Subject: Oh dear
Posted by jnz on Thu, 29 Oct 2009 07:57:46 GMT
View Forum Message <> Reply to Message

http://safebrowsing.clients.google.com/safebrowsing/diagnostic?site=http://www.r
enegadeforums.com/&client=googlechrome&hl=en-GB

Subject: Re: Oh dear
Posted by Goztow on Thu, 29 Oct 2009 07:59:45 GMT
View Forum Message <> Reply to Message

"Google didn't find anything malicious but will still list a site as suspicious, but most certainly will not tell you why!"

Subject: Re: Oh dear
Posted by danpaul88 on Thu, 29 Oct 2009 14:21:18 GMT
View Forum Message <> Reply to Message

Gah! Every time I try to open the forums or click on any links it gives me a big red warning page and I have to click Ignore every time to get to the page! This is so annoying!

I assume this is the work of some asshat who got banned or something trying to get some sort of revenge?

Subject: Re: Oh dear
Posted by Spoony on Thu, 29 Oct 2009 14:41:44 GMT
View Forum Message <> Reply to Message

i'm having the same sort of problems

Subject: Re: Oh dear
Posted by Renardin6 on Thu, 29 Oct 2009 15:28:22 GMT
View Forum Message <> Reply to Message

http://forum.avast.com/index.php?topic=47096.0

This is why.

Quote:Every 3.6 seconds a website is infected

Infected websites have been the single biggest threat over the past six months, and the threat vectors that have seen the most growth are Web 2.0 and social networking technologies,

---

according to the report, which was released Wednesday by security firm Sophos.

Approximately 23,500 infected webpages are discovered every day – that's a new one every 3.6 seconds, according to Sophos' recently released July security threat report. That infection rate is faster than in 2008, during which the first half of that year saw a newly infected website being identified every 4.5 seconds, Richard Wang, manager, Sophos Labs U.S. told SCMagazineUS.com on Tuesday.

http://www.scmagazineus.com/Every-36-seconds-a-website-is-infected/article/14041 4/

They list some solution there:

http://forum.avast.com/index.php?topic=49347.0

I am afraid all the websites hosted by Crimson are touched.

www.renguard.com has the same problem.

Subject: Re: Oh dear
Posted by reborn on Thu, 29 Oct 2009 15:32:28 GMT
View Forum Message <> Reply to Message

Renardin6 wrote on Thu, 29 October 2009 10:28[url]
I am afraid all the websites hosted by Crimson are touched.

www.renguard.com has the same problem.

Does that also include http://www.starvingcats.com ?

Subject: Re: Oh dear
Posted by Renardin6 on Thu, 29 Oct 2009 15:34:27 GMT
View Forum Message <> Reply to Message

nope, APB is fine.

Toggle Spoiler

File Attachments
1) virus.jpg, downloaded 945 times

Command and Conquer: Renegade Official Forums - Windows Internet Explorer

http://www.renegadeforums.com/index.php?t=post&th_id=35058&reply_to=408723&rid=1841&start=0

⭐ Favoris | 👍 🌐 Sites suggérés ▾ | 🌐 Galerie de composants ... ▾

⊞ ▾ | 🌐 Every 3.6 seconds a websit... | f Facebook | Christine Korza | ◯ Command and Conqu... ✕ | 🌐 Command and Conquer: ...

✉ Private Messaging

Post Form

Logged in user:	Renardin6 [logout]
Forum:	General Discussion
Title:	Re: Oh dear
Poll:	[CREATE POLL]
Message Icon:	⦿ No Icon

Smiley Shortcuts:
[list all smilies]

Formatting Tools:

B *I* U | ≣ ≣ ≣ | 🌐 🔒 📝 | ≟ ≔ 📑 {··} | Size ▾ | Color ▾ | Font ▾

Body:

Forum Options
HTML code is **OFF**
FUDcode is **ON**
Images are **ON**
Smilies are **ON**
Editing Time Limit: Unlimited

nope, APB is fine.

File Attachments:	**Allowed File Extensions:** (unrestricted) **Maximum File Size:** 1024Kb **Maximum Files Per Message:** 10
	[ ] Parcourir...	Upload File
Options:	☐ **Post Notification** Notify me when someone replies to this message. ☑ **Include Signature**

Nom d
Nom d
Type c
Version

Tra

A

Sta
☑

http:/

Subject: Re: Oh dear
Posted by Tupolev TU-95 Bear on Thu, 29 Oct 2009 15:34:29 GMT
View Forum Message <> Reply to Message

Renardin6 wrote on Thu, 29 October 2009 15:28
www.renguard.com has the same problem.

no problem with renguard

i think we are at war against the virus

Subject: Re: Oh dear
Posted by ErroR on Thu, 29 Oct 2009 16:28:13 GMT
View Forum Message <> Reply to Message

for firefix users, you can disable the 'warn me when I'm about to enter a infected site' thing and re enable it when finished browsing ren forums..

Subject: Re: Oh dear
Posted by Goztow on Thu, 29 Oct 2009 16:31:16 GMT
View Forum Message <> Reply to Message

My 1337 Nod32 doesn't report any trouble on this site. Nore did Symantec corporate at work...

Subject: Re: Oh dear
Posted by Tupolev TU-95 Bear on Thu, 29 Oct 2009 16:41:19 GMT
View Forum Message <> Reply to Message

same here

on my toher comp my GayVG dont detect nothin

Subject: Re: Oh dear
Posted by Goztow on Thu, 29 Oct 2009 17:00:38 GMT
View Forum Message <> Reply to Message

I think I found the problem and it seems to resort in the renguard.com website. As it's hosted on the same box, i suppose it copied itself over. I warned Crimson about it.

Subject: Re: Oh dear
Posted by ChewML on Thu, 29 Oct 2009 17:12:23 GMT

I got a warning for a trojan last night, wasn't sure where the hell it would have came from... but I guess it was prolly from here... oh well Norton FTW!

Toggle Spoiler

Also Renadrin lern2spoiler.

File Attachments
1) trojan.jpg, downloaded 937 times

http://www.renegadeforums.com/index.php?t=msg&th=35058&start=0&rid=23934

Google

Command and Conquer: Rene

PROFILE

Re: Oh dear [message #408767]

goliath35
Messages: 649
Registered: April 2009
Location: Birmingham England
PHASE TRANSPORT

same here

on my toher comp my GayVG dont detect

some soldier said during

WHAT THE HELL IS THAT

profile

Rate Topic ▼

Goto Forum:
General Discussion

Total time taken to generate the page: 0.02371 se

🌐 Norton Internet Security

Security History Advanced Details

Alert Summary

Severity	Activity	Date & Time
● High	Auto-Protect has detected Trojan.Pidief.F	10/29/2009 12:25

Advanced Details

Risk Category	Virus
Definitions Version	2009.10.28.038
Severity	High ● ● ●
Component	Auto-Protect
Status	Blocked
File Name	c:\users_____\appdata\local\microsoft\windows\temporary internet files\low\content.ie5\ufvwsbwd\dummyifon[1].pdf

.:: Contact :: Home ::.

Powered by: FUDforum 2.7.7RC2.
Copyright ©2001-2007 FUD Forum Bulletin Board Soft

Norton Internet Security

Command and Con...   🌐 Norton Internet Sec...   🌐 Norton Internet Sec...

Subject: Re: Oh dear
Posted by Sladewill on Thu, 29 Oct 2009 19:34:54 GMT

whens it gona be sorted?

Subject: Re: Oh dear
Posted by Tupolev TU-95 Bear on Thu, 29 Oct 2009 20:52:59 GMT

Sladewill wrote on Thu, 29 October 2009 19:34whens it gona be sorted?
imo it might take a while

Subject: Re: Oh dear
Posted by halo2pac on Thu, 29 Oct 2009 21:52:02 GMT

Renardin6 wrote on Thu, 29 October 2009 09:28I am afraid all the websites hosted by Crimson are touched.

does she have any children hosted as well?
If I was to be hosted would I be touched?
If I view this site from my iTouch would it be touched and become a hasbeenTouched?

Hahaha just kidding crimson. Love ya

btw site works fine on my itouch.

Subject: Re: Oh dear
Posted by nope.avi on Thu, 29 Oct 2009 22:12:42 GMT

every time I try to view the site on my phone I get redirected to Google

---

Subject: Re: Oh dear
Posted by Crimson on Thu, 29 Oct 2009 22:13:28 GMT

I have cleaned off the virus and Blazer is trying to find the point of entry. It might be a bit before Google reviews the site and lifts the warning, but I have submitted for review.

Subject: Re: Oh dear

Posted by _SSnipe_ on Thu, 29 Oct 2009 22:16:48 GMT
View Forum Message <> Reply to Message

Crimson wrote on Thu, 29 October 2009 15:13I have cleaned off the virus and Blazer is trying to find the point of entry. It might be a bit before Google reviews the site and lifts the warning, but I have submitted for review.
"Blazer is trying to find the point of entry"

By that you mean what?, sorry don't mean to bother I am just wondering is all.

gj to u both

Subject: Re: Oh dear
Posted by Crimson on Thu, 29 Oct 2009 22:17:54 GMT
View Forum Message <> Reply to Message

Uhh... the way that some random russian tard was able to add that iframe crap to the bottom of dozens of random files on the server. At least it was an excuse to do some more housecleaning of sites I don't host anymore.

Subject: Re: Oh dear
Posted by R315r4z0r on Thu, 29 Oct 2009 22:31:07 GMT
View Forum Message <> Reply to Message

Damn, google. Tellin' me what I can and can't view on the internet!

Subject: Re: Oh dear
Posted by Spoony on Thu, 29 Oct 2009 22:41:34 GMT
View Forum Message <> Reply to Message

i've gotten that antivirus system pro shit now... can anyone help with that?

Subject: Re: Oh dear
Posted by Omar007 on Thu, 29 Oct 2009 22:49:44 GMT
View Forum Message <> Reply to Message

I just use IE () for the moment xD

Crimson WroteI have cleaned off the virus and Blazer is trying to find the point of entry. It might be a bit before Google reviews the site and lifts the warning, but I have submitted for review.

I got ESET Smart Security (Nod32 technologie) which detected no virusses and Spyware Doctor didnt either

Hope it gets fixed soon though

Subject: Re: Oh dear
Posted by Tupolev TU-95 Bear on Thu, 29 Oct 2009 22:51:47 GMT
View Forum Message <> Reply to Message

so does this mean we win the war against the malicious attack?

Subject: Re: Oh dear
Posted by slosha on Thu, 29 Oct 2009 23:30:01 GMT
View Forum Message <> Reply to Message

It's all better now.

Subject: Re: Oh dear
Posted by Tupolev TU-95 Bear on Thu, 29 Oct 2009 23:33:17 GMT
View Forum Message <> Reply to Message

what do u mean all better?

it still says that thing under the site

Subject: Re: Oh dear
Posted by Goztow on Fri, 30 Oct 2009 07:30:46 GMT
View Forum Message <> Reply to Message

For FF: tools -> options -> security and disable "block infected sites" or whatever it's called.
However, this will remove all blocking of sites that google considers infected.

Subject: Re: Oh dear
Posted by Omar007 on Fri, 30 Oct 2009 09:54:47 GMT
View Forum Message <> Reply to Message

Well its gone now ^^

Subject: Re: Oh dear
Posted by danpaul88 on Fri, 30 Oct 2009 10:25:01 GMT
View Forum Message <> Reply to Message

Goztow wrote on Fri, 30 October 2009 07:30For FF: tools -> options -> security and disable "block infected sites" or whatever it's called. However, this will remove all blocking of sites that google considers infected.

You can turn it back on now Gozy, the website seems to have been removed from the list of attack sites as it's no longer warning me about it.

Subject: Re: Oh dear
Posted by Sladewill on Fri, 30 Oct 2009 11:10:07 GMT
View Forum Message <> Reply to Message

clear

Subject: Re: Oh dear
Posted by Dover on Fri, 30 Oct 2009 19:29:16 GMT
View Forum Message <> Reply to Message

Crimson wrote on Thu, 29 October 2009 15:17some random russian tard

Scrin?

Subject: Re: Oh dear
Posted by EvilWhiteDragon on Fri, 30 Oct 2009 21:37:59 GMT
View Forum Message <> Reply to Message

Dover wrote on Fri, 30 October 2009 20:29Crimson wrote on Thu, 29 October 2009 15:17some random russian tard

Scrin?
Let's ban him anyway, just to be sure it's not him...

Subject: Re: Oh dear
Posted by GEORGE ZIMMER on Fri, 30 Oct 2009 21:38:37 GMT
View Forum Message <> Reply to Message

EvilWhiteDragon wrote on Fri, 30 October 2009 15:37Dover wrote on Fri, 30 October 2009 20:29Crimson wrote on Thu, 29 October 2009 15:17some random russian tard

Scrin?
Let's ban him anyway, just to be sure it's not him...
Pretty sure no one of importance would object to this.

Subject: Re: Oh dear
Posted by renalpha on Fri, 30 Oct 2009 22:58:22 GMT
View Forum Message <> Reply to Message

what happend was that one of the persons who acces the ftp got infected with a virus.

His ftp information was keylogged which sended this information to a server, over there it uploaded iframe scripts.

Its not a forum leak, its just a pc which is infected.

KEEP YOUR PC CLEAN

Subject: Re: Oh dear
Posted by StealthEye on Fri, 30 Oct 2009 23:23:54 GMT
View Forum Message <> Reply to Message

Is that a guess or is that what actually happened? Because I'd be more surprised if that's the case than if it's some script bug exploit somewhere. Did you find anything about what caused it yet, Crimson/Blazer?

Subject: Re: Oh dear
Posted by Crimson on Sat, 31 Oct 2009 00:46:47 GMT
View Forum Message <> Reply to Message

LOL like I use an insecure method like FTP to connect to the server... SCP FTW.

Subject: Re: Oh dear
Posted by renalpha on Sat, 31 Oct 2009 12:19:16 GMT
View Forum Message <> Reply to Message

Yes, you can do that using the SSH protocol to go on with SFTP.
However, if someone else uses the ftp protocol, than that is what happend. Cannot see any other reason, occurs sometimes on websites of my customers.