

Federal Computer Week

'Noisy' cyberattacks have little effect

- By [William Jackson](#)
- Jul 08, 2009

Denial-of-service attacks against government Web sites in this country and South Korea appear to have had little impact and are not particularly sophisticated, experts say.

"It's a very noisy attack," said Rick Howard, intelligence director at VeriSign iDefense, which provides cybersecurity and intelligence services for private- and public-sector organizations. "Everyone in government says it didn't affect them that much."

"It's been more of a nuisance," said Phil Neray, vice president of security Strategy at Guardium. "We have countermeasures for denial-of-service attacks."

Several security companies have obtained the malicious code used to carry out the attacks. Symantec Corp. identified it as W32.dozer and a variant of the MyDoom worm that has infected a large number of computers.

About three-quarters of the targeted sites are run by the South Korea government, and most of the rest are U.S. government sites, including those for the Homeland Security, Defense and Transportation departments; the Secret Service; the Federal Trade Commission; and possibly the White House. A number of financial sites, including the Nasdaq and New York stock exchanges, and the Washington Post's Web site have also reportedly been hit in the same wave of attacks.

The distributed denial-of-service attacks used networks of compromised computers called botnets to send high volumes of traffic to sites with the intention of overloading the Web servers and making the sites unavailable. Although such attacks can be irritating and result in lost productivity if successful for a long enough period, they do no damage to the systems they are targeting.

Techniques for mitigating the attacks include distributing incoming requests among a large number of gateways so that the volume at any one site is small enough to be handled. Because most agencies have such solutions ready, the impact has been small, although the FTC site reportedly was unavailable for part of the day July 7.

There had been scattered reports of denial-of-service attacks over the July 4th weekend, but the bulk of the attacks appeared to have begun late on July 6 and early on July 7. The Shadowserver Foundation, which tracks botnet activity, showed a sharp spike in denial-of-service activity from known botnets on those days, shooting from a baseline of less than 100 to more than 700 for a short time.

Reports from South Korea have speculated that the attacks are state-sponsored activity from North Korea. But "they don't have any proof of that," Howard said.

He said others have speculated that the attacks were spurred by someone upset with the Post's news coverage, a response by North Korea to international condemnation of its recent missile tests, or an attempt to focus attention on U.S. cybersecurity policies and defenses.

Neray called the attacks an example of political cyber terrorism probably being carried out by a nation state, although there is little evidence of the source of the attacks. Reports from South Korea earlier this year indicated that North Korea had established a cyber warfare unit. Neray said the denial-of-service attack could be another example of North Korean provocations, in line with the recent missile tests.

Sophisticated attacks that do not draw attention to themselves and might allow information to be quietly gathered or manipulated without the owners' knowledge are a more serious threat than denial-of-service attacks, Neray said.

Sen. Tom Carper (D-Del.), chairman of the Homeland Security and Governmental Affairs Committee's Federal Financial Management,



**Get more done
with less
space.**

HP Blade Server System

 

[Click to learn more >](#)

Government Information, Federal Services and International Security Subcommittee, said today that the incidents highlight the need for improved cyber defenses.

Carper called for passage of legislation he introduced in April — the U.S. Information and Communications Enhancement Act of 2009 (S. 921), which would rewrite the Federal Information Security Management Act of 2002. The legislation would enhance the power of the Homeland Security Department's U.S. Computer Emergency Readiness Team to take action before a cyberattack penetrates government networks.

About the Author

William Jackson is a senior writer for GCN.



hp **Get more done.** With help from emtec federal

Click for our latest whitepapers on streamlining server infrastructure.



© 1996-2009 1105 Media, Inc. All Rights Reserved.