

One number. One voicemail. Wonderful.

Turn your desk and mobile phones into one with Sprint Mobile Integration.



Get it now

COMPUTERWORLD Government

Print Article Close Window

Online attack hits US government Web sites

Robert McMillan

July 7, 2009 (IDG News Service) A botnet comprised of about 50,000 infected computers has been waging a war against U.S. government Web sites and causing headaches for businesses in the U.S. and South Korea.

The attack started Saturday, and security experts have credited it with knocking the U.S. Federal Trade Commission's (FTC's) Web site offline for parts of Monday and Tuesday. Several other government Web sites have also been targeted, including the U.S. Department of Transportation (DOT).

"The DOT has been experiencing network incidents since this past weekend. We are working with the U.S. Computer Emergency Readiness Team [US-CERT] at this time," a DOT spokeswoman said Tuesday.

A spokeswoman for the U.S. Department of the Treasury confirmed that the Treasury's Web site had been hit with a denial-of-service attack. "We're working with our service provider to mitigate the impact," she said.

A spokeswoman for the FTC could not say what caused the outage at that agency's Web site, and the US-CERT did not return calls seeking comment.

Other targets have included banking Web sites in Korea, U.S. Bancorp, the U.S. Secret Service, the U.S. Department of Homeland Security, the U.S. Department of State, the White House, the U.S. Department of Defense, the New York Stock Exchange, the Nasdaq and the Washington Post, according to security researchers studying the incident.

The attack, while powerful, is not particularly sophisticated and appears to be more of a nuisance than a threat to security. It uses a variety of well-known distributed denial of service (DDoS) attacks that try to overwhelm Web sites with useless requests and make them unavailable for legitimate users, security experts say. Most of the targeted sites appeared to be working normally on Tuesday.

Such DDoS attacks are relatively common, but a few things make this week's incident unusual. The botnet code behind the attack does not use typical antivirus evasion techniques and does not appear to have been written by a professional malware writer, according to Joe Stewart, a researcher with SecureWorks who has looked at the code.

On Saturday and Sunday the attack was consuming 20 to 40 gigabytes of bandwidth per second, about 10 times the rate of a typical DDoS attack, one security expert said after being briefed by the US-CERT on Tuesday. "It's the biggest I've seen," said the expert, who asked not to be identified because he was not authorized to discuss the matter. By Tuesday it was averaging about 1.2 gigabytes per second, he said.

Security experts estimate the size of the botnet at somewhere between 30,000 and 60,000 computers.

It is also unusual to see relatively low-profile government Web sites being hit. "Who goes around targeting a site like the FAA or the U.S. Treasury? It's not something that most people would think to attack," Stewart said.

The FTC in the past has brought actions against spammers and Internet fraudsters. Last month it [shut down](#) an Internet service provider called Pricewert, which had been associated with botnets, spam and child pornography.

No one knows who is behind the attack, although Stewart said it could have been launched by a single person. "It just seems to me that somebody is mad for some reason at capitalist governments," he said. Security experts say most of the infected machines are located in South Korea, but that doesn't mean the attack originated there.

The fact that the DDoS attack took down government computers is an embarrassment to the U.S., which is working to strengthen the country's cyber-security defenses under President Barack Obama.

"These are very basic attacks and stuff we've seen for a very long time. The scale of these isn't very huge either," said one security expert, who spoke on condition of anonymity because he wasn't authorized to discuss the matter publicly. "It's embarrassing that these sites have been hit for four or five days and they're still being affected. Think of the money that eBay and Amazon would lose in four to five days of this."

(Grant Gross in Washington and Nancy Gohring in Seattle contributed to this story.)