InSecurity Complex
August 6, 2009 4:32 PM PDT

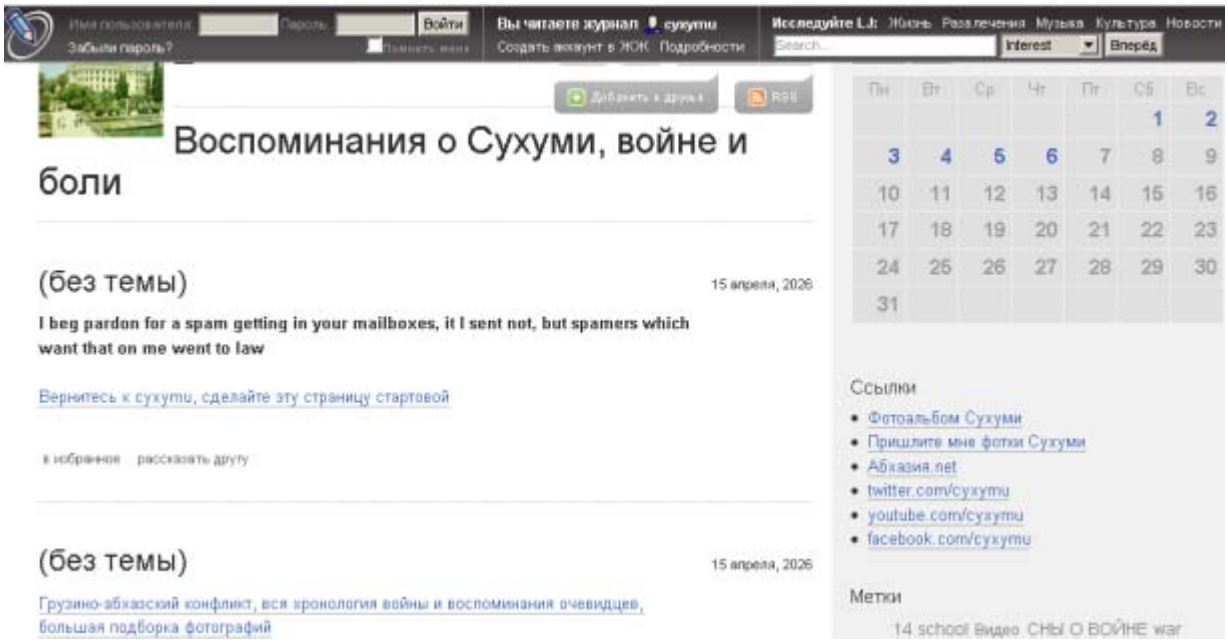
Twitter, Facebook attack targeted one user

by Elinor Mills

A Georgian blogger with accounts on Twitter, Facebook, LiveJournal, and Google's Blogger and YouTube was targeted in a denial-of-service attack that led to the sitewide outage at Twitter and problems at the other sites on Thursday, according to a Facebook executive.

The blogger, who uses the account name "Cyxymu," (the name of a town in the Republic of Georgia) had accounts on all of the different sites that were attacked at the same time, Max Kelly, chief security officer at Facebook, told CNET News.

"It was a simultaneous attack across a number of properties targeting him to keep his voice from being heard," Kelly said. "We're actively investigating the source of the attacks, and we hope to be able to find out the individuals involved in the back end and to take action against them, if we can."



Cyxymu LiveJournal account on cached version of Google. (Credit: LiveJournal)

Kelly declined to speculate on who was behind the attack, but he said: "You have to ask who would benefit the most from doing this and think about what those people are doing and the disregard for the rest of the users and the Internet."

Twitter **was down for several hours** beginning early Thursday morning, and it suffered periodic slowness and time-outs throughout the day.

Cyxymu's LiveJournal page wasn't accessible, but a cached version showed that it was updated on Thursday with a message about the denial-of-service, or DoS, attacks on his accounts on the United States-based sites. "Now it's obvious it's a special attack against me and Georgians," said the message, in Russian.

The site also apologized for a spam e-mail attack in which the sender was spoofed and made to look like the e-mails were sent by him. Screenshots are shown. It's unclear whether or how the spam attack is related to the DoS attacks.

In the distributed denial-of-service (DDoS) attack on the sites, computers that have been compromised by viruses or other malware are instructed by the attacker's computer to visit the specific Web sites all at the same time and repeatedly. The barrage of connection requests overwhelms the target sites, making it so that legitimate Web traffic can't get through.

Such coordinated attacks require the efforts of tens of thousands or more of hijacked computers, which together form a botnet. Spammers send e-mails with malicious attachments or URLs to millions of people to create botnets. Criminals also **can lease existing botnets** for specific campaigns for as little as 5 cents to 10 cents per bot.

A Facebook representative dismissed a theory that the attack was triggered by a spam campaign in which e-mails had links to the sites. It's unlikely that there would be enough recipients--all clicking on the URLs at the same time--to bring a site down, he said. There was a spam campaign that directed people to Cyxymu's accounts, but it wasn't the cause of the DoS, he said.

"The people who are coordinating this attack, the criminals, are definitely determined and using a lot of resources," Kelly said. "If they're asking our infrastructure to generate hundreds of pages a second, that's a lot of pages our users can't see."

Facebook and Google were able to minimize any impact to their sites, including Blogger, YouTube, and Google Sites, a free Web site service. Facebook even managed to keep the Cyxymu account accessible to Web surfers from that region, Kelly said, though it was inaccessible to people in other geographic areas, including San Francisco.

This was the first coordinated attack on the sites, and all the companies involved were working closely on the investigation, he said. "My team and the teams that are working together at all these companies are doing a really good job very quickly, and I'm proud and happy," he said.

Twitter and LiveJournal did not immediately return e-mails and calls seeking comment.

A Google representative offered this statement: "We are aware that a handful of non-Google sites were impacted by a DoS attack this morning and are in contact with some affected companies to help investigate this attack. Google systems prevented substantive impact to our services."

Political conflicts between Russia and its former republic spilled online last year with **DoS attacks** and Web site defacements going in both directions.

For more information, listen to **Larry Magid's podcast interview** with Elinor Mills.

Updated at 7:39 p.m. PDT, with Facebook saying a spam campaign did not cause the DoS, and at 6:35 p.m., with information from Cyxymu's site, more about the spam attack, how DDoS attacks work, and background on the Russia-Georgia conflict.

Elinor Mills covers Internet security and privacy. She joined CNET News in 2005 after working as a foreign correspondent for Reuters in Portugal and writing for The Industry Standard, the IDG News Service, and the Associated Press. E-mail Elinor.

Topics: **Criminal Hackers**, **Security**

Tags: **Google**, **Facebook**, **Twitter**, **DOS attack**

Share: Digg Del.icio.us Reddit Yahoo! Buzz Facebook