

RE: Bittorrent – utorrent

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ids/2007-03/msg00055.html>

- *From:* "Erick Jensen" <ejensen@xxxxxxxxxxx>
 - *Date:* Mon, 19 Mar 2007 17:11:01 -0500
-

With that said...

If I am a client in your network and you come to me and say, STOP THE BIT TORRENT!! (Because you have no idea what I downloaded) I will come back and say, I downloaded a copy of Red Hat via Bit Torrent. How do you argue that? You have to make a broad policy of "No Bit Torrent for any reasons". That would be the only way to ensure that no illegal/copyrighted material comes in. It would also be a very impractical way to handle the situation.

If you were able to enforce the "No Bit Torrent" policy, wouldn't it just be easier to check the desktops for a bit torrent client installed? No extra overhead needed.

There still needs to be a way to differentiate the legit bit torrents from illegal/copyrighted bit torrents.... I don't see one, and if there is one, don't tell Comcast!!

Last idea: Watch for file downloads that end in .torrent That would be your only clue to what kind of material is in the encrypted bit torrent stream.

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

From: listbounce@xxxxxxxxxxxxxxxxxxx [<mailto:listbounce@xxxxxxxxxxxxxxxxxxx>] On Behalf Of David J. Bianco
Sent: Monday, March 19, 2007 9:40 AM
To: Ove Dalgård Hansen
Cc: focus-ids@xxxxxxxxxxxxxxxxxxx
Subject: Re: Bittorrent – utorrent

Ove Dalgård Hansen wrote:

I am in a bit of trouble,

On a network where i am configuring IDS – using ASA5510 + SSM module, we try to deny access to Bittorrent downloads – it consumes quite a bit of bandwith and is not allowed by the company's policy.

We try to filter bittorrent which succedes – but the utorrent changes protocol and goes by the SSL port 443 and thereby circumvent the IDS, since its not possible to see the encrypted traffic.

Does anyone out there have a good idea of how i am to solve the issue?

RE: Bittorrent – utorrent

Hi, Ove. I see that you've gotten quite a few responses, but I have to say that they all seem pretty impractical. Decrypting SSL? Um...

Anyway, it turns out that P2P traffic is actually pretty easy to detect if you have the right monitoring tools. Most of the other posters here have been assuming that you'd want to use a signature based IDS like snort or some gateway content inspection device, but by now you've already figured out that they don't work well for this.

The trick is to look for intrinsic characteristics of P2P traffic. Specifically, BitTorrent works by contacting a lot of different peers to download small portions of the larger file. What you need to do is to look for individual systems on your network that talk to lots of different external hosts. The more hosts they talk to, the more likely that they're running some P2P application. Most BitTorrent transfers stand out quite clearly when you create a list of your own hosts, sorted by the number of external hosts they've talked to in the last 24 hours.

The advantages to this are that it doesn't matter if they use SSL or not, since you're not reading the bits, just the session data records. Also, they can change ports all they like, since you're only concerned with the number of unique IPs they talk to.

There are two disadvantages, though. First, you have to set up some infrastructure to monitor session records. I'm using Sguil, so I already have this information handy in a SQL database, but you could use something like NetFlow or SFlow if your routers support it. There are also a number of standalone tools like Argus or SANCP that would do the job, albeit with a bit of scripting work on your part.

The second disadvantage is that you can't tell *exactly* what P2P traffic you're seeing. I do sometimes see Skype traffic, for example, that looks a bit like BitTorrent when you're just seeing the session records. However, for larger transfers (TV shows, movies, ISOs), the BitTorrent stands out because it often involves a thousands of unique IPs, more than would be expected in a typical Skype session.

Anyway, I hope this helps answer your question. This is a good example of how using the right tool for the job can really simplify things. Not all monitoring is done via signature matching!

David

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

RE: Bittorrent – utorrent

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.
