

Re: Encrypted javascript on probable virus page

Source: <http://newsgroups.derkeiler.com/Archive/Alt/alt.comp.anti-virus/2007-09/msg00060.html>

- *From:* "Ant" <not@xxxxxxxxxx>
 - *Date:* Wed, 5 Sep 2007 22:46:13 +0100
-

"Virus Guy" wrote:

Not sure what this is all about. I only get this behavior with IE6.
It doesn't do this (display message) with firefox or an old version of
Netscape.

I believe ActiveX is only supported by MSIE.

This is probably attempting to exploit a known IE (IE6?) bug – anyone
know which one?

Several; most or all of which should be now patched. You're taking a
big risk following these kind of links with IE, or even any other
standard browser. You should use wget or some other utility to fetch
the raw unrendered page.

Are there any on-line javascript de-obfuscators?

The unscrambling routine is in the script so you can do it yourself.

[fncarp.com]

Well – you get the idea. A different IP every time you look it up

It's a fast-flux botnet. The domain has a TTL (time to live) of zero
seconds, the name servers somewhat longer of two days. All the IP
addresses (hosts and name servers) point to compromised machines on
various networks.