

Internet criminals gaining ground, experts say

Deborah Gage, Chronicle Staff Writer

Tuesday, May 6, 2008

Criminal attacks against major Web sites have grown so common that Internet users have no reliable way to know which sites are safe to visit, no matter how well known those destinations are, security experts say.

News of the latest attack comes from Finjan, an Israeli security firm, which is reporting today that last month it found a large cache of information - including confidential medical records, financial records and business e-mails - sitting unprotected on a computer network server in Malaysia.

[[Related story: Protecting yourself from infected sites](#)]

The data came from more than 40 major financial companies around the world, including the United States, and was stolen from computers belonging to doctors and home users conducting online banking and, in some cases, from machines inside corporate networks that the hackers managed to penetrate and infect. Finjan has notified the companies, which it declined to identify, as well as law enforcement agencies in several countries.

Included in the stolen information were medical diagnoses and insurance details, Social Security numbers, the recorded keyboard strokes of online shopping sessions and e-mails from businesses discussing an impending court case.

The largest banks "were not surprised we found this data," said Yuval Ben-Itzhak, Finjan's chief technology officer. "The second-tier banks were surprised and thanked us very much. Other businesses were also very appreciative - overall, we had a very positive response."

At any moment, thousands of sites are sitting on the Web hosting malicious software code designed to try to steal information, said Mary Landesman, a researcher at ScanSafe, a Web security provider in San Mateo.

The numbers are staggering - in April, Yahoo Inc. detected 7.8 billion links served up by search engines that led to compromised sites. In statistics collected by hackers, who were tracking an attack of their own that was discovered last year by Finjan, 500,000 computers had been infected.

Many of these attacks are invisible to computer users - there are no clues in the appearance of a Web site that you are being redirected to a compromised site.

If your computer is vulnerable, all it takes to get infected is to visit a hacked site. Most likely, you will unwittingly download a Trojan, a piece of software disguised as a valid program but that really performs another action, such as shipping out your personal information to a server that could be halfway around the world.

Never-ending scrutiny

"We have our hands full on a daily basis tracking this stuff," said Paul Ferguson, a researcher for Trend Micro, a Web security vendor in Cupertino. "Professional criminals and organized crime have ongoing, sustained campaigns to rob consumers blind."

The attacks come in waves, Landesman said. In September, media and entertainment sites were attacked; in November, it was sports sites; and in January, she said, it was the "general purpose mainstream sites, the brick and mortar of the Internet."

Some of the sites are well known - during the past few months they've included MySpace, USA Today, MSNBC and several more of the Web's top sites.

The goal is to steal and sell personal information to conduct identity theft and sometimes extortion.

Researchers say the attacks have been rising since early 2007. They peg them to the rise of a malicious software code industry that mirrors the legitimate software industry. For a few hundred dollars, thieves can buy toolkits with names like Mpack and Adpack that automate attacks - and even come with customer service.

The toolkits take advantage of flaws in popular software such as Web browsers, Yahoo Messenger, Apple's QuickTime, Adobe Flash and JavaScript.

Some of these flaws are mistakes in the code for which software vendors supply a patch. The idea for the hackers is to exploit the flaws before computer users get around to applying the patches.

Some sites to blame

Sometimes, the attacks can be blamed on Web site operators. In one recent case, sites were compromised because they were running misconfigured versions of Microsoft's Internet Information Server.

"There are a lot of mom-and-pop operations out there, and they hire some (Web) consultant who comes in and collects the money and goes," Ferguson said.

But the attacks also take advantage of design flaws in the Web itself, which was not created with security in mind. Some of the same software that makes the Web so exciting to use also makes it a gold mine for thieves.

"If a security guy had designed the Web, it would look different - like a mainframe with a green screen - and we'd all be excited by blinking urls," said John Pescatore, a vice president at Gartner. "The Internet has exploded because of what security people say are fatal flaws."

All Web sites are vulnerable to these attacks, and site operators who don't take precautions - by testing code before they post it, for example, or using Web security gateways to block malicious sites - are at risk, he said.

An attack that Trend Micro was tracking on Friday, for example, went like this: Cyber criminals selected Internet addresses owned by particular companies in Italy and scanned their Web sites for exploitable software flaws. They also found a vulnerable server in San Diego and infected that. "Now they were open for business," Ferguson said.

Computers exploit flaws

They loaded the server with a malicious software program that scanned any computers that visited the target sites for software flaws. When the program found flaws, it temporarily redirected victims' computers from the target sites to the server, which downloaded yet another malicious program onto the computers, allowing thieves

Internet criminals gaining ground, experts say

to run their programs undetected. The computers were then returned to the target site.

In this case, because the server was in the United States, Trend Micro was able to report the case to the FBI.

Big companies whose sites have millions of visitors a month are prime targets - Sears.com, Target.com and Walmart.com were all attacked in March.

But big sites also tend to have better security, Landesman said. An even bigger danger to the public are smaller niche sites - like the baby-naming site YeahBaby, which was hit last month - that have loyal repeat visitors and show up high in search results.

"It's a domino effect," she said. "If they can compromise one site and get to the site owner's system, sometimes they can gain complete access of the hosting server, and all other sites that sit on it are impacted. It's pretty amazing to watch."

Seeking peace of mind

Computer users often can't tell whether a Web site they're visiting is compromised. While none are foolproof, there are a number of things you can do to help protect yourself, such as:

- Keeping browsers up-to-date to make use of the latest security features.
- Downloading free Web plug-ins that help block malicious sites.

For more detailed tips, see story on A10

E-mail Deborah Gage at dgage@sfchronicle.com.

<http://sfgate.com/cgi-bin/article.cgi?f=/c/a/2008/05/06/MNMS10HCM0.DTL>

This article appeared on page **A - 1** of the San Francisco Chronicle