

Forum:[Hack Forums](#)

Thread: [DDOS Protection Changes](#)

Omniscient - May 7, 2015, 11:02 am

Going to have to discuss this openly to members.

Cloudflare has an exploit that's being used to bypass their security. It's related basically to CNAME DNS entries. Basically anyone can setup a cname pointing to HF then attack that cname entry and it will 100% bypass the Cloudflare protection scheme. It's fucked up. It's really fucked up.

I knew about this exploit months ago and reported it to them. At the time they basically dismissed it. I removed any cnames in my own account that I knew were being used to attack HF and it resolved the issue. Then about 2 weeks ago we had the weekend with 2 days of extended downtime. I was actually offline spending time with family.

I sent ticket after ticket to Cloudflare and they were basically clueless and the support person I initially had was a moron. Eventually they bumped up my ticket to higher tech and they stopped the attack. At least it appeared that way.

Over the course of the past 2 weeks the CNAME exploit has repeatedly been used as I believe it's now a little more well-known and actively being used as a Cloudflare bypass in DDOS attacks. This has become a real problem of course as unfortunately over time I've changed my protection scheme so much that I rely in-part with Cloudflare.

Because Cloudflare is a reverse proxy setup the traffic hitting my server requires DPI (Deep Packet Inspection) for the attacking IPs to be stopped at the server firewall level. Otherwise it goes to Apache which even if blocked by Apache still gobbles up resources and chokes the service thus making the denial of service complete. This is what has been happening.

Possible combats to this would be to install some sort of DPI alteration to my server firewall. Possible to do but annoying as fuck and very resource (CPU) intense. It's not optimal. My other option is NGINX reverse proxy which doesn't choke and would likely work to stop the types of attacks that have recently occurred. Last option was to double up the protection that Cloudflare offers by using another reverse proxy and WAF setup such as Sucuri.net.

Yesterday attacks resumed taking us offline once again. Another support ticket with Cloudflare was opened. I let them know point blank about the CNAME exploit and I was offline. Hours passed and still no results.

The problem with successful DDOS attacks against HF is that they just embolden attacks, word spreads, and even more attacks occur. So my main objective when HF is under attack is fast and efficient mitigation. Thwarting attacks is a high priority for me. I not only want the uptime but I also want to show attackers that their efforts are wasted. Our uptime has greatly improved because of that.

Back to Cloudflare...so the attack last night persisted. The support ticket was becoming frustrating. A change was required in order to deal with this. The fastest change I could immediately come up with was Sucuri. So that's what I did. At 10pm last night I paid for a new account, changed server configurations, and began the necessary changes to add their protection into our serving scheme.

So far it's been a reasonable success with a few problems. I think we're going to lose NSFW mode. At least in it's current form.

Sucuri allows me to block countries not just challenge them as Cloudflare does. That means a lot of users are 100% blocked. For now the listed allowed countries is relatively small and I'm sure adjustments will be made.

We still run through Cloudflare for now. I can't be 100% sure I will continue to use them or if I'll downgrade my Business account to just Pro. I'm pretty frustrated that for nearly two weeks they haven't fixed this problem and I'm guaranteed 100% uptime. Even worse is their inept responses to me in support tickets. I've lost faith in their service and that's an understatement.

Going forward I may or may not run both services. I may drop the Business CF account into a simple Pro account. I was already planning on a major change to our servers this summer which may include running Nginx on port 80 and reverse-proxy to Apache. Some wonder why I still run Apache and that's because it does have some very useful modules I use including a couple custom ones I wrote. I just don't have the time or patience to deal with the same type of setup with Nginx. But running it as a reverse-proxy should allow me even more control and another layer of protection.

I've had a sleepless night and hoping to do all I can today to get things working as best as possible but changes will occur and odd behaviors will happen. Feel free to report them to me either directly or through PM. I'm likely going to be agitated all day over this. I'm less than pleased at Cloudflare and so far I can already see limitations and problems with Sucuri.

On a final note: Many of you have been reporting to me incorrectly the exploit and what you deem as fixes. Most of these reports don't understand the attack (skids). Many of those don't understand that I already block the traffic at the service level but Apache SUCKS and if you have 5000 IPs coming in it will choke hardcore despite my efforts. And without DPI at the server firewall level the traffic can't be stopped. This was a complete failure of Cloudflare whose protection scheme I've paid for and failed. I put that downtime on them. I made them aware of the problem months ago. Before 99% of those using the exploit even knew it existed.

Thanks to everyone who has assisted and supported HF. Let's hope our uptime gets to 99.9%.

Spoiler ([Click to View](#)) Fuck sleep. Coffee day

Krew - May 7, 2015, 11:06 am

Damnit, that sucks. Would you advise other webmasters to use Sucuri over CloudFlare as well? I assume you would since Cloudflare has clearly been lacking.

Captain Steve Rogers - May 7, 2015, 11:10 am

If there is a good alternative for CF then go for it, CF sucks!

Angel Beats?? - May 7, 2015, 11:18 am

Omni you could just return 444 to any attacks with incorrect hosts. That should have been enough.

Omniscient - May 7, 2015, 11:25 am

Quote:Omni you could just return 444 to any attacks with incorrect hosts. That should have been enough.

And that's the kind of response that I'm talking about. Any blocking at the service level (Apache) is ineffective. Apache still opens the connection and makes the response. It's the weak point in my setup. Either you're a skid and you don't understand what I stated clearly above or you just didn't

read it. Which is it?

Quote:Omni, are you able to design the firewall page that the new system throws at us?
It doesn't appear that I have that ability. The white page is annoying and I think that's when their protection is triggered. Just need to figure out the best way to alter things without actually removing valuable protection. Sucuri definitely has their limitations and I have to figure out how to work around them.

HF is a very different beast. We're huge, we have lots of traffic, we have lots of pages, and we have lots of custom needs.

Gook - May 7, 2015, 11:31 am

Is there no other option then cloudflare/Sucuri for you?

How can such a big company let something like this happen, its a serious "bug/exploit"

Are all attacks to HF done like this?

webdev77 - May 7, 2015, 11:32 am

(May 7, 2015 11:31 AM)Gook Wrote: [CITE](#) Is there no other option then cloudflare for you?

Is that a serious question? Of course there are other options, but they aren't going to be simply a matter of paying a few bucks for a different service.

Who Soup - May 7, 2015, 11:33 am

I was just about to ask about all of these recent attacks, hf has been downed a lot recently I'm glad that this issue is being fixed though.

N1nj4Styl3 - May 7, 2015, 11:33 am

That pretty summed up everything that has been happening the past 2 weeks.

Thanks for letting us know Omniscient, keep up the good work. Hope this stops immediately and a solution rises by CF's side.

Roger Waters - May 7, 2015, 11:35 am

While trying to make a response to this thread I've received two gateway errors and I've lost everything I typed up. Grrr... Fuck CloudFlare.

Omniscient - May 7, 2015, 11:35 am

Quote:Is there no other option then cloudflare for you?

Are you another idiot that didn't read or understand my first post?

Quote:That pretty summed up everything that has been happening the past 2 weeks.
Not a summary. It was a full disclosure explanation. If anyone read it and didn't understand it then they are not well-versed as a sysadmin.

Angel Beats?? - May 7, 2015, 11:37 am

I'm sorry I haven't used apache for such a long time I didn't realise it was that much worse than nginx, I thought you were doing something different as protection. my bad.

Duck On Quack - May 7, 2015, 11:37 am

Nice changes, seems alot more stable now except the white pages. Not a big issue though already got a script that refreshes if it runs into them (fairly unstable):P

N1nj4Styl3 - May 7, 2015, 11:38 am

(May 7, 2015 11:35 AM)Omniscient Wrote: [\[CITE\]](#) Not a summary. It was a full disclosure explanation. If anyone read it and didn't understand it then they are not well-versed as a sysadmin. And that's enough I suppose. At least most of us got a taste of what have you been through with CF and what are your future plans on getting this fixed.

I see nothing missing.

Krew - May 7, 2015, 11:39 am

*ignored

Anyway, I am getting this more than often & results in page freezes.

<https://imgur.com/BPczxbI>

eXero - May 7, 2015, 11:40 am

Fuck Cloudflare. Buy them out and shut them down!

sqsgkrIhdwg - May 7, 2015, 11:44 am

So actually you run both CloudFlare and Sucuri ? And CloudFlare is the front proxy ?

If I understand correctly, when you use both services sometimes cloudflare returns his cache without asking sucuri ... That's why we had odd issues.

I just went through ten 502 cloudflare error pages without being able to access the site right now.

I know how you feel about the CNAME exploit. So simple but yet not fixed ... At the same time, if they fix it let's say by forcing the proxy-mode when the domain is not the same, it would also take down the mail reverse ...

Milk™ - May 7, 2015, 11:46 am

Important to spend time with your family ofc. But I'm so thankful that you made this community :)

Omniscient - May 7, 2015, 11:48 am

Quote:So actually you run both CloudFlare and Sucuri ? And CloudFlare is the front proxy ?
Correct.

Quote:when you use both services sometimes cloudflare returns his cache without asking sucuri ...
That's why we had odd issues.

Correct as well that's why last night I altered how the cache works. Seems all good now.

240sx - May 7, 2015, 11:53 am

I only got a MySQL error last night and that's about it.

Code SQL Error:

2006 - MySQL server has gone away

Query:

```
SELECT * FROM mybb_sessions WHERE sid='a8ef3556434c1ad416807de1b37872d0' AND  
ip='fuck off' LIMIT 1
```

Probably the time you were changing servers I presume.

+One - May 7, 2015, 11:56 am

As xadamx said, you're really working hard to improve the website. This will also make it easier for you to maintain the website at its best. Cheers ?

sqsgkrIhdwg - May 7, 2015, 11:57 am

(May 7, 2015 11:53 AM)Badger Wrote: [\[CITE\]](#) I only got a MySQL error last night and that's about it.

Code SQL Error:

2006 - MySQL server has gone away

Query:

```
SELECT * FROM mybb_sessions WHERE sid='a8ef3556434c1ad416807de1b37872d0' AND  
ip='fuck off' LIMIT 1
```

Probably the time you were changing servers I presume.

It's really a bad idea to show your session ID.

Someone could connect to your account if it still valid.

I suggest you reconnect before it happens.

haydrazs - May 7, 2015, 11:57 am

Damn this sucks alot, hope fully it will be fixed :)

Omniscient - May 7, 2015, 11:57 am

(May 7, 2015 11:53 AM)Badger Wrote: [\[CITE\]](#) I only got a MySQL error last night and that's about it.

Code SQL Error:

2006 - MySQL server has gone away

Query:

```
SELECT * FROM mybb_sessions WHERE sid='a8ef3556434c1ad416807de1b37872d0' AND  
ip='fuck off' LIMIT 1
```

Probably the time you were changing servers I presume.

Sessions table was truncated a couple times to speed up the correction of the cross-login problems.

240sx - May 7, 2015, 11:58 am

(May 7, 2015 11:57 AM)L-EARN Wrote: [\[CITE\]](#) It's really a bad idea to show your session ID.

Someone could connect to your account if it still valid.

I suggest you reconnect before it happens.

Expired doesn't matter lol.

(May 7, 2015 11:57 AM)Omniscient Wrote: [\[CITE\]](#) Sessions table was truncated a couple times to speed up the correction of the cross-login problems.

Ah alright thanks for the information Omni.

?

Royal ! - May 7, 2015, 12:11 pm

Amazing skills Omni ? . Right now, for me HF is working totally smooth without any issues at all.

Also I wonder what those kids out there gain by ddosing HF?. They already must know that they just can't Succeed because HF is owned and maintained by an amazing tech person who is extremely dedicated to whatever he does.

Bluffer - May 7, 2015, 12:21 pm

Awesome I was wondering why HF went down right as I was sending a PM yesterday.

Glad that you are doing your best to fix it.

Condoms - May 7, 2015, 12:31 pm

Are you still planning on using the Google service or is that a entirely different topic?

Dean Winchester? - May 7, 2015, 12:34 pm

"Gateway time-out"

slow clap

just kidding it just lasted half a second but still ?

maybe you updated something for all i know

Abraham Lincoln - May 7, 2015, 12:34 pm

(May 7, 2015 12:31 PM)Condoms Wrote: [\[CITE\]](#) Are you still planning on using the Google service or is that a entirely different topic?

I think that's a different topic. That requires a time to get added to the program, while right now he's just looking for instant protection.

G???????f????s? - May 7, 2015, 12:37 pm

If you ask me, you should ditch C.F. completely. I'm not a big web dev but I'm fairly sure you can just copy the files from CF over to a vps with great specs and great ddos protection and staff that actually give a Fuck about what they're doing.

Omniscient - May 7, 2015, 12:44 pm

(May 7, 2015 12:37 PM)G???????f????s? Wrote: [\[CITE\]](#) If you ask me, you should ditch C.F. completely. I'm not a big web dev but I'm fairly sure you can just copy the files from CF over to a vps with great specs and great ddos protection and staff that actually give a Fuck about what they're doing.

?

?

?

?

???

That was my reaction in smiley version.

Joshz - May 7, 2015, 12:48 pm

I received an nginx 405 not allowed error today for around 2 minutes while attempting to pm someone. It's a new error I haven't seen before, only happened once. The regular reported error has happened less but still occasionally.

I don't know much about website protection. That said, maybe consider using something other than cloud flare? They really are quite incompetent.

Meow - May 7, 2015, 12:49 pm

Good thing you did this Omni,I saw some other popular forums (MPGH..) getting ddosed even tho they have CF protection. ?

More and more people know about that exploit..

Datageni - May 7, 2015, 12:53 pm

Thanks for letting us know, Omni.

ZuGgY - May 7, 2015, 12:56 pm

Thanks for the update/information.

Sad about NSFW :(

G???????f????s? - May 7, 2015, 12:57 pm

(May 7, 2015 12:44 PM)Omniscient Wrote: [\[CITE\]](#) ?

?

?

?

???

That was my reaction in smiley version.
I specialize in full retard.

Repeat - May 7, 2015, 12:57 pm

I am happy that you didn't destroy the website. ?

haydrazs - May 7, 2015, 12:57 pm

(May 7, 2015 12:37 PM)G???????f????s? Wrote: [\[CITE\]](#) If you ask me, you should ditch C.F. completely. I'm not a big web dev but I'm fairly sure you can just copy the files from CF over to a vps with great specs and great ddos protection and staff that actually give a Fuck about what they're doing.

oh god did you just make all of that up to appear like you had a valid opinion on this subject?

--

oh and i'm slightly confused, the problem is mostly fixed now?

G???????f????s? - May 7, 2015, 12:59 pm

(May 7, 2015 12:57 PM)Haydrazs Wrote: [\[CITE\]](#) oh god did you just make all of that up to appear like you had a valid opinion on this subject?

--

oh and i'm slightly confused, the problem is mostly fixed now?

I made that up because I'm stupid

C?a?r?bon - May 7, 2015, 1:33 pm

(May 7, 2015 11:25 AM)Omniscient Wrote: [\[CITE\]](#) And that's the kind of response that I'm talking about. Any blocking at the service level (Apache) is ineffective. Apache still opens the connection and makes the response. It's the weak point in my setup. Either you're a skid and you don't understand what I stated clearly above or you just didn't read it. Which is it?

Killed him with knowledge ?

Repeat - May 7, 2015, 1:42 pm

Have you tried politely asking them to stop the DDoS?

'An0ny - May 7, 2015, 1:48 pm

CloudFlare have been working fine till now, this exploit & the other cf bypass are both working fine to bypass CloudFlare. But there are some rules you could do to prevent it, which hes doing now.

I am using CloudFlare free fine, i think PRO would be more than enough as they've also increased the r/s limit.

Omniscient - May 7, 2015, 1:51 pm

Quote:Have you tried politely asking them to stop the DDoS?

I would never engage in a discussion with anyone attacking HF.

Quote:CloudFlare have been working fine till now, this exploit & the other cf bypass are both working fine to bypass CloudFlare. But there are some rules you could do to prevent it, which hes doing now.

How I'm currently setup the bypass is effective. I relay that info in the first post. The amount of traffic hitting Apache chokes it. So ANY suggestion to use .htaccess or any Apache based rule will not be effective. I've tried to make that clear and people still send me the suggestion.

lemmon - May 7, 2015, 1:56 pm

(May 7, 2015 12:37 PM)G???????f????s? Wrote: [\[CITE\]](#) If you ask me, you should ditch C.F. completely. I'm not a big web dev but I'm fairly sure you can just copy the files from CF over to a vps with great specs and great ddos protection and staff that actually give a Fuck about what they're doing.

This post seriously hurt my face.

'An0ny - May 7, 2015, 1:56 pm

(May 7, 2015 01:51 PM)Omniscient Wrote: [\[CITE\]](#) How I'm currently setup the bypass is effective. I relay that info in the first post. The amount of traffic hitting Apache chokes it. So ANY suggestion to use .htaccess or any Apache based rule will not be effective. I've tried to make that clear and people still send me the suggestion.

I think what you are doing now should be fine, hopefully CloudFlare will prevent this. I think that white page / cookie check is annoying people, but i'd rather see a white page here and there than downtime.

Any certain reason you are using Apache? I've had nothing but issues with Apache when getting attacks. It kills it easily. I am using plain nginx my self, and set up my own rule(s) to prevent it which so far seems to work.

lemmon - May 7, 2015, 1:58 pm

(May 7, 2015 01:48 PM)An0ny Wrote: [\[CITE\]](#) CloudFlare have been working fine till now, this exploit & the other cf bypass are both working fine to bypass CloudFlare. But there are some rules you could do to prevent it, which hes doing now.

I am using CloudFlare free fine, i think PRO would be more than enough as they've also increased the r/s limit.

Someone probably hasn't hit your site with a big enough botnet then, Cloudflare Free wont protect your site with that much traffic with or without the exploit.

'An0ny - May 7, 2015, 1:59 pm

(May 7, 2015 01:58 PM)cowe Wrote: [\[CITE\]](#) Someone probably hasn't hit your site with a big enough botnet then, Cloudflare Free wont protect your site with that much traffic with or without the exploit. CloudFlare free or pro or business has no difference if this exploit is out. So I don't understand your statement.

lemmon - May 7, 2015, 1:59 pm

(May 7, 2015 01:56 PM)An0ny Wrote: [\[CITE\]](#) Any certain reason you are using Apache? I've had nothing but issues with Apache when getting attacks. It kills it easily. I am using plain nginx my self, and set up my own rule(s) to prevent it which so far seems to work.

He mentioned that he wrote modules and enjoys the features for apache in a previous post.

'An0ny - May 7, 2015, 2:00 pm

(May 7, 2015 01:59 PM)cowe Wrote: [\[CITE\]](#) He mentioned that he wrote modules and enjoys the features for apache in a previous post.

Yup, just took me time to read the entire topic.

Maybe one day you'll move to Nginx ?

Using nginx as front end proxy should prevent it/stop the attacks/decrease.

Abraham Lincoln - May 7, 2015, 2:13 pm

(May 7, 2015 01:59 PM)An0ny Wrote: [\[CITE\]](#) CloudFlare free or pro or business has no difference if this exploit is out. So I don't understand your statement.

Pro costs much less than a business account.

All you get is better support (which he feels is bad and not worth it)

Omniscient - May 7, 2015, 2:24 pm

Quote:Any certain reason you are using Apache? I've had nothing but issues with Apache when getting attacks.

Realize I've been using Apache since before Nginx was even a project. I know it's not optimal for my environment but certain things I still need it for. All my custom stuff is written as Apache modules which won't be easy, fun, or quick to write for Nginx.

Quote:Maybe one day you'll move to Nginx

After the 2nd downtime we had a couple weeks ago I realized I needed to add it to prevent these attacks. I don't have time though to really do what I need so for now it's a double ddos protection.

Quote:Using nginx as front end proxy should prevent it/stop the attacks/decrease.

Correct. As well as give me other control options as well. It's not a matter of knowing how to do it...it's a matter of having the time to make the changes. Especially considering I already plan hardware changes this summer. I'm going to wait till that happens before change more deeply our serving structure.

Quote:Pro costs much less than a business account.

It's not about cost me for me on this. It's more that I don't want to see CF get money for a service it doesn't actually provide. I'm contemplating calling them out on their 100% uptime guarantee but for now I'd rather keep my friendly disposition with them while I still use their service.

'An0ny - May 7, 2015, 2:46 pm

(May 7, 2015 02:24 PM)Omniscient Wrote: [\[CITE\]](#) -Understandable, i assume once you get some time you'll move to Nginx one day. I would assume this would save the server a lot of resource usage, and possibly costs.

What you are using now should be fine, let's hope CloudFlare get their asses and fix this stupid "exploit". Can barely call it exploit, embarrassing for them.

:) sucks I couldn't help.

bfreakz - May 7, 2015, 3:01 pm

I was unable to access HF for about 24 hours. Kept saying my country was blocked, however now it works? Can you give any input Omni. I know you don't discuss country bans, but I really can't afford paying a VPN to access HF if this will keep happening.

Blazin - May 7, 2015, 4:02 pm

This sucks hope you get it all sorted Omni

Omniscient - May 7, 2015, 6:13 pm

(May 7, 2015 03:01 PM)Modovich Wrote: [\[CITE\]](#) I was unable to access HF for about 24 hours. Kept saying my country was blocked, however now it works? Can you give any input Omni. I know you don't discuss country bans, but I really can't afford paying a VPN to access HF if this will keep happening.

Obvious. Your country was blocked. Now it's not.

Charlemagne - May 7, 2015, 6:15 pm

I am trying to think of some way that would fix this, but I know nothing about web development. All I can offer you, Omni, is a wish of luck when trying to fix this.

Doxicity - May 7, 2015, 6:25 pm

Sucks to hear this, but I'm sure you'll fix it all in due time.

Serious question though, does this mean Chile has been blocked again?

Canonsx130 - May 7, 2015, 6:51 pm

A very nice read. You should sticky this and give yourself the sticky award. This was very informative.

EDIT: It's stuck already. Thanks :D

Prince™ - May 7, 2015, 7:49 pm

Damn, looks like you spent a hell of a time with Cloudflare support to get this resolved.

Good to see HF back on track Omni, thank you!

VodkaNik - May 7, 2015, 8:26 pm

By creating this thread your probably going to have a wave of kids doing the exploit if not new ones.

Best of luck

0x1027 - May 8, 2015, 2:01 am

Is it just me that been having this problem atm. When I click the logo or home button. EVERY time I have to wait 6-7 to be re verified. Is that a bug with cloud flare?

Omniscient - May 8, 2015, 11:20 pm

I just went through my past trouble ticket with Cloudflare. It was in Dec of 2014 I said this to them:

Quote:Also I suspected origins were from a cname entry I have with hackforums.com (CF hosted DNS) which aliases to hackforums.net.

If that's the cause and it bypasses the Cloudflare WAF rules then I have to assume this is an exploitable bug as anyone can create a cname at any domain then attack it through that method to bypass the WAF.

Please investigate this.

And...

Quote:My concern though is that the cname, which anyone can setup, bypassed the WAF. This is alarming behavior unless because it was on my own CF account that you allowed the bypass.

One would hope that cname or not any traffic hitting the domain would go through the filter. I'm a bit

puzzled by this and maybe you can forward this to some engineers for review.
To which they responded....

Quote:Understood, and thank you for clarifying. I am discussing this issue with our engineers, and I'll get back to you as soon as we've taken a look.

After that nothing. Obviously 5 months later and it's not fixed and the exploit is more widely known. I'm actually hoping by making this public that Cloudflare manages to address it now and deal with it.

For us, I'm still reviewing the setup we have and I don't like it. Changes will need to be made to fit my requirements. Well at least I got Gauth a handful of other things done first. :(I have a feeling my next couple weeks are going to suck for me with heavy workload.

N1nj4Styl3 - May 8, 2015, 11:24 pm

Omni, have you tried calling them? This might work as it does with PayPal once chargebacks/limits happen.. there's a better communication, you know. Calling them might help I guess. (I know they do not offer support through phone, but there's one in Whois information.. I suppose?)

Found this: +1.6503198930

Syracusia - May 8, 2015, 11:29 pm

There is a fundamental problem in CloudFlare's system that allows these attacks to happen. Their current setup of how they manage the domains in correlation with their protection and CDN is great for simple use. Although it needs to be revised so requests under a separate domain which may cname to a victim's servers, still SHOULD go through the standard DPI associated with the legitimate CF user.

It seems that the CF service simply looks at the requested domain, and applies the relevant CF configurations and optimizations including firewall with that domain record.

Although what seems to be fundamentally wrong, as you noted in your OP, is that if the domain is simply appointing to let's say hackforums.net under cname.attackerswebsite.com then Cloudflare will only apply the rules for "cname.attackerswebsite.com" which the attacker can set to no security.

I believe that is the issue, which they MUST fix otherwise their service is essentially useless.

I will tweet to the owner, he currently follows me on Twitter.

(May 8, 2015 11:24 PM)N1nj4Styl3 Wrote: [\[CITE\]](#) Omni, have you tried calling them? This might work as it does with PayPal once chargebacks/limits happen.. there's a better communication, you know. Calling them might help I guess. (I know they do not offer support through phone, but there's one in Whois information.. I suppose?)

Calling them, MAY be effective, although he has illustrated that the support system is futile.

Charging back is just ignorant.

The only effective option at this point would be to go public, as Omni has done on this forum with the issue.

Perhaps a blog post on a major security website would make a call to action for CF.

Negative publicity towards CF will bring their attention to the issue. As they care about the \$, you must remember CF is a business.

(May 8, 2015 11:20 PM)Omniscient Wrote: [\[CITE\]](#) I just went through my past trouble ticket with Cloudflare. It was in Dec of 2014 I said this to them:

And...

To which they responded....

After that nothing. Obviously 5 months later and it's not fixed and the exploit is more widely known. I'm actually hoping by making this public that Cloudflare manages to address it now and deal with it.

For us, I'm still reviewing the setup we have and I don't like it. Changes will need to be made to fit my requirements. Well at least I got Gauth a handful of other things done first. :(I have a feeling my next couple weeks are going to suck for me with heavy workload.

On a second thought, I have an idea for how we can stop these attacks.

I assume it is some form of XML-RPC or other Layer 7 attack.

Since all of the attacks are coming from example.attackerswebsite.com they would be easy to isolate.

You could then make a script that would grab ALL of the IPs with that criteria, as they would only be malicious connections.

You could then firewall the IPs upstream by contacting your DC, or even at the layer 4 which wouldn't use too much CPU time.

Figm3ntation - May 8, 2015, 11:44 pm

Sorry, I'm not a professional or anything and I don't really understand everything but why not replace Apache with NGINX? NGINX isn't that hard to learn and setup plus the ability to use it as a firewall.

Have you tried Incapsula?

Omniscient - May 8, 2015, 11:46 pm

Quote:Although what seems to be fundamentally wrong, as you noted in your OP, is that if the domain is simply appointing to lets say <https://hackforums.net> under cname.attackerswebsite.com then cloudflare will only apply the rules for "cname.attackerswebsite.com" which the attacker can set to no security.

My guess exactly. And in December when I pointed it out they could have looked into it. This week when I spelled it out for them they SHOULD have looked into it...they didn't. They should have corrected this by now. They haven't.

I'm fairly certain that eventually they will and the sooner the better. I'm just rather disappointed that I was forced to use another service for a service I pay Cloudflare for.

Quote:Since all of the attacks are coming from example.attackerswebsite.com they would be easy to isolate.

Isolating them isn't the problem. The problem is what to do with the IPs and block it before it hits the service level (Apache). I outlined in the first post that I have 2 basic options. Setup DPI (deep packet inspection) so I can firewall block at my server, which because all traffic come from Cloudflare a requires special setup. Or to run Nginx as a reverse proxy on port 80 and send legit traffic to Apache on another port. Likely the Nginx reverse proxy will be easier to setup and I'm guessing by the amount of traffic that it will be effective enough to stop the attacks effectiveness.

This was my biggest fear when I moved to Cloudflare. That I would have to rely on their protection

scheme because it's either you trust and accept their packets or your site goes offline. Up till now they've done a reasonably good job. I have no idea why they are dropping the ball now. I do notice that some of the people I speak with in Support do not seem as knowledgeable.

btw I already run Nginx on the server for our static content. Unfortunately had to disable it because Sucuri will only secure port 80. I just know I have a lot of work in front of me to get HF running as I need.

Syracusia - May 8, 2015, 11:53 pm

(May 8, 2015 11:46 PM)Omniscient Wrote: [\[CITE\]](#) My guess exactly. And in December when I pointed it out they could have looked into it. This week when I spelled it out for them they SHOULD have looked into it...they didn't. They should have corrected this by now. They haven't.

I'm fairly certain that eventually they will and the sooner the better. I'm just rather disappointed that I was forced to use another service for a service I pay Cloudflare for.

Isolating them isn't the problem. The problem is what to do with the IPs and block it before it hits the service level (Apache). I outlined in the first post that I have 2 basic options. Setup DPI (deep packet inspection) so I can firewall block at my server, which because all traffic come from Cloudflare a requires special setup. Or to run Nginx as a reverse proxy on port 80 and send legit traffic to Apache on another port. Likely the Nginx reverse proxy will be easier to setup and I'm guessing by the amount of traffic that it will be effective enough to stop the attacks effectiveness.

This was my biggest fear when I moved to Cloudflare. That I would have to rely on their protection scheme because it's either you trust and accept their packets or your site goes offline. Up till now they've done a reasonably good job. I have no idea why they are dropping the ball now. I do notice that some of the people I speak with in Support do not seem as knowledgeable.

Ah, I see a problem now with my potential solution of isolating the attacking IP addresses. Even though it bypasses the CF protection, they would still be coming from CF ip addresses so you can't simply block all connections from the malicious IP addresses. As they would simply be under the CF server's IPs.

What I was thinking, before realizing that was that we could contact your DC and have them just plain block the connections from those IP address before they reach your server, but I see now that is impossible.

CF, is actually HELPING with the attack in this instance as it makes the attacks unable to be fire walled by IP address.

To firewall the attacks, every request must be analyzed which would be very costly, and something that CF SHOULD be doing.

The NGINX solution would be effective in moving the server load from your main content server, although I would hope that we wouldn't have to go to such a measure for a problem that CF should be able to resolve.

What happens when they start attacking your NGINX reverse proxy? If you set up some form of DPI software/firewall here it would also eat a ton of CPU resources on the nginx machine.

Which wouldn't be a problem, but it would just be expensive to have another server running when you are paying for a service which should be doing this already.

Also that would be another step of latency that we shouldn't have.

CF is supposed to speed things up, not allow hackers to get whitelisted IP address attacks on us and then make us add another relay.

The most effective solution at this point, is to make the issue known by some big security blogs/news.

One other option is to make the nginx server in the same DC as your content server(s) then relay the clean data over a local network for less latency increase.

Syracusia - May 8, 2015, 11:58 pm

(May 8, 2015 11:44 PM)Figm3ntation Wrote: [\[CITE\]](#) Sorry, I'm not a professional or anything and I don't really understand everything but why not replace Apache with NGINX? NGINX isn't that hard to learn and setup plus the ability to use it as a firewall.

Have you tried Incapsula?

What the fuck? Simply using NGINX wouldn't solve this problem.

It's not an exploit manifesting from the apache server.

It's the fact that the server is having to process thousands of malicious requests every second.

Vip?r - May 9, 2015, 12:05 am

Damn Omni works way too hard for us, thanks man.

SIM-297877 - May 9, 2015, 12:06 am

I am not sure i will ever understand the point in DDoS attacks. Anyways good luck, hope CF gets there shit fixed.

Syracusia - May 9, 2015, 12:10 am

(May 9, 2015 12:06 AM)SaturnsVoid Wrote: [\[CITE\]](#) I am not sure i will ever understand the point in DDoS attacks. Anyways good luck, hope CF gets there shit fixed.

The point is that the website is offline, which is what the hackers want.

Omniscient - May 9, 2015, 12:11 am

Quote:CF, is actually HELPING with the attack in this instance as it makes the attacks unable to be fire walled by IP address.

Essentially true. Because I can't stop an attack with my server firewall without special alterations. The benefit of Sucuri is that they have the DPI setup already and already do an Nginx reverse proxy.

Quote:The NGINX solution would be effective in moving the server load from your main content server, although I would hope that we wouldn't have to go to such a measure for a problem that CF should be able to resolve.

I'm giving them another week to resolve this. I updated my ticket with them already. Unfortunately it's the weekend now so I may not get results for a few days.

Quote:What happens when they start attacking your NGINX reverse proxy?

Nginx handles more connections. At least it should. And I can block the IPs and certain attack patterns at the proxy level.

Quote:What the fuck? Simply using NGINX wouldn't solve this problem.

Technically it should based on the size and patterns of these attacks I'm fairly confident I could

actually mitigate the attacks.

The way I have Apache setup is kind of retarded but it's just part of my legacy setup that I haven't had time to fully alter. I plan to redo the entire backend this summer (coming up fast). This whole problem is ing up my timeframe to get the work done.

Syracusia - May 9, 2015, 12:20 am

(May 9, 2015 12:11 AM)Omniscient Wrote: [\[CITE\]](#) Essentially true. Because I can't stop an attack with my server firewall without special alterations. The benefit of Sucuri is that they have the DPI setup already and already do an Nginx reverse proxy.

I'm giving them another week to resolve this. I updated my ticket with them already. Unfortunately it's the weekend now so I may not get results for a few days.

Nginx handles more connections. At least it should. And I can block the IPs and certain attack patterns at the proxy level.

Technically it should based on the size and patterns of these attacks I'm fairly confident I could actually mitigate the attacks.

The way I have Apache setup is kind of retarded but it's just part of my legacy setup that I haven't had time to fully alter. I plan to redo the entire backend this summer (coming up fast). This whole problem is ing up my timeframe to get the work done.

Essentially true. Because I can't stop an attack with my server firewall without special alterations. The benefit of Sucuri is that they have the DPI setup already and already do an Nginx reverse proxy."

Yeah I was reading an article by them the other day in which they developed a firewall solution for a customer which was facing similar problems to you.

"

I'm giving them another week to resolve this. I updated my ticket with them already. Unfortunately it's the weekend now so I may not get results for a few days.

"

That should be more than enough time for them, you are and have been very reasonable with them. If it was me I would have dropped them within 24 hours of no resolution.

"

Nginx handles more connections. At least it should. And I can block the IPs and certain attack patterns at the proxy level. "

Well I personally use NGINX for all of my websites due to its optimizations for my non PHP files.

Although technically Apache could be more effective for a website which is mainly PHP based.

As Nginx has to use php-fpm which is another application server for the PHP scripts, while apache has built in processing for php.

There is a lot of data which shows that Apache performs better than nginx for delivery of php scripts.

I am looking at a study right now which shows, Apache performed about 40% better than nginx in regards to PHP.

So for a forum, your apache setup isn't as bad as you think. In fact it might be a lot better.

" And I can block the IPs and certain attack patterns at the proxy level.

Technically it should based on the size and patterns of these attacks I'm fairly confident I could actually mitigate the attacks."

Although that would be one benefit of running an nginx website.

Here is a link to an article showing the benefits of nginx vs apache
http://blog.a2o.si/2009/06/24/apache-mod_php-compared-to-nginx-php-fpm/

" I plan to redo the entire backend this summer (coming up fast). This whole problem is ing up my timeframe to get the work done."

We should take into account the possible benefits of these changes to ensure the changes are actually effective.

As it will take some to develop everything so that the migration is seem less for our users, we must make sure the changes we are making are effective.

We can run some tests over summer and collect performance data.

Also lets do the rework on an alternate server so there is no downtime, once we have tested and ensured everything is working then we can migrate the solution onto our main content server.

I would definitely be able to custom develop a firewall system for you over summer

AlphaDelta - May 9, 2015, 12:30 am

(May 8, 2015 11:58 PM)Novaly Wrote: [\[CITE\]](#) What the fuck? Simply using NGINX wouldn't solve this problem.

It's not an exploit manifesting from the apache server.

It's the fact that the server is having to process thousands of malicious requests every second. You don't solve DDoS attacks you mitigate them, which using NGINX over Apache would actually do to some degree.

HF at this time runs on Apache 2.2.22 (Debian) [which apparently has some denial of service problems](#).

Syracusia - May 9, 2015, 12:33 am

(May 9, 2015 12:30 AM)AlphaDelta Wrote: [\[CITE\]](#) You don't solve DDoS attacks you mitigate them, which using NGINX over Apache would actually do to some degree.

HF at this time runs on Apache 2.2.22 (Debian) [which apparently has some denial of service problems](#).

Please don't talk about a topic you are ignorant on.

You mitigate attacks, by solving how they work and making a SOLUTION. This isn't just adding some reverse proxy which can handle a 50Gb/s layer 4 flood. This is solving how we can detect and firewall these attacks before they hit the server.

You fail to understand that the attack is not manifesting from a vulnerability in Apache itself.

Omniscient - May 9, 2015, 12:33 am

Read about PFSense <https://www.pfsense.org> I would love to play around with that.

Quote:Although technically Apache could be more effective for a website which is mainly PHP based.

Which is why I still use and even to a degree, require Apache. We are a heavily php based site.

Quote:So for a forum, your apache setup isn't as bad as you think. In fact it might be a lot better. I like Apache a lot. I have no plans to drop it. Just put Nginx in front of it. Dynamic content shouldn't be served by Nginx. Just not how it should be done.

Quote:We can run some tests over summer and collect performance data.

Also lets do the rework on an alternate server so there is no downtime, once we have tested and ensured everything is working then we can migrate the solution onto our main content server.

There are lot of "we" in that statement.

Syracusia - May 9, 2015, 12:35 am

(May 9, 2015 12:33 AM)Omniscient Wrote: [\[CITE\]](#) Read about PFSense <https://www.pfsense.org> I would love to play around with that.

Which is why I still use and even to a degree, require Apache. We are a heavily php based site.

I like Apache a lot. I have no plans to drop it. Just put Nginx in front of it. Dynamic content shouldn't be served by Nginx. Just not how it should be done.

There are lot of "we" in that statement.

I will begin researching into pfSense.

Agreed, that is how the ideal website should operate. Nginx for static Apache for dynamic

And yes a lot of "we" as I believe I have a lot to offer and could help you make an amazing web solution.

I have an understanding of how these attacks work from the ground up and how to develop solutions to detect and stop them.

Omniscient - May 9, 2015, 12:45 am

Quote:And yes a lot of "we" as I believe I have a lot to offer and could help you make an amazing web solution.

Yeah but no. Sorry but no one touches my configuration.

Quote:I have an understanding of how these attacks work from the ground up and how to develop solutions to detect and stop them.

I don't have need for your help but I'm sure a lot of members do. You should offer them help since they might be more receptive to it.

clark.dll - May 9, 2015, 12:48 am

Fucking losers with nothing better to do than target a site they were probably banned from. Sorry you have to go through all of this shit just because somebody has too much time on their hands.

Thanks for giving us more information regarding the downtime.

Syracusia - May 9, 2015, 12:51 am

(May 9, 2015 12:45 AM)Omniscient Wrote: [\[CITE\]](#) Yeah but no. Sorry but no one touches my configuration.

I don't have need for your help but I'm sure a lot of members do. You should offer them help since they might be more receptive to it.

I understand completely, I am the same way.

Figured I would give the offer.

Please keep in touch with me though, despite not being able to work together we can still bounce ideas off each other.

My email is: theonlineservices@gmail.com

I can send you other contact information if you prefer another method.

Hope you make an effective solution! ?

AlphaDelta - May 9, 2015, 12:52 am

(May 9, 2015 12:33 AM)Novaly Wrote: [\[CITE\]](#) Please don't talk about a topic you are ignorant on.

You mitigate attacks, by solving how they work and making a SOLUTION. This isn't just adding some reverse proxy which can handle a 50Gb/s layer 4 flood. This is solving how we can detect and firewall these attacks before they hit the server.

You fail to understand that the attack is not manifesting from a vulnerability in Apache itself.

Sweetheart I wasn't implying the problem was a result of an vulnerability of Apache I was merely pointing out the fact that the server software was outdated and it was unrelated to your reply, it was my fault for structuring my response in a way that it could have been easily misconstrued.

You have however pointed out that I was wrong about my initial point, thank you for that, but you worded it in a way that is insulting and I'd just like to point out that if it were intentional I'd advise you to talk a little bit nicer, people aren't going to listen to you if you're insulting or talking down to them.

Syracusia - May 9, 2015, 12:54 am

(May 9, 2015 12:52 AM)AlphaDelta Wrote: [\[CITE\]](#) Sweetheart I wasn't implying the problem was a result of an vulnerability of Apache I was merely pointing out the fact that the server software was outdated and it was unrelated to your reply, it was my fault for structuring my response in a way that it could have been easily misconstrued.

You have however pointed out that I was wrong about my initial point, thank you for that, but you worded it in a way that is insulting and I'd just like to point out that if it were intentional I'd advise you to talk a little bit nicer, people aren't going to listen to you if you're insulting or talking down to them.

Sorry if I come off blunt, I just don't sugarcoat stuff. Not because I don't want to, simply because it is unnecessary for me to.

Dan. - May 9, 2015, 1:37 am

I assume you're not a litespeed fan.

Angel Beats?? - May 9, 2015, 5:23 am

(May 8, 2015 11:58 PM)Novaly Wrote: [\[CITE\]](#) What the fuck? Simply using NGINX wouldn't solve this problem.

It's not an exploit manifesting from the apache server.

It's the fact that the server is having to process thousands of malicious requests every second. Actually having nginx as the frontend would help a huge amount, you could block incorrect host records with ease, while using barely any resources.

'An0ny - May 9, 2015, 7:21 am

(May 9, 2015 05:23 AM)Ang?l Beats Wrote: [\[CITE\]](#) Actually having nginx as the frontend would help a huge amount, you could block incorrect host records with ease, while using barely any resources. You can do that with Apache too.

However I am not completely sure how, for nginx it's done automatically for me with virtual hosts.

I made all invalid virtual hosts go to the default nginx page, someone attacked it so i made it return 0 bytes (444) and boom issue fixed.

```
Code server {  
    listen 80 default_server;  
    return 444;  
  
}
```

apache will have issue handling this much traffic i think

Angel Beats?? - May 9, 2015, 7:54 am

(May 9, 2015 07:21 AM)An0ny Wrote: [\[CITE\]](#) You can do that with Apache too.

However I am not completely sure how, for nginx it's done automatically for me with virtual hosts.

I made all invalid virtual hosts go to the default nginx page, someone attacked it so i made it return 0 bytes (444) and boom issue fixed.

```
Code server {  
    listen 80 default_server;  
    return 444;  
  
}
```

apache will have issue handling this much traffic i think
Apache doesnt support 444 thats what I was saying.

Repeat - May 9, 2015, 8:09 am

You're both stupid. He doesn't need your help nor did he ask for it.

'An0ny - May 9, 2015, 8:25 am

(May 9, 2015 08:09 AM)Repeat Wrote: [\[CITE\]](#) You're both stupid. He doesn't need your help nor did he ask for it.

Shut the fuck up, he made a discussion thread which means we're allowed to discuss it. Not just ass kiss and say good luck.

(May 7, 2015 11:02 AM)Omniscient Wrote: [\[CITE\]](#) Going to have to discuss this openly to members.

XPRMX - May 9, 2015, 8:31 am

if anything why not add load balancing servers i am not sure if you already have those in place or not. I am not really a fan of cloudflare because if you buy 1 product from them you need to buy a thousand more for that 1 product to work.

'An0ny - May 9, 2015, 8:31 am

(May 9, 2015 08:31 AM)XPRMX Wrote: [\[CITE\]](#) What about staminus? Ive heard about them being a good ddos protection service. if anything why not add load balancing servers? if you havnt already. cant get more shit protection than staminus, js

Fudster - May 9, 2015, 10:05 am

May I ask...Who is your Server ISP even? Like I have a OVH server, Been DDOSed plenty of times (probably small attacks compared to the attacks on here) But whenever there is a attack on my server OVH handles it.

Like so...

So basically I am asking if you host has any server level firewall setup, Not a software firewall but rather a hardware firewall. Wonder if it would help or not....CF + the firewall.

* Fudster waits for Omni to reply back calling him a skid.

JDCL - May 9, 2015, 10:07 am

(May 9, 2015 10:05 AM)Fudster™ Wrote: [\[CITE\]](#) May I ask...Who is your Server ISP even? Like I have a OVH server, Been DDOSed plenty of times (probably small attacks compared to the attacks on here) But whenever there is a attack on my server OVH handles it.

Like so...

[img]-snip-[/img]

you blanked out the ip in the text down there, but you didn't block the title. You should fix that.

Fudster - May 9, 2015, 10:19 am

(May 9, 2015 10:07 AM)Joclings Wrote: [\[CITE\]](#) you blanked out the ip in the text down there, but you didn't block the title. You should fix that.

Yeah. Thanks :? Fixed.

hey0 m9 rekt - May 9, 2015, 11:07 am

Good to know you're doing everything you can, Omni <3

Repeat - May 9, 2015, 11:12 am

(May 9, 2015 08:25 AM)An0ny Wrote: [\[CITE\]](#) Shut the fuck up, he made a discussion thread which means we're allowed to discuss it. Not just ass kiss and say good luck.

Have your jimmies been rustled to your liking sir?

'An0ny - May 9, 2015, 12:01 pm

(May 9, 2015 10:05 AM)Fudster™ Wrote: [\[CITE\]](#) May I ask...Who is your Server ISP even? Like I have a OVH server, Been DDOSed plenty of times (probably small attacks compared to the attacks on here) But whenever there is a attack on my server OVH handles it.

Like so...

So basically I am asking if you host has any server level firewall setup, Not a software firewall but rather a hardware firewall. Wonder if it would help or not....CF + the firewall.

* Fudster™ waits for Omni to reply back calling him a skid.
sir, there is a difference between layer-4 and layer-7

from what i know, hes using OVH :)

the only layer-7 protected hosting that actually works must be CNServers.

Angel Beats?? - May 9, 2015, 12:07 pm

(May 9, 2015 12:01 PM)An0ny Wrote: [CITE](#) sir, there is a difference between layer-4 and layer-7

from what i know, hes using OVH :)

the only layer-7 protected hosting that actually works must be CNServers.

Hes using limestonenetworks. Layer 4 isnt the problem here he just needs to get a decent firewall for layer 7 which omni has done.

Omniscient - May 9, 2015, 12:13 pm

Sadly I'm already seeing problems with Sucuri. Their API is crap. Their support is slow.

Quote:I assume you're not a litespeed fan.

No, I'm not. Under another environment I might use it but pretty sure I need Apache. Nginx is by far the easiest to manage for an http reverse-proxy.

Quote:Actually having nginx as the frontend would help a huge amount, you could block incorrect host records with ease, while using barely any resources.

I should be able to do a lot of effective blocking at the Nginx level with minimal resources.

Quote:You can do that with Apache too.

Not true. Each Apache thread requires a ton more resources. Resources that choke the server with large attacks.

Quote:He doesn't need your help nor did he ask for it.

Pretty much. I'm not puzzled by what I need to do. I just need to do it. Find the time. Tear stuff apart. HF will likely experience some downtime. I already run Nginx on one server but likely I would go forward with my plan to do a complete backend change. That's a massive undertaking. We might even get rid of the CDN I use.

Quote:if anything why not add load balancing servers

With Nginx in front that's possible to do. But in-truth we don't need a load balancer.

Quote:cant get more shit protection than staminus

Briefly used them. They suck. They only care if you pay them \$10k a month. Ridiculous.

Quote:May I ask...Who is your Server ISP even?

We're on LSN but it doesn't matter about which ISP it is. The attacks that are bypassing Cloudflare would probably get past the OVH protection scheme because it's Layer7.

Quote:Hes using limestonenetworks. Layer 4 isnt the problem here he just needs to get a decent firewall for layer 7 which omni has done.

Pretty much. And Cloudflare was doing great against Layer 7 attacks with IMUA mode but failed because of the CNAME bypass. That's the crux of the current problem.

Thanks to everyone for their input but unless something changes or there is new information for me to report to members I'm going to close this.

Thanks.