 99% of our protection scheme is automated.

Quote:As when HF is down it is never longer than a few minutes. Does some firewall kick in?

Yup. Custom coding so that we're not always under full protection but when attacks begin protections automatically start. Even better is that when attacks end the protections disable after a time.

Industry - September 4, 2016, 12:26 pm

Site can be a little slow here and there, but that's to be expected with enhanced security. I have only encountered minimal downtime or accessibility problems since you implemented it. Loading time does not seem to be affected by it either, overall I'm liking it. Nearly 6 years in the forums and it just keep getting better with every passing day!

Good shit Omnidude,

USMC Chris - September 4, 2016, 12:28 pm

(Sep 4, 2016 12:23 PM)Omniscient Wrote: [\[CITE\]](#) No tools would be able to penetrate all those layers in that way.

Not how the serving technology works.

One layer calls the next layer which then calls the next layer. Each layer is essentially invisible to that 3rd layer. So yes, if you do by chance get past Cloudflare you'd see the next layer but that wouldn't tell you what's next. Highly unlikely all the layers would get penetrated. And even if they were. Would take me about 15 minutes to change the setup, which is part of my design as well. I can change at least 3 layers IPs on a whim, just in case. And sometimes I do change our IPs a matter of added security, which is why DNS sometimes gets screwy for members. Tunnels and IPs are very easy to change.

That's a pretty intricate system you run, easy to say you got the sites security under control (from my perspective, at least). Security for anything is a constantly ongoing battle, but it seems like you're a few steps ahead of the game in counter-measures as it stands.

Thanks for the knowledge!

webgoat - September 4, 2016, 12:45 pm

HF loads so faster for me. Max 0,5 seconds..

Omniscient - September 4, 2016, 12:45 pm

Also note that this is just the ddos protection scheme. I run a lot of additional security, triggers, and honeypots in order to detect and prevent intrusions. Which is why I am always incredibly skeptical when people say HF was dumped. The measures in place to prevent that are just as complicated.

Tweaking - September 4, 2016, 1:01 pm

Damn, that's a nice amount of requests.

ZuGgY - September 4, 2016, 8:32 pm

Very interesting stuff to read and know about.

Thank you for the information.

Dagurmeyo - September 4, 2016, 9:36 pm

I don't think there is a need for all those relays which makes the packets travel way too long before reaching the actual server, handling 180 million of requests is usually done with load-balancing and synchronized SQL servers, to balance the load I would setup multiple web servers serving the exact same content and apply multiple IP Addresses on the main DNS so the clients will not always chose the same server and thus balance the load across the servers, as for the SQL Servers there is multiple softwares to synchronize SQL servers and also cache SQL queries which also helps to decrease the load time and save up on resources.

As for preventing possible attack attempts on a web application that you don't code yourself a WAF is indeed the best solution, Cloudflare is really bad at doing this job so I guess that part is to be made with a web-server plugin, or an addon to the web application.

I also wouldnt recommend using multiple reverse proxy services such as Cloudflare and Securi together, better stick with one single CDN/Reverse Proxy, a good one that performs pretty well is Incapsula, but that's only a personal choice.

(Sep 4, 2016 12:23 PM)Omniscient Wrote: [\[CITE\]](#) No tools would be able to penetrate all those layers in that way.

Not how the serving technology works.

One layer calls the next layer which then calls the next layer. Each layer is essentially invisible to that 3rd layer. So yes, if you do by chance get past Cloudflare you'd see the next layer but that wouldn't tell you what's next. Highly unlikely all the layers would get penetrated. And even if they were. Would take me about 15 minutes to change the setup, which is part of my design as well. I can change at least 3 layers IPs on a whim, just in case. And sometimes I do change our IPs a matter of added security, which is why DNS sometimes gets screwy for members. Tunnels and IPs are very easy to change.

First post explains that. Each of these layers is a form of ddos protection. 99% of our protection scheme is automated.

Yup. Custom coding so that we're not always under full protection but when attacks begin protections automatically start. Even better is that when attacks end the protections disable after a time.

Why don't you just white-list access between your servers and blacklist every other traffic on a server that shouldnt get any other then from the other servers?

Changing IP Addresses serves no purpose, that's not what's gonna block any attack on a long term.

FamousHater - September 4, 2016, 9:42 pm

(Sep 4, 2016 09:36 PM)Dagurmeyo Wrote: [\[CITE\]](#) I don't think there is a need for all those relays which makes the packets travel way too long before reaching the actual server, handling 100 million of requests is usually done with load-balancing and synchronized SQL servers, to balance the load I would setup multiple web servers serving the exact same content and apply multiple IP Addresses

on the main DNS so the clients will not always chose the same server and thus balance the load across the servers, as for the SQL Servers there is multiple softwares to synchronize SQL servers and also cache SQL queries which also helps to decrease the load time and save up on resources.

As for preventing possible attack attempts on a web application that you don't code yourself a WAF is indeed the best solution, Cloudflare is really bad at doing this job so I guess that part is to be made with a web-server plugin, or an addon to the web application.

I also wouldnt recommend using multiple reverse proxy services such as Cloudflare and Securi together, better stick with one single CDN/Reverse Proxy, a good one that performs pretty well is Incapsula, but that's only a personal choice.dont think omni needs advice how to run the site. it has excellent up time and speed for all the attacks that happen to it. i do agree there are better options then cloudflare tho

Dagurmeyo - September 4, 2016, 9:45 pm

(Sep 4, 2016 09:42 PM)FamousHater Wrote: [\[CITE\]](#) dont think omni needs advice how to run the site.

it has excellent up time and speed for all the attacks that happen to it.

i do agree there are better options then cloudflare tho

Load should not be reduced by filtering traffic, but only balancing the traffic onto the different servers you have, unless its malicious and spam traffic obviously..

Even if I think that the legit traffic that comes to HackForums alone could totally be served with a simple Nginx server with few SQL servers, problem is that malicious/spam traffic that comes due to the site being a "hacking" forum I guess.

Roy Wood\$ - September 5, 2016, 6:18 am

(Sep 4, 2016 11:13 AM)Omniscient Wrote: [\[CITE\]](#) Glad you asked.

<https://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack/>

Damn im gonna assume that was HF lol. I wonder who was that butthurt to try and fail at taking hf off for long?

Omniscient - September 5, 2016, 7:50 am

Quote: I would setup multiple web servers serving the exact same content and apply multiple IP Addresses on the main DNS

Load balancing is sort of done by Cloudflare. They actually cache a ton of the static content and deliver it from a worldwide network. And as a future step I would consider an actual backend load balance setup if I felt it was required. I dable with load balancing already to see how the effects are and so far it's not helped one bit. Running multiple VPN web servers will not speed up HF or prevent ddos attacks for HF. I'd much rather run a ultra-powerful single web server with another ultra-powerful database server, which is how we're run. We do of course lose a certain amount of redundancy but that's negligible and servers rarely fail.

Quote:I also wouldnt recommend using multiple reverse proxy services such as Cloudflare and Securi together, better stick with one single CDN/Reverse Proxy

Securi is only enabled during the worst of attacks which are getting past Cloudflare.

Quote:Why don't you just white-list access between your servers and blacklist every other traffic on a server that shouldnt get any other then from the other servers?

Oh you're very smart, thanks Captain Obvious.

Quote: Changing IP Addresses serves no purpose, that's not what's gonna block any attack on a long term.

It was never mentioned as part of my DDOS prevention. It is however part of my security setup. And I do have legitimate reasons which I won't go into detail about. You seem smart enough, I bet you can guess.

Be aware that HF has special needs when it comes to security and ddos prevention. I'm positive we experience more DDOS attacks than probably any other website in the world. That's not a boast either because I wish it wasn't. But I believe it's true.

Thanks everyone for a nice thread.