

RE: WAS: Bittorrent – utorrent NOW: Certificate Talk

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ids/2007-03/msg00056.html>

- *From:* "Erick Jensen" <ejensen@xxxxxxxxxxx>
 - *Date:* Mon, 19 Mar 2007 17:10:57 -0500
-

Another point is the big guys provide insurance. If your encryption is cracked they cover damages up to whatever amount. That's the only plus (I see) to using one of the larger certificate companies.

-----Original Message-----

From: listbounce@xxxxxxxxxxxxxxxxxxxx [<mailto:listbounce@xxxxxxxxxxxxxxxxxxxx>]
On Behalf Of Tremaine Lea
Sent: Sunday, March 18, 2007 6:41 PM
To: Randal T.Rioux
Cc: focus-ids@xxxxxxxxxxxxxxxxxxxx
Subject: Re: WAS: Bittorrent – utorrent NOW: Certificate Talk

On 18-Mar-07, at 12:45 AM, Randal T. Rioux wrote:

Tremaine Lea wrote:

Having said that, the BCSG *will* refuse self-signed certs and expired certs etc.

That is the stupidest thing I've ever heard. Honestly, a paid-for cert is barely more trustworthy than a self-signed cert. The entire cert system is broken by design, and benefits nobody but the money collectors at the major companies (VeriSign, Entrust, etc).

Can somebody convince me that my understanding is mistaken?

Thanks,
Randy

It's as stupid as IE7's handling of it really. Without a better understanding of the certification process by the end user, the benefits are certainly not as clear. Certainly it prevents MITM issues during the https transaction, but that may be about it with some exceptions. With IE7 it can certainly produce problems on an internal network, at least initially. IE7 will actually refuse to connect you with the site. Bluecoat at least provides you with the opportunity to exclude a network from checks, like your own.

On the pros side of the fence, with a paid certificate such as those through Verisign, the benefit over a self signed cert is a lot clearer. Unfortunately there are companies that will hand you a cert with very little in the way of verification which destroys the usefulness of it. Self signed certs are useful in instances where you trust the issuer to begin with, or in corporate networks. For a small company trying to establish an ecommerce presence however, they have not yet earned the trust or established themselves to the point where jane and joe intertubes can (or should?) trust them.

Tremaine

Test Your IDS

Is your IDS deployed correctly?

Find out quickly and easily by testing it with real-world attacks from CORE IMPACT.

Go to

http://www.coresecurity.com/index.php5?module=Form&action=impact&campaign=intro_sfw
to learn more.

Test Your IDS

Is your IDS deployed correctly?

Find out quickly and easily by testing it with real-world attacks from CORE IMPACT.

Go to http://www.coresecurity.com/index.php5?module=Form&action=impact&campaign=intro_sfw
to learn more.
