Record-breaking cyberattack hits anti-spam group (Update 2)

March 27 2013, by Raphael Satter

The Internet may have been slowed by one of the largest cyber attacks ever seen, which targeted a European group that patrols the Web for spam, security experts said Wednesday.

A record-breaking cyberattack targeting an anti-spam watchdog group has sent ripples of disruption coursing across the Web, experts said Wednesday.

Spamhaus, a site responsible for keeping ads for counterfeit Viagra and

bogus weight-loss pills out of the world's inboxes, said it had been buffeted by the monster denial-of-service attack since mid-March, apparently from groups angry at being blacklisted by the Swiss-British group.

"It is a small miracle that we're still online," Spamhaus researcher Vincent Hanna said.

Denial-of-service attacks overwhelm a server with traffic—like hundreds of letters being jammed through a mail slot at the same time. Security experts measure those attacks in bits of data per second. Recent cyberattacks—like the ones that caused persistent outages at U.S. banking sites late last year—have tended to peak at 100 billion bits per second.

But the furious assault on Spamhaus has shattered the charts, clocking in at 300 billion bits per second, according to San Francisco-based CloudFlare Inc., which Spamhaus has enlisted to help it weather the attack.

"It was likely quite a bit more, but at some point measurement systems can't keep up," CloudFlare chief executive Matthew Prince wrote in an email.

Patrick Gilmore of Akamai Technologies said that was no understatement.

"This attack is the largest that has been publicly disclosed—ever—in the history of the Internet," he said.

It's unclear who exactly was behind the attack, although a man who identified himself as Sven Olaf Kamphuis said he was in touch with the attackers and described them as mainly consisting of disgruntled Russian

Internet service providers who had found themselves on Spamhaus' blacklists. There was no immediate way to verify his claim.

He accused the watchdog of arbitrarily blocking content that it did not like. Spamhaus has widely used and constantly updated blacklists of sites that send spam.

"They abuse their position not to stop spam but to exercise censorship without a court order," Kamphuis said.

Gilmore and Prince said the attack's perpetrators had taken advantage of weaknesses in the Internet's infrastructure to trick thousands of servers into routing a torrent of junk traffic to Spamhaus every second.

The trick, called "DNS reflection," works a little bit like mailing requests for information to thousands of different organizations with a target's return address written across the back of the envelopes. When all the organizations reply at once, they send a landslide of useless data to the unwitting addressee.

Both experts said the attack's sheer size has sent ripples of disruptions across the Internet as servers moved mountains of junk traffic back and forth across the Web.

"At a minimum there would have been slowness," Prince said, adding in a blog post that "if the Internet felt a bit more sluggish for you over the last few days in Europe, this may be part of the reason why."

At the London Internet Exchange, where service providers exchange traffic across the globe, spokesman Malcolm Hutty said his organization had seen "a minor degree of congestion in a small portion of the network."

But he said it was unlikely that any ordinary users had been affected by the attack.

Hanna said his site had so far managed to stay online, but warned that being knocked off the Internet could give spammers an opening to step up their mailings—which may mean more fake lottery announcements and pitches for penny stocks heading to people's inboxes.

Hanna denied claims that his organization had behaved arbitrarily, noting that his group would lose its credibility if it started flagging benign content as spam.

"We have 1.7 billion people who watch over our shoulder," he said. "If we start blocking emails that they want, they will obviously stop using us."

Gilmore of Akamai was also dismissive of the claim that Spamhaus was biased.

"Spamhaus' reputation is sterling," he said.