Norton Internet Security 2003 blacklist fault?

Source: http://www.derkeiler.com/Mailing−Lists/NT−Bugtraq/2003−09/0026.html

---

From: Greg Lawton (*gjl_at_PENACASATA.DEMON.CO.UK*)
Date: 08/22/03

```
Date:         Fri, 22 Aug 2003 21:12:23 +0100
To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM
```

Hello, all. First time poster on this list − so be gentle!

I was going to post this in a Symantec newsgroup first, and give them a chance to respond − but I took one look at the hundreds of groups that they run...

Basically, Norton Internet Security (tested with the current 2003 version) has, like any other firewall, an ability to stop access to a given site depending on a firewall rule.

I have discovered that when you enter a rule to block a specific site, the software does a regular lookup for the sites IP address at the time you enter the rule. (So it can't add sites while you're off line − it has to be able to talk to your DNS server). That IP address is used as the blacklist target.

Several worrying problems with this :−

1) If the blocked site then changes IP address, it's not caught. The ruleset will give the name of the site you think it's blocking, but it doesn't know it's moved. Since the block runs on IP addresses, that site is free to be accessed again.
2) Because large sites have multiple subdomains, such as www.bbc.co.uk, news.bbc.co.uk, this means that just entering bbc.co.uk (don't know why you'd want to ban the fine BBC, but it's an example) won't block news.bbc.co.uk.

Basically, it doesn't block on matching the URL typed with the ruleset, it blocks on a blacklist of IP addresses resolved at the time each site was added.

What do you all think?

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo
Whatever Happened to Octopus?

LEGATO RepliStor, formerly known as Octopus, delivers breakthrough

replication performance that's 5X faster than the competition in an
independent head−to−head test. Learn how RepliStor uses patented,
asynchronous, real−time replication, to deliver disaster recovery, data
distribution and consolidated backups. It is the first replication solution
to achieve Windows 2003 certification. Get the performance report now.

http://portal1.legato.com/products/replistor/upgrade.cfm

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo