

## Cyberattacks on federal Web sites may be smokescreen

By Jill R. Aitoro 07/08/09

The type of cyberattack that took down multiple federal Web sites this week is more of a nuisance than a threat to national security, according to computer security experts, but it can be used to conceal more serious attacks on networks and systems.

Denial-of-service attacks, under which Web sites are bombarded with heavy amounts of traffic in an effort to force them to shut down, [knocked a number of agencies' sites offline](#) starting July 4, including those of the State, Transportation and Treasury departments, the Secret Service, and the Federal Trade Commission. No sensitive information was stolen or classified systems accessed, according to a [Washington Post report](#).

After detecting the attacks, the Homeland Security Department's Computer Emergency Response Team, which analyzes cyber threats and disseminates warning information, issued guidance on mitigating the threats to public and private sector organizations.

"If this were an attack directed at a critical service or during a time of national crisis, I'd say this could be a serious problem, but there are no indications that this event is anything more than a directed nuisance," said Dean Turner, executive editor of the *Internet Security Threat Report*, published by Symantec, a security software provider.

But some security experts wonder whether there's more to the attacks than meets the eye. Denial-of-service attacks against public Web sites can be an effective means of distracting network administrators while other, more sensitive computer systems and applications are targeted. DHS has not released any advisories to indicate more serious attacks occurred against federal computer networks or systems, but that doesn't mean they haven't taken place, said a former intelligence official who asked to not be named.

"I worry about what we don't see more than what we do see," he said. "Create a smokescreen by taking down a bunch of Web pages, and then while you're lamenting and trying to fix it, I'll eat your breakfast somewhere else without you even knowing."

Turner agreed that denial-of-service attacks can be a diversion from more serious incidents, where hackers "hide in and amongst the noise, while the other attack is low and slow."

The growing number of collaborative online services federal agencies offer makes Web sites a bigger target than ever, said Tom Kellermann, vice president of security awareness at Core Security Technologies and the former senior data risk management specialist for the World Bank's security team. Agencies, he said, need to focus on locking down their Web applications.

"The most troubling reality is what occurred before and after the sites were attacked," he said. "Was [malicious code] used to infiltrate the back-end networks and databases? It is paramount that government agencies increase their level of Web application testing and network penetration tests to ascertain their vulnerability before they are hacked."

Attacks will continue to increase as agencies rely more and more on the Internet, said Dale Meyerrose, former chief information officer for the Office of the Director of National Intelligence. He currently serves as vice president and general manager of cyber and information assurance for the information technology consulting firm Harris Corp.

"Every capability in reverse is a vulnerability," he said. "The ability to send a message opens an avenue of attack. So you develop cyber awareness and that's what helps keep you well."

---

© 2009 BY NATIONAL JOURNAL GROUP, INC. ALL RIGHTS RESERVED