Subject: More morons utilizing the "Relay" to spam attack
Posted by Javaxcx on Mon, 03 Mar 2003 03:39:44 GMT
View Forum Message <> Reply to Message

http://www.n00bstories.com/image.view.php?id=1950793322&gallery=575

This was a simotanious attack on myself, Taskbot1, and Taskbot7 for approximately 15 minutes a piece. I ended up leaving after the game ended, in which the spamming continued until I left the game.

If anyone has any information, please make an input, thanks.

Subject: More morons utilizing the "Relay" to spam attack
Posted by Deathgod on Mon, 03 Mar 2003 03:42:56 GMT
View Forum Message <> Reply to Message

ALERT YOU HAVE BEEN ATTACKED BY FUCKTARD
FUCKTARD CASTS SPAM BOMB
CRITICAL HIT!!!!!!!!!!!!!!11111
FUCKTARD DEALS YOU 21214646872 DAMAGE
DEATH IS YOU
END OF GAME

Subject: More morons utilizing the "Relay" to spam attack
Posted by ----- on Mon, 03 Mar 2003 03:44:45 GMT
View Forum Message <> Reply to Message

Fucktards beware

Subject: Sniff the spammers, then post their WOL names.
Posted by Blazer on Mon, 03 Mar 2003 03:49:24 GMT
View Forum Message <> Reply to Message

While the Renegade game/client itself does not reveal who sent the page, if you run a sniffer it will. Heres the way it works. when you type "/invite Blazer", it just sends me a normal page with the text "<WWINVITE>". And the Renegade game/client will say "Javaxcx invited you to join him blah blah blah". If you reject his invitation and click "Decline" instead of "join", it sends them a normal page, with "<WWDECLINE>". This makes renegade say "Yo!" and "Your invitation was declined".

Now...the spammers log into relay and just cut and paste or using an mirc script to just flood you with <WWDECLINE> pages.

Here's the good part. As I said, while the renegade game/client itself does not show who these

pages are from, a sniffer will. Remember, you are getting a NORMAL page, just as if you typed /page blazer0x <WWDECLINE>. So if you run a sniffer, you WILL see a page from the spammer, including their WOL username.

I suggest you install Ethereal http://www.ethereal.com/distribution/win32/ethereal-setup-0.9.9.exe

Play with it a bit, learn how to start up a capture quickly. Then the next time you are hit with one of these spam attacks, just alt-tab out of renegade, fire up ethereal and now you will have a log of their username.

I'm not going to give a sniffing-101 in how to use Ethereal, but I can tell you the most useful way to view the packet log is to find one definite packet, and click on it and select "view tcp stream". Ethereal will then open up a window and show you all the packets in easy to read plaintext format.

Subject: More morons utilizing the "Relay" to spam attack
Posted by Javaxcx on Mon, 03 Mar 2003 03:54:13 GMT
View Forum Message <> Reply to Message

Thanks Blazer, hopefully I can find out who this twerp is.

Subject: Oo
Posted by ----- on Mon, 03 Mar 2003 03:54:58 GMT
View Forum Message <> Reply to Message

Hey blazer. on another topic do you know why I was banned from RadiantX?

Subject: Re: Oo
Posted by Blazer on Mon, 03 Mar 2003 04:06:16 GMT
View Forum Message <> Reply to Message

Taskbot1Hey blazer. on another topic do you know why I was banned from RadiantX?

No clue...I hadn't heard

Subject: More morons utilizing the "Relay" to spam attack
Posted by ----- on Mon, 03 Mar 2003 04:10:08 GMT
View Forum Message <> Reply to Message

Didn't you notice the peace and quiet?
The lack of Bigtext "STFU N00B"?
The fact that there were no fights?

Are you sure you didn't notice?

Subject: More morons utilizing the "Relay" to spam attack
Posted by [sg]the0ne on Mon, 03 Mar 2003 04:29:11 GMT

Back in the day (before the internet was 'cool') these *types* of attacks were no big deal - now there are, ppl take them seriously. Basicly you could equate this to a denial of service attack -- I`m sure there ISP would be most interested and would take it seriously as long as its presented in the proper manner.

There is a way to stop this, its called Hey you fucking n00b you dont have internet access anymore ! Perhaps they'll think twice after they have to sign up for a new ISP (they better fucking hope they have ANOTHER broadband provider in their area   )

Subject: More morons utilizing the "Relay" to spam attack
Posted by DaveGMM on Mon, 03 Mar 2003 07:27:35 GMT

[sgthe0ne]Back in the day (before the internet was 'cool') these *types* of attacks were no big deal - now there are, ppl take them seriously. Basicly you could equate this to a denial of service attack -- I`m sure there ISP would be most interested and would take it seriously as long as its presented in the proper manner.

There is a way to stop this, its called Hey you fucking n00b you dont have internet access anymore ! Perhaps they'll think twice after they have to sign up for a new ISP (they better fucking hope they have ANOTHER broadband provider in their area   )

Its seems like a DoS of Renegade.... hmm.

Have you pissed anyone... wait, of course you have, your Java

Maybe its a random attack, though I doubt it.

Subject: More morons utilizing the "Relay" to spam attack
Posted by Sk8rRIMuk on Mon, 03 Mar 2003 08:59:01 GMT

Ethreal is ace I used it before and caught the person who was my best m8 and did it back to him don't take these things to serious theres gonna be a motive behind this and you will find out if/when this next happens.

-Sk8rRIMuk

Subject: More morons utilizing the "Relay" to spam attack
Posted by Majiin Vegeta on Mon, 03 Mar 2003 09:31:58 GMT
View Forum Message <> Reply to Message

cant you just type /r F**K OFF

then it wil page them back...sayin there name also?

Subject: More morons utilizing the "Relay" to spam attack
Posted by Sk8rRIMuk on Mon, 03 Mar 2003 09:38:50 GMT
View Forum Message <> Reply to Message

Majiin Vegetacant you just type /r F**K OFF

then it wil page them back...sayin there name also?

lol never though of that   .

-Sk8rRIMuk

Subject: More morons utilizing the "Relay" to spam attack
Posted by Javaxcx on Thu, 06 Mar 2003 00:57:42 GMT
View Forum Message <> Reply to Message

I have an update:

Taskbot7 and I were again in a private sniper server. Set to 5 players, and only the 2 of us residing. Anyway, 2 more people join up, and we continue to play. Anyway, someone called "lil2tight" ended up joining. He decided it would be nice of him to go off and try and nuke some buildings, so I stopped him, momentarily after, he says "kick all" in the all chat, and I proceed to disconnect, along with everyone else, including him. Taskbot7 did not, because he was the host.

What happened afterward, was that I was unable to rejoin the server because of a failing port neogaition. I assume the relay was used to change the port used by Taskbot7, and cut the rest of us off.

name: lil2tight

Any information, please bring it to my attention.

Subject: Re: Sniff the spammers, then post their WOL names.
Posted by Griever92 on Thu, 06 Mar 2003 01:01:47 GMT
View Forum Message <> Reply to Message

BlazerWhile the Renegade game/client itself does not reveal who sent the page, if you run a sniffer it will. Heres the way it works. when you type "/invite Blazer", it just sends me a normal page with the text "<WWINVITE>". And the Renegade game/client will say "Javaxcx invited you to join him blah blah blah". If you reject his invitation and click "Decline" instead of "join", it sends them a normal page, with "<WWDECLINE>". This makes renegade say "Yo!" and "Your invitation was declined".

Now...the spammers log into relay and just cut and paste or using an mirc script to just flood you with <WWDECLINE> pages.

Here's the good part. As I said, while the renegade game/client itself does not show who these pages are from, a sniffer will. Remember, you are getting a NORMAL page, just as if you typed /page blazer0x <WWDECLINE>. So if you run a sniffer, you WILL see a page from the spammer, including their WOL username.

I suggest you install Ethereal http://www.ethereal.com/distribution/win32/ethereal-setup-0.9.9.exe

Play with it a bit, learn how to start up a capture quickly. Then the next time you are hit with one of these spam attacks, just alt-tab out of renegade, fire up ethereal and now you will have a log of their username.

I'm not going to give a sniffing-101 in how to use Ethereal, but I can tell you the most useful way to view the packet log is to find one definite packet, and click on it and select "view tcp stream". Ethereal will then open up a window and show you all the packets in easy to read plaintext format.

Hmm, i would love to figure out who these a$$holes are that keep doing this to me. now i can

---

Subject: More morons utilizing the "Relay" to spam attack
Posted by Blazer on Thu, 06 Mar 2003 02:31:22 GMT
View Forum Message <> Reply to Message

Javaxcxhe says "kick all" in the all chat, and I proceed to disconnect, along with everyone else, including him. Taskbot7 did not, because he was the host.

What happened afterward, was that I was unable to rejoin the server because of a failing port neogaition. I assume the relay was used to change the port used by Taskbot7, and cut the rest of us off.

OMG he knows the secret "kick all" command! Just kidding. The relay can no longer be used to do things like changing the port or server name or playerlimit of servers. WOL is basically a stripped down modified ircd, and they made the channels +t to stop this (the server info is stored in the channel topic).

Are you sure he said "kick all" and not "fuck all" or something like that? Taskbot should still have the renlog.txt on his hard drive...maybe it should be reviewed to see exactly what happened.

Subject: More morons utilizing the "Relay" to spam attack
Posted by Javaxcx on Thu, 06 Mar 2003 20:41:29 GMT
View Forum Message <> Reply to Message

Hmm... Taskbot7 says that he does not have the renlog.txt on his HDD. I highly doubt that this person would say "fuck all", and all of us would disconnect.

I would like to also point out, that I rejoined his server again after he restart it, and within minutes, everyone in there disconnected again. I don't know of any text sent, because I must've disconnected before any text appeared. I'm sorry, I don't know.

Assuming it was a command "kick all", how could it be used to disconnect the entire server, and change the port?

Subject: More morons utilizing the "Relay" to spam attack
Posted by Blazer on Thu, 06 Mar 2003 22:31:32 GMT
View Forum Message <> Reply to Message

JavaxcxAssuming it was a command "kick all", how could it be used to disconnect the entire server, and change the port?

There is no way for a remote player to do this. Who knows though it could be a variation on the exploit I found that caused the 1.037 patch.

Subject: More morons utilizing the "Relay" to spam attack
Posted by Griever92 on Fri, 07 Mar 2003 02:53:01 GMT
View Forum Message <> Reply to Message

lol, found the bastard, paid his comp a little visit......