New cyberattacks target small businesses

Posted 7/4/2011 11:32:58 AM |

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 been using a uniquely insidious type of automated attack to inject malicious code on some 20,000 to 3 0,000 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 small business owners don't realize about how intently profit-minded hackers are striving to wrest control of their websites to run scams, says Maxim Weinstein executive director of the non-profit StopBadware public awareness group.

"A sophisticated and evolved criminal underground is constantly trying to avoid being detected while spreading their malware ever more effectively," says Weinstein.

Mass injection attacks begin with the bad guys obtaining the usernames and passwords for the administrator accounts of smaller websites. They can purchase logins from data thieves, steal it for themselves, or get them free from hacktivist groups that publicly post stolen account data.

After logging on as the site administrator, the hacker then injects a small program, called a script, that gives him full control of the website server.

Because mass injection can be automated, such attacks have become a staple of the cyberunderground. IBM's X-Force security division monitored and blocked fewer than 10,000 such attacks per month in early 2008. By mid-2009 it blocked more than 500,000 per month, according to the most recent data.

Hackers target small business websites because they know those companies "do not have the resources for sophisticated security measures," says Michael Lin, vice president at VeriSign, a division of Symantec.

Criminals use corrupted websites to spread infections to other PCs, thereby fueling data theft as well as scams to sell fake drugs, pitch worthless antivirus 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.

The latest mass-injection attacks —including one that recently hit Passen Law Group, a two-man personal injury firm in Chicago — are extremely difficult to detect and remove, says Huang. About a month ago, attorney Matt 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."

Shortly afterward, Google notified Passen that his website was infected and blocked access to it. Over the next few weeks, Passen, who depends on his website to attract clients, hired experts to find and delete the viral script three times; 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.

Most often, the owner of a hacked website doesn't see anything suspicious. The infected site eventually turns up on one of the blacklists maintained by Google, Microsoft and a handful of other entities that continually look for, and block access to, sites running malicious scripts.

Google's blacklist, which is used by Google Chrome, Firefox and Apple's Safari browsers, currently blocks access to some 700,000 sites, says StopBadware's Weinstein.

Remediation can be a real pain. A cottage industry of consultants and technicians has cropped up to help small business owners, but prices and quality of work varies. A good starting point for any small business owner is to seek free guidance at StopBadware.org.

CodeGuard offers a free service that backs up sites and then continuously monitors for fresh infection. Should a site be compromised, CodeGuard enables the owner to eradicate infections by returning the site to a known clean state."

"The game is changing," says CodeGuard's Moeller. "Anyone who has a website can be attacked, and you have a responsibility to make sure you're not hosting malicious content."