

**Virtualization
for Dummies**

Download the **FREE** eBook today!
Understand virtualization and how it can work for you.

Sponsored by  IDG  Sun  AMD

COMPUTERWORLD Security

 Print Article  Close Window

Cyberattacks knock out Georgia's Internet presence

Large-scale attacks, traffic rerouting traced to Russian hacker hosting network

Gregg Keizer

August 11, 2008 ([Computerworld](#)) Hackers, perhaps affiliated with a well-known Russian criminal network, have attacked and hijacked Web sites belonging to Georgia, the former Soviet republic now in the fourth day of war with Russia, a security researcher claimed on Sunday.

Some Georgian government and commercial sites are unavailable, while others may have been hijacked, said Jart Armin, a researcher who tracks the notorious Russian Business Network (RBN), a malware and criminal hosting network.

"Many of Georgia's Internet servers were under external control from late Thursday," [Armin said early Saturday](#) in an entry on his Web site. According to his research, the government's sites dedicated to the Ministry of Foreign Affairs, the Ministry of Defense, and the country's president, Mikhail Saakashvili, have been blocked completely, or traffic to and from those sites' servers have been redirected to servers actually located in Russia and Turkey.

As of midnight Eastern time on Sunday, Georgia's presidential and defense ministry sites were unavailable from the U.S. Although the [foreign ministry's site](#) remained online, the most recent news item was dated Aug. 8, the day Georgian and Russian forces first clashed.

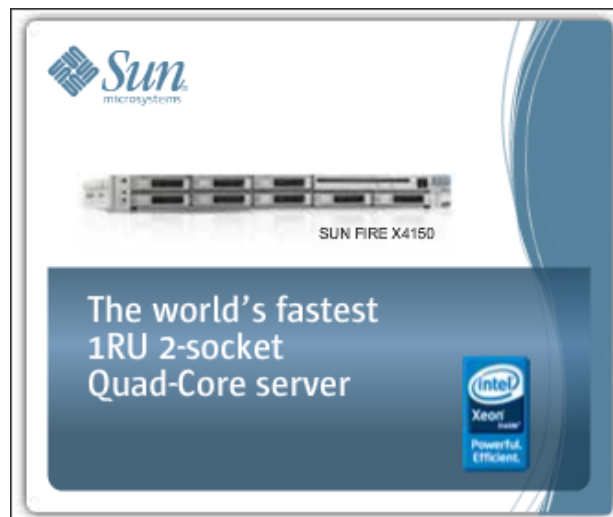
Armin warned that Georgian sites that appeared online may actually be bogus. "Use caution with any Web sites that appear of a Georgia official source but are without any recent news [such as those dated Saturday, Aug. 9, or Sunday, Aug. 10], as these may be fraudulent," he said in another entry posted midafternoon on Sunday.

Statements from Georgia's foreign ministry have appeared in a [blog hosted on Google](#), perhaps in an attempt to circumvent attacks.

Researchers at the [Shadowserver Foundation](#), which tracks malicious Internet activity, confirmed some of Armin's claims. "We are now seeing new attacks against .ge sites [*Editor's note: .ge is the top-level domain for Georgia.*] ... [www.parliament.ge](#) and [president.gov.ge](#) are currently being hit with HTTP floods," the researchers said in a Sunday update to a July post.

On Saturday, Armin reported that key sections of Georgia's Internet traffic had been rerouted through servers based in Russia and Turkey, where the traffic was either blocked or diverted. The Russian and Turkish servers Armin identified, he said, "are well known to be under the control of RBN and influenced by the Russian government."

RBN, which pulled up stakes last year and [shifted network operations to China](#) in an attempt to avoid scrutiny, has been fingered for a wide range of criminal activities, including a [massive subversion](#) of Web sites last March.



Later on Saturday, Armin added that network administrators in Germany had been able to temporarily reroute some Georgian Internet traffic directly to servers run by [Deutsche Telekom AG](#). Within hours, however, the traffic had been again diverted to Russian servers, this time to ones based in Moscow.

The attacks are reminiscent of other coordinated campaigns [against](#) Estonian government Web sites in April and May 2007 and against about 300 Lithuanian sites on July 1. Like Georgia, both countries are former republics in the Soviet Union.

Three weeks ago, a distributed denial-of-service attack [knocked Georgia's presidential site](#) offline for about a day.

Late Sunday, Russian ground forces were reported [advancing toward Gori](#), an important transportation hub in central Georgia.