

Cyber Security Vulnerabilities

A one-pager for the Internet Caucus Advisory Committee

October 2007

Bots are the weapon of choice for cyber crime and orchestrated attacks

Given just one page to catalog cyber security vulnerabilities, we chose to focus on just one threat – *bots* – remotely-controlled programs hidden on millions of computers worldwide.

Bot networks are already generating attacks of overwhelming volume, in ways that are nearly impossible to stop or to trace back to their origins. Earlier this year, government web sites in Estonia were crippled by denial-of-service attacks coming from a network of bots. Investigators still don't know who triggered and controlled the attack.

Bot networks are growing in number and power, to where they now pose a serious threat to the U.S. government, businesses and online consumers. According to Secure Computing, more than 250,000 personal computers are infected with bots each day, putting at least 10 million computers at the disposal of those with bad intentions.

Bots are used by illegitimate businesses to generate billions of spam emails and to spread malware worldwide. Moreover, criminal organizations use bots for identity theft via phishing scams. Attacks like that in Estonia may be merely practice drills by crime factions to showcase their computing firepower and their ability to disrupt networks.

Can we stop the bots?

Law enforcement and internet infrastructure companies are cooperating to discover who's planting and orchestrating bot net attacks, but with limited success. The Internet's very nature makes investigations difficult, especially after the fact.

In what amounts to an arms race, operators of the Internet infrastructure are investing constantly to add capacity to handle the volumes of transactions generated by bot attacks. They are also adding teams of professionals and new systems to perform real-time network monitoring and rapid response.

But there remains one aspect of the bot threat that can't be addressed by centralized systems or government investigators. End users are a critical line of defense, in how they recognize and avoid deceptive tricks designed to download bots to their computers. User awareness is becoming even more critical as the Internet rapidly expands beyond the billion people online today, and reaches the four billion people not yet online.

The 'Next Billion' Internet Users may bring on the 'Next Billion' Bots

The *Wall Street Journal* reported this week that ICANN, manager of the Internet domain name system, is implementing internationalized domain names (IDNs). IDNs will help the next billion Internet users enter web addresses entirely in their native language and character sets. As part of this project, ICANN is encouraging users to test native character domain names in their browsers, email software, and other applications.

At the same time, ICANN and others should be warning new internet users against downloading any patches or new applications unless they are dealing with a trusted website and scanning for viruses and malware. Otherwise, ICANN is inviting the "next billion" users to download the "next billion" bots capable of generating spam, phishing fraud, and the kind of denial-of-service attacks that brought down Estonia's internet.

Contact: Steve DelBianco

sdelbianco@ACTonline.org

202-420-7482