

# Wireless World: Attack of the 'botnets'

March 17 2006

---

A botnet -- or robotic network -- sends an instant message to your smart phone. You think it is from a friend and open the IM. But it's not a chatty note at all, as the automated message fraudulently scans the system, looking for your credit-card numbers, bank-account statements and secret passwords.

Experts tell United Press International's Wireless World that computer criminals are now using these "botnets" to attack consumers and businesses via text messaging, adding to the threats and problems created by the new, emerging mobile technology.

Researchers at Foster City, Calif.-based Face Time Security Labs this week identified the new threat, which they characterize as high risk. As companies like Research In Motion (the developer of the BlackBerry handheld wireless communications device) and Skype add instant-messaging capabilities, this kind of problem is only expected to increase, experts said.

The increased attacks on instant-messaging networks come just as the technology application is starting to take off here in the United States. Instant and text messaging first took off in Europe.

"One of the biggest reasons why text messaging is soaring is lower cost," Brian Hicks, co-director of Independent Mobile, a marketer of mobile technologies based in Framingham, Mass., told Wireless World. "It used to be that you would have to pay a la carte. Every carrier now offers text messaging packages. Some start as low as \$2.99."

Consumers and businesses like this kind of messaging technology because it is a simple way to communicate while on the go, Hicks said.

Instant messaging can be, however, somewhat disruptive in the workplace, Paul Kole, a telecom expert and president of Paul Kole & Associates in Cambridge, Mass., told *Wireless World*. "The biggest issue with instant messaging is being interrupted during work, and not always by work-related messages," said Kole. "It's also very tempting to use IM behind someone's back during a meeting."

Another big, emerging issue is storage of all of these text and instant messages "in order to document business information," said Kole.

According to Jason Cherveney, president of Sanity Solutions, a computer consulting firm based in Denver, a lot of companies are starting to examine "at-rest encryption," meaning that they encrypt all of the data in a database, not just information that is in transit.

Stephen Foskett, a director at GlassHouse, a reseller and software developer based in Framingham, Mass., tells *Wireless World* that the cost of storage can be quite expensive -- \$1 a month per stored tape. Many large corporations have 50,000 tapes of corporate information already in storage.

This is expected to increase exponentially with the rise of instant and text messaging. "In order to capture the few messages that are important, many times you need to sort through them all," said Kole. "There's a good chance that a large amount of personal chatter might get stored in addition to all of the important information, which does add up in storage costs."

Even university libraries -- including the facility at Princeton University -- are now using instant messaging to assist students. Students instant

message the librarian, who looks to see if books or articles are available for research projects. She then instant messages the student, telling him what is on the shelf and what is checked out. This is most certainly faster than the old-fashioned card catalog that most of us used during our own college days.

"It is absolutely the most economical way to communicate," said Hicks.

Computer hackers know this -- which is why they have developed the botnet attacks. Researcher Face Time has identified more than 40 unique files, already, that are used for attacks via instant-messaging networks, including one that hides the stealth application in the systray under the heading "beh.exe."

The researchers have provided the information about the hackers to federal authorities, who are investigating. Protection of the legitimate instant-messaging communities is vital if they are to survive. Text messaging is taking the benefits of the computer and bringing it out to people when they are mobile.

"The growth of online communities and social networks has been staggering, but their success is limited so long as they remain tied to the PC," said Carl Ford, vice president of Pulver.com, a leading interactive content developer. "Extending presence and availability to mobile phones is a no-brainer."

*Copyright 2006 by United Press International*

Citation: Wireless World: Attack of the 'botnets' (2006, March 17) retrieved 19 April 2024 from <https://phys.org/news/2006-03-wireless-world-botnets.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.