

Forum:[Hack Forums](#)

Thread: [Remove these infected ads!](#)

Ace Boogie - December 28, 2011, 8:34 am

Story:

Two days ago, two of my computers were infected by a rogue Anti-virus. Today, a Java drive-by executed on my computer. However, Kaspersky was able to quarantine the Trojan and I terminated Java as soon as I could which may have prevented the virus from running on my computer. If you are an Ub3r or L33t, you shouldn't have to worry about this, however, if you do log out and log in every time (like me), then you should worry about it.

This is a warning to everyone, use an ad blocker to prevent your self from getting infected. I guarantee that at least 100 members have been infected. This is not a joke, many people have reported this but this is the 3rd time that I am being infected due to the advertisements. Well, to be honest, I don't know if it is the advertisements but it is the most obvious source to me.

??s?? - December 28, 2011, 8:37 am

Damn, is this serious? Imao. It could be possible, but I would find it hard to believe Omni would do something like that. But how does Omni even get ads, I thought google doesn't allow hacking/malicious discussions on forums they put there ads on.

Ace Boogie - December 28, 2011, 8:38 am

It's not Google Ads that Omniscient is using.

TreeHugger - December 28, 2011, 8:39 am

Don't know what your talking about but, umm that sucks.

??s?? - December 28, 2011, 8:39 am

Oh, then what is he using? Is he just adding his own code into the index, and just doing personal deals with people to put there business banner up, or does he just use an other company?

Ace Boogie - December 28, 2011, 8:40 am

No, I am not going to get repfucked for being infected 3 times from ads at HackForums. It's not even a reason. I am just warning everyone that the ads have been infecting people. Many people have reported this, check my other thread.

Analyst - December 28, 2011, 8:42 am

It started small. But, members have caught my attention with this.

I think this is worth the investigation. So, everyone can feel safe and secure about they're accounts.

Ali?s - December 28, 2011, 8:44 am

(Dec 28, 2011 09:40 AM)Pansophical Wrote: [\[CITE\]](#) No, I am not going to get repfucked for being infected 3 times from ads at HackForums. It's not even a reason. I am just warning everyone that the ads have been infecting people. Many people have reported this, check my other thread.

See if another member posted this he would have been shunned out. But seeing as you're beyond a Vet. HF user your word has major chances to stand it's ground.

I'm uber as well so I do not see ads but if you're pointing this out then it must be true, no sarcasm intended.

Radke - December 28, 2011, 8:48 am

This sounds pretty bad. ./ Hopefully omni will jump on this and sort it out for us, I'm sure it wasn't intentional and he always does what's best for the community. those ads should be gone soon.

Scooter - December 28, 2011, 8:51 am

(Dec 28, 2011 09:39 AM)Virux™ Wrote: [\[CITE\]](#) Oh, then what is he using? Is he just adding his own code into the index, and just doing personal deals with people to put there business banner up, or does he just use an other company?

I believe he uses [BaronsMedia](#).

Source: <https://hackforums.net/misc.php?action=help&hid=25>

From what I know, he can't use Google Ads because of the "Hack" in Hackforums.

Approach - December 28, 2011, 8:54 am

It's partly Google Adsense and also some other ads not from adsense.

How come you're seeing ads even though you're an ub3r member?

LethalMG - December 28, 2011, 8:56 am

Nah you just downloaded shit and now ads are everywhere on your computer but it's the site's problem, we don't see any ads!!

Ignite. - December 28, 2011, 8:59 am

(Dec 28, 2011 09:54 AM)JackDeRips Wrote: [\[CITE\]](#) It's partly Google Adsense and also some other ads not from adsense.

How come you're seeing ads even though you're an ub3r member?

Probably when hes not logged in to his account, you can see the Ads.

Tzesi - December 28, 2011, 8:59 am

(Dec 28, 2011 09:56 AM)LethalMG Wrote: [\[CITE\]](#) Nah you just downloaded shit and now ads are everywhere on your computer but it's the site's problem, we don't see any ads!!

What LethalMG said.

probably some malicious software..

Ace Boogie - December 28, 2011, 9:02 am

I log on and log off everyday, which is why I see the ads. No, my computer is not infected with any other malicious software as I hardly download anything from any where.

TWO of my computers were infected just from visiting HackForums so you CANNOT say that it is something else.

Nostre - December 28, 2011, 9:03 am

I don't think this suggestion would get accepted. But I've posted a thread regarding this issue.

<https://hackforums.net/showthread.php?tid=2056947>

iBlowFish - December 28, 2011, 9:05 am

Last night I got the Windows 7 security center rouge AV. Needless to say I was pretty fucking pissed.

Ace Boogie - December 28, 2011, 9:07 am

(Dec 28, 2011 09:56 AM)LethalMG Wrote: [\[CITE\]](#) Nah you just downloaded shit and now ads are everywhere on your computer but it's the site's problem, we don't see any ads!!

Do not attempt to accuse me of infecting my self by downloading and executing "shit" without knowing the situation. I only see advertisements when I am logged off, and I am pretty sure everyone see's the advertisements when they are logged off. It's not my fault that you do not log off.

Han. - December 28, 2011, 9:08 am

I have used AdBlocker Plus since the dawn of time and I am amazed that people still complain about ads. It's as if they haven't heard of plugins.

However, I do agree that Omniscient obviously wouldn't try to infect members, considering this is how he makes money and there would be no point in jeopardizing that over spreading.

Besides, I'm sure he acknowledges himself that HF has a lot of skiddies and that they do deserve it, it's just a shame that regualr members have to put up with their crap.

Someone stop me! ?

Ace Boogie - December 28, 2011, 9:10 am

(Dec 28, 2011 10:03 AM)Genuine Wrote: [\[CITE\]](#) I don't think this suggestion would get accepted. But I've posted a thread regarding this issue.

<https://hackforums.net/showthread.php?tid=2056947>

Well, if a lot of members are claiming that they've been infected from just visiting HackForums (and of course, there are lots of people who are claiming to have been infected from visiting HackForums), this suggestion should get approved or Omniscient should at least contact Barons Media regarding this issue.

As soon as this incident occurred, I installed AdBlocker Plus (Firefox add-on).

(Dec 28, 2011 10:08 AM)Heinz Wrote: [\[CITE\]](#) Besides, I'm sure he acknowledges himself that HF has a lot of skiddies and that they do deserve it, it's just a shame that regualr members have to put up with their crap.

Someone stop me! ?

Did you not think for a moment that some members who are L33t and Ub3r log off from HackForums?

Glassy - December 28, 2011, 9:53 am

They may have been an error in the past couple of days. At the moment, the ads seem fine and if you feel the need to block them, then please do so. Otherwise, these ads will not be removed as it can help Omni in many ways.

ProfitNow - December 28, 2011, 10:16 am

<https://hackforums.net/showthread.php?tid=1323998>

I had the same issue.

lunix - December 28, 2011, 10:39 am

sure is a great day to be using FreeBSD.

lanConnor - December 28, 2011, 10:39 am

This happened to me too. Fucked up my \$700 laptop. :(

zombiehacker - December 28, 2011, 10:41 am

Remove the infected adds, infected me and my friend who are users on hackforum, we lost our mcdonalds login info.

+Pirate - December 28, 2011, 10:43 am

I'm in the process of removing it right now :/

Anyone have any idea of the site name?

Andz6 - December 28, 2011, 10:43 am

I just got infected by these ads. I found out that it was a temporary file in C:\Users\me\AppData\Local and was qlx.exe. I am using kaspersky now to scan if any other parts were infected. I hope this helps.

Boing - December 28, 2011, 10:45 am

(Dec 28, 2011 11:39 AM)Marketplace Wrote: [\[CITE\]](#) This happened to me too. Fucked up my \$700 laptop. :(

Fucked up a 700\$ laptop? Damn, you must be really a noob with PC if you think that a malware can destroy PCs. Just clean it.

Do as this guy said:

(Dec 28, 2011 11:48 AM)linux Wrote: [\[CITE\]](#) you are all idiots, look in task manager for a suspicious process that shouldn't be there. secondly look in startup locations using regedit.

Also, you can't get infected without clicking Run on the Java driveby.

If it was an exploit pack, you need to update your browser/OS.

+Pirate - December 28, 2011, 10:45 am

It can be in any of these areas

Windows 7 and Windows Vista Files and Folders:

%AllUsersProfile%\U3F7PNVFNCSSJK2E86ABFBJ5H
%LocalAppData%\ppn.exe
%Temp%\U3F7PNVFNCSSJK2E86ABFBJ5H
%LocalAppData%\U3F7PNVFNCSSJK2E86ABFBJ5H
%AppData%\TEMPLATES\U3F7PNVFNCSSJK2E86ABFBJ5H

Windows XP Files and Folders:

%AllUsersProfile%\Application Data\u3f7pnvfncsjk2e86abfbj5h
%LocalAppData%\kdn.exe
%LocalAppData%\u3f7pnvfncsjk2e86abfbj5h
%Temp%\u3f7pnvfncsjk2e86abfbj5h
%UserProfile%\Templates\u3f7pnvfncsjk2e86abfbj5h

Bvsed - December 28, 2011, 10:46 am

I just reformatted my PC 2 days ago from having a rogue virus and I do sometimes log in and out from the site.

lunix - December 28, 2011, 10:48 am

you are all idiots, look in task manager for a suspicious process that shouldn't be there. secondly look in startup locations using regedit.

+Pirate - December 28, 2011, 10:51 am

(Dec 28, 2011 11:48 AM)lunix Wrote: [\[CITE\]](#) you are all idiots, look in task manager for a suspicious process that shouldn't be there. secondly look in startup locations using regedit.
When you close the process it comes back as a different name.

It does not let you use 90% of .exe's without manually finding them first, which is quite hard since Microsoft changes the names around.

Can't open computer in safe mode.

lunix - December 28, 2011, 10:53 am

(Dec 28, 2011 11:51 AM)+Pirate Wrote: [\[CITE\]](#) When you close the process it comes back as a different name.

It does not let you use 90% of .exe's without manually finding them first, which is quite hard since Microsoft changes the names around.

Can't open computer in safe mode.

hence why I said look in regedit. delete/lock the startup entries, then reboot. You should be able to delete the executable.

holy shit so much for "hackforums", people don't even understand the basic concepts of malware.
???

lanConnor - December 28, 2011, 10:53 am

When I say fucked up, I didn't mean it broke and I had to throw it out.

I removed everything, it was just a pain in the ass.

OsulMofo - December 28, 2011, 10:54 am

Guys, How to prevent getting infected:

Download Google Chrome/Firefox
Install Ad-Block

Solved.

Boing - December 28, 2011, 10:55 am

(Dec 28, 2011 11:53 AM)Marketplace Wrote: [\[CITE\]](#) When I say fucked up, I didn't mean it broke and I had to throw it out.

I removed everything, it was just a pain in the ass.

Then the price of the computer that you mentioned (700\$) is useless.
It doesn't have sense.

lunix - December 28, 2011, 10:56 am

(Dec 28, 2011 11:54 AM)?R??????? Wrote: [\[CITE\]](#) Guys, How to prevent getting infected:

Download Google Chrome/Firefox

Install Ad-Block

Solved.

google chrome is botnet... by downloading and installing google chrome (agreeing to the terms and conditions) you have infected yourself with googles botnet.

???

Osu|Mofo - December 28, 2011, 10:58 am

Google Chrome is Botnet.

Do you really thing when you install google chrome you're infected by google?
You seriously must be very stupid.

Ace Boogie - December 28, 2011, 11:01 am

(Dec 28, 2011 11:58 AM)?R??????? Wrote: [\[CITE\]](#) Google Chrome is Botnet.

Do you really thing when you install google chrome you're infected by google?
You seriously must be very stupid.
He is stupid. That's the most stupid thing I've heard all year.

+Pirate - December 28, 2011, 11:01 am

Is it just me or does some tabs open up with "CPV".*** when you're infected?

linux - December 28, 2011, 11:04 am

(Dec 28, 2011 12:01 PM)Pansophical Wrote: [\[CITE\]](#) He is stupid. That's the most stupid thing I've heard all year.

google chrome is a botnet, if you believe otherwise you must be very stupid. have you ever actually read the terms and conditions of google chrome lately?

<http://precursorblog.com/content/google-chrome-we-dont-need-your-permission>
<http://www.securitronlinux.com/uncategorized/google-chrome-botnet-fact-or-fiction/>
http://www.pcworld.com/article/168244/chrome_and_more_chrome_that_pesky_botnet.html

chrome downloads files and performs system modifications without your permission, it communicates with a remote control server, it even creates a hidden critical process that cannot be removed easily. sure seems like a botnet to me. ?

Ace Boogie - December 28, 2011, 11:19 am

(Dec 28, 2011 12:04 PM)linux Wrote: [\[CITE\]](#) google chrome is a botnet, if you believe otherwise you must be very stupid. have you ever actually read the terms and conditions of google chrome lately?

<http://precursorblog.com/content/google-chrome-we-dont-need-your-permission>
<http://www.securitronlinux.com/uncategorized/google-chrome-botnet-fact-or-fiction/>
http://www.pcworld.com/article/168244/chrome_and_more_chrome_that_pesky_botnet.html

chrome downloads files and performs system modifications without your permission, it communicates with a remote control server, it even creates a hidden critical process that cannot be removed easily. sure seems like a botnet to me. ?

Google's going to take over the world. It's called Googluminati (!). However, your point is certainly interesting.

Pinstriped - December 28, 2011, 11:22 am

(Dec 28, 2011 12:19 PM)Pansophical Wrote: [\[CITE\]](#) Google's going to take over the world. It's called Googluminati. However, your point is certainly interesting.Lol, I like how he just proved you wrong easily, now you're agreeing with him. c:

Ace Boogie - December 28, 2011, 11:26 am

(Dec 28, 2011 12:22 PM)Soulmate Wrote: [\[CITE\]](#) Lol, I like how he just proved you wrong easily, now you're agreeing with him. c:

I am not agreeing with him. I am just saying his point is quite interesting and Googleuminati is a joke I made up, which I think failed (after I reading the post back, I didn't find it funny ?).

Added (!) after Googluminati to show sarcasm.

Infinity? - December 28, 2011, 11:33 am

Yeh, I was infected by a rogue Anti-Virus three times by visiting HF when my login cookies were cleared. Seemed like a 0-day to me as I didn't click nor accept any Java applets. Had to do a system restore three times. I recommend everyone to install ADBlock Plus and NoScript.

linux - December 28, 2011, 11:41 am

Do you want to know the real secret to not getting infected while still maintaining a functional computer?

Spoiler ([Click to View](#))

Install Linux/BSD/Mac OS X

Andz6 - December 28, 2011, 1:25 pm

(Dec 28, 2011 12:41 PM)linux Wrote: [\[CITE\]](#) Do you want to know the real secret to not getting infected while still maintaining a functional computer?

Install Linux/BSD/Mac OS X

You can still get infected with a mac you tool, its just viruses are more reguarly created for windows operating systems as macintosh's have a lot less users. Mac os x is based on a unix kernel, which is very secure, but there are still security holes.

The Exploit - December 28, 2011, 1:27 pm

ad.yeildmanager is making this happen. Just thought I would let you guys know.

Guess Who Is Back - December 28, 2011, 1:27 pm

Let's wait and see what omni will say about this.

Crappie - December 28, 2011, 2:54 pm

I was infected too. Let just wait and see what happens

linux - December 28, 2011, 5:26 pm

(Dec 28, 2011 02:25 PM)Andz6 Wrote: [\[CITE\]](#) You can still get infected with a mac you tool, its just viruses are more reguarly created for windows operating systems as macintosh's have a lot less users. Mac os x is based on a unix kernel, which is very secure, but there are still security holes.
[img]http://cdn.hackforums.net/images/smilies/omg.gif[/img]

And when was the last time you seen an OS X virus in the wild?

Nmanpure Pkr - December 28, 2011, 5:39 pm

Please refer to this post.

(Dec 28, 2011 03:34 AM)Omniscient Wrote: [\[CITE\]](#) For those making claims they are being exploited while visiting here. You need to check your AV logs and contact me with the info. If indeed a java driveby is happening from the ad network I need to know, track it down, and report it.

Omni has no control of the ads that are displayed here. Do what he says so he can report those ads.

Andz6 - December 29, 2011, 5:28 am

(Dec 28, 2011 06:26 PM)lunix Wrote: [\[CITE\]](#)

[img]http://cdn.hackforums.net/images/smilies/omg.gif[/img]

And when was the last time you seen an OS X virus in the wild?

"Apple has better commercials, but the Mac is no harder to break into than a Windows PC," said Gartner security analyst John Pescatore.

Don't think that your security on a mac is any better, with the amount of exploits that have been available on Apple's devices such as the iPhone, iPod and iPad. I know for a fact that there is a PDF exploit that is available for Mac on S.E.T

lunix - December 29, 2011, 6:56 am

(Dec 29, 2011 06:28 AM)Andz6 Wrote: [\[CITE\]](#) "Apple has better commercials, but the Mac is no harder to break into than a Windows PC," said Gartner security analyst John Pescatore.

Don't think that your security on a mac is any better, with the amount of exploits that have been available on Apple's devices such as the iPhone, iPod and iPad. I know for a fact that there is a PDF exploit that is available for Mac on S.E.T

Where did I say security is better? I was also talking about all Unix/Unix-Like systems as a whole. iPhone/iPad/iPod are not Mac OS X, then run iOS ???

The majority of all malware/exploits are for windows, people want to target windows alone because it holds the greatest market share for operating systems. It is very rare that someone will waste their time coding malware for Linux, BSD, Mac, Solaris and all those othes specific machines. ?

Julia Gillard - December 29, 2011, 7:11 am

It doesn't matter what operating system you use you'll still get infected important using a android with a anti virus and important probably still at risk but i doubt its the adds its probably users visiting the wrong site which often infects your pc often or just hijinx in my honest Opinion just be carefully what you click and where you go

jackisback - December 29, 2011, 7:15 am

(Dec 28, 2011 12:41 PM)lunix Wrote: [\[CITE\]](#) Do you want to know the real secret to not getting infected while still maintaining a functional computer?

Spoiler ([Click to View](#))

Install Linux/BSD/Mac OS X

You have to be one of the most uninformed users on this site. All operating systems get viruses.

linux - December 29, 2011, 7:23 am

(Dec 29, 2011 08:15 AM)jackisback Wrote: [\[CITE\]](#) You have to be one of the most uninformed users on this site. All operating systems get viruses.

You have to be one of the most uninformed users on this site. If you knew anything about Unix/Unix-Like systems you would understand that it is very rare that they will ever encounter a virus for their platform in the wild, people simply do not waste their time coding malware to target less than 0.05% of the operating system market.

If you understood how unix worked you would know that even if you do get infected very little damage can be done to the system.

jackisback - December 29, 2011, 7:46 am

(Dec 29, 2011 08:23 AM)linux Wrote: [\[CITE\]](#) You have to be one of the most uninformed users on this site. If you knew anything about Unix/Unix-Like systems you would understand that it is very rare that they will ever encounter a virus for their platform in the wild, people simply do not waste their time coding malware to target less than 0.05% of the operating system market.

If you understood how unix worked you would know that even if you do get infected very little damage can be done to the system.

The fact is that viruses for OS X do exist. Even though the amount of users affected is currently very small. It's important to note that the number of Mac users is increasing.

1nf4m0us - December 29, 2011, 12:31 pm

Now I remember... My avast detected something one/two weeks ago when I wasn't l33t..

decoded123 - December 29, 2011, 12:39 pm

Yes. There has been plenty of attacks that was detected by Norton here too!

Rhythm - December 29, 2011, 12:49 pm

Last I checked you couldn't become infected from viewing a web page?

Java Drive-Bys, (unless you have some primitive browser) require authentication before running.

jackisback - December 29, 2011, 1:59 pm

(Dec 29, 2011 01:49 PM)Rhythm Wrote: [\[CITE\]](#) Last I checked you couldn't become infected from viewing a web page?

Java Drive-Bys, (unless you have some primitive browser) require authentication before running. Not if a new exploit has been discovered.

Ace Boogie - December 29, 2011, 4:02 pm

(Dec 29, 2011 01:49 PM)Rhythm Wrote: [\[CITE\]](#) Last I checked you couldn't become infected from viewing a web page?

Java Drive-Bys, (unless you have some primitive browser) require authentication before running. Not always. Silent Drive-Bys do exist.

Boing - December 30, 2011, 2:23 am

(Dec 29, 2011 05:02 PM)Pansophical Wrote: [\[CITE\]](#) Not always. Silent Drive-Bys do exist. Silent Drive-bys are Exploit packs..

They have like nothing to do with Java's drive-by.

Ace Boogie - December 31, 2011, 9:48 am

(Dec 30, 2011 03:23 AM)RTFM. Wrote: [\[CITE\]](#) Silent Drive-bys are Exploit packs..

They have like nothing to do with Java's drive-by.

Considering a Java-Driveby executed on my computer and Kaspersky quarantined a file from temporary files and I did not have an option to run anything Java related, I believe that silent Java Drive-by's do exist, possibly a new exploit.

I use Firefox 9.0.1 (Latest Firefox).

Nitrox - December 31, 2011, 10:15 am

Well, I have seen similar things as well. My Antivirus keeps blocking the ads when I first open up HF. And I logout and login everytime, so I am confronted with the ads everytime. But when the site first loads before I login, I press the "Esc" key on my keyboard to prevent the ads from loading.

But, the ads are infected, and that's true. Omni should do something about this!

+Pirate - December 31, 2011, 10:17 am

Omni does not know what ad is the one that is specifically infecting people.

When he finds it, he will block and remove it.

Nitrox - December 31, 2011, 10:21 am

(Dec 31, 2011 11:17 AM)+Pirate Wrote: [\[CITE\]](#) Omni does not know what ad is the one that is specifically infecting people.

When he finds it, he will block and remove it.

All ads are blocked by my AV. I guess very few ones are clean. And I don't think Omni will be checking all the ads throughout the day to find which one or which ones are infected.

carlos_matos - December 31, 2011, 1:05 pm

Unless your a multi account, OP, there's no way you could've known.

Nitrox - December 31, 2011, 1:21 pm

(Dec 31, 2011 02:05 PM)Irise Wrote: [\[CITE\]](#) Unless your a multi account, OP, there's no way you could've known.

He could login to the same account from multiple computers? ?

Boing - December 31, 2011, 2:56 pm

(Dec 31, 2011 10:48 AM)Pansophical Wrote: [\[CITE\]](#) Considering a Java-Driveby executed on my computer and Kaspersky quarantined a file from temporary files and I did not have an option to run anything Java related, I believe that silent Java Drive-by's do exist, possibly a new exploit.

I use Firefox 9.0.1 (Latest Firefox).

If it is silent, it can ONLY be an exploit (pack).

Nothing to do with Java..

Video - December 31, 2011, 3:01 pm

Why no just get adblock for your browser.

jackisback - December 31, 2011, 4:19 pm

(Dec 31, 2011 04:01 PM)Video Wrote: [\[CITE\]](#) Why no just get adblock for your browser.

Because they shouldn't be infected in the first place.