

HTTP DDoS attack on our servers

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/incidents/2003-07/0046.html>

From: Markus Peter (*warp_at_spin.de*)

Date: 07/08/03

Date: Tue, 08 Jul 2003 15:06:32 +0200

To: incidents@securityfocus.com

Hello

Since yesterday, about 8pm CET, we observe a strange phenomenon on one of our servers, which appears like a DDoS attack. The characteristics do not match those of the typical known UDP DDoS tools but is TCP based.

Basically, > 8.000 IP numbers are sending HTTP requests to our server on a non-HTTP port (8000), which ran an entirely different, not HTTP related service on this machine. The IP numbers are mostly assigned to Europe and North America.

The requests always look the same way:

```
GET /index.htm HTTP/1.1
Accept: */*
User-Agent: UserAgent
Connection: close
Host: <our ip number>
```

Please note that they literally supplied "UserAgent" as User-Agent – I only removed our ip number from the requests. Each attacking host opens multiple connections per second. Even though the server which ran at 8000 could not handle HTTP requests at all and immediately closed the connection after the first sent line, the sheer number of connection attempts was enough to basically force us to put the service offline, as we had over 60.000 concurrent TCP connections due to this.

Due to the above described characteristics, I'm pretty sure that it's not just a misguided link on some large website, but some sort of non-browser program doing the requests.

We nmapped some of the requesting machines. All of the scanned hosts appear to be running windows, with all of them having TCP port 45836 open. If we try connecting to that port, the connection is either immediately closed again by the remote end, or occasionally kept open indefinitely, but in neither case any data is sent back to us.

SecurityFocus Incidents: HTTP DDoS attack on our servers

I'm now completely puzzled on what is happening and what kind of tool we confront. Anyone else experiences incidents like those?

--

Markus Peter - SPiN AG
warp@spin.de

Attend the Black Hat Briefings & Training, July 28 - 31 in Las Vegas, the world's premier technical IT security event! 10 tracks, 15 training sessions, 1,800 delegates from 30 nations including all of the top experts, from CSO's to "underground" security specialists. See for yourself what the buzz is about! Early-bird registration ends July 3. This event will sell out. www.blackhat.com
