

Re: 26 min Nasa film of Gemini 4 eva VIRUS ALERT

Source: <http://sci.tech-archive.net/Archive/sci.space.history/2006-12/msg00749.html>

- *From:* "Jonathan" <beals@xxxxxxxxxxxxxx>
 - *Date:* Thu, 14 Dec 2006 23:24:21 -0500
-

"Vincent D. DeSimone" <desimone8@xxxxxxxxxxxxxx> wrote in message
[news: oSdnRJf-tLgIRzYnZ2dnUVZ_q6vnZ2d@xxxxxxxxxxxxxx](news:oSdnRJf-tLgIRzYnZ2dnUVZ_q6vnZ2d@xxxxxxxxxxxxxx)

The moment I entered that website, my
anti-virus package informed me

that I

had acquired the bloodhound.exploit.104
virus. I was able to stop it

dead

and it was probably from one of the ads on
the page, but still...

Google serving up a virus? Kind of hard to believe. Did you
inform
Google?

Some Anti-Virus software claim to 'see' a virus, while there is none.
McAfee and Norton also have that habit...

I use Kaspersky and no virussus in my PC...

André

I'm using Norton. Checking the log, I find that the infected file was
placed in my Temporary Internet Files folder. And no, I haven't contacted
Google.

Source: C:\Documents and Settings\...\Temporary Internet
Files\Content.IE5\31WGBV8U\3162764041-videos[2].js
Click for more information about this risk : Bloodhound.Exploit.104

Re: 26 min Nasa film of Gemini 4 eva VIRUS ALERT

Action taken: Automatically deleted

Source: Manual Scanner

Risk category: Virus

Click for more information about this risk : Bloodhound.Exploit.104

Action taken: Deleted

Description: Affected areas:

1 Files:

3162764041–videojs[1].js within C:\Documents and Settings\...\Local Settings\Temporary Internet

Files\Content.IE5\31WGBV8U\3162764041–videojs[1].js – Deleted

December 12, 2006

Bloodhound.Exploit.104

This evening I received several virus alerts from a computer indicating a Bloodhound.Exploit.104 infection in a file in the temporary internet files folder. The filename ended in "videojs.js".

Bloodhound is Symantec Antivirus's attempt at a heuristic detection. The writeup at the Symantec website indicates that Bloodhound.Exploit.104 is a heuristic detection for Microsoft Internet Explorer DHTML Node Normalize Vulnerability (as described in Microsoft Security Bulletin MS06–072).

A quick Google revealed that videojs.js is a javascript used on the website video.google.com. A visit to that website, and soon I too had Symantec detecting the bloodhound.exploit.104. (and the video would not load) I am using the 12/12 rev 19 virus definitions.

I looked at www.symantec.com

<http://www.infosecblog.org/>

Microsoft Security Bulletin MS06–072).

<http://www.microsoft.com/technet/security/Bulletin/MS06–072.msp>

Re: 26 min Nasa film of Gemini 4 eva VIRUS ALERT