



TUESDAY, JULY 5, 2011

Hackers target small-company sites

Many owners don't know they've been compromised

By Byron Acohido
USA TODAY

Criminals who infect websites are making the Internet much riskier for small-business owners.

Since early June, one gang has used a uniquely insidious attack to place malicious code, called "scripts," on some 20,000 to 30,000 sites, many of them small businesses that rely on the Internet to reach customers, says Wayne Huang, chief technical officer at website security firm Armorize.

Many businesses don't realize how intently hackers strive to take control of their sites to run scams, says Maxim Weinstein, executive director of the non-profit StopBadware consulting firm.

Because mass injection can be automated, such attacks have become a staple of the cyberun-

derground. IBM's X-Force security division blocked fewer than 10,000 such attacks a month in early 2008; by mid-2009 it blocked more than 500,000 a month.

Criminals use corrupted websites to spread infections to other PCs, thereby fueling data theft as well as scams to sell fake drugs, pitch worthless anti-virus protection and steal from online bank accounts. "Your website essentially serves as a surrogate host for malicious content," says David Moeller, CEO of website monitoring and backup company CodeGuard.

Attacks like the one that recently hit Passen Law Group, a two-man personal injury firm in Chicago, are extremely difficult to detect and remove, Huang says. About a month ago, attorney Matt

Ripe for cyberattack

Hackers target small businesses' websites because:

- 36%** rely on free consumer anti-virus applications.
- 31%** have no anti-spam.
- 23%** have no anti-spyware.
- 15%** have no firewall.
- 13%** have no security at all.

Source: Panda Security fall 2010 survey of companies with two to 1,000 computers in North America, Europe and Latin America

Passen clicked to the main page of his firm's website and says he saw "a series of letters and numbers that made no sense to me."

Then Google notified Passen that his website was infected and blocked access to it. Over the next few weeks, Passen hired experts to delete the viral script. The first two fixes lasted about a week each before the infection recurred. "It will easily cost us a couple thousand dollars to remedy, and I can't tell you what the costs are in terms of lost business opportunity," Passen says.

Remediation can be a real pain. Free guidance is available from StopBadware.org. And once a website is returned to a clean state, CodeGuard offers a free service that enables the owner to eradicate any malicious scripts.