Hackers expose weakness in visiting trusted sites

August 2 2009, By JORDAN ROBERTSON , AP Technology Writer

(AP) -- A powerful new type of Internet attack works like a telephone tap, except operates between computers and Web sites they trust.

Hackers at the Black Hat and DefCon security conferences have revealed a serious flaw in the way Web browsers weed out untrustworthy sites and block anybody from seeing them. If a criminal infiltrates a network, he can set up a secret eavesdropping post and capture credit card numbers, passwords and other sensitive data flowing between computers on that network and sites their browsers have deemed safe.

In an even more nefarious plot, an attacker could hijack the auto-update feature on a victim's computer, and trick it into automatically installing malware pulled in from a hacker's Web site. The computer would think it's an update coming from the software manufacturer.

The attack was demonstrated by three hackers. Independent security researcher Moxie Marlinspike presented alone, while Dan Kaminsky, with Seattle-based security consultancy IOActive Inc., and security and privacy researcher Len Sassaman presented together.

They reached essentially the same conclusion: There are major problems in the way browsers interact with Secure Sockets Layer (SSL) certificates, which is a common technology used on banking, e-commerce and other sites handling sensitive data.

Browser makers and the companies that sell SSL certificates are working

on a fix.

Microsoft Corp., whose Internet Explorer browser is the world's most popular, said it was investigating the issue. Mozilla Corp., which makes the No. 2 Firefox browser, said most of the problems being addressed were fixed in the latest version of its browser, and that the rest will be fixed in an update coming this week.

VeriSign Inc., one of the biggest SSL certificate companies, maintains that its certificates aren't vulnerable.

Tim Callan, a product marketing executive in VeriSign's SSL business unit, added that the "tap" won't work against so-called Extended Validation SSL certificates, which cost more and involve a deeper inspection of a company's application for a certificate.

The attack falls into a class of hacks known as "man-in-the-middle," in which a criminal plants himself between a victim's computer and a legitimate Web site and steals data as it moves back and forth.

Jeff Moss, founder of the Black Hat and Defcon conferences who this summer was appointed to the Homeland Security Department's advisory council, said the fact a hacker has to actually break into a victim's network for the attack to work can limit its usefulness.

"That's the nice mitigating thing," he said.

But he warned that "for targeted attacks it's absolutely deadly. This is the way you can get everything. If you can get in the middle, you can get everything. It's a big, giant wake-up call for the industry."

SSL certificates are a critical technology in assigning trust on the Web.

Sites buy them to encrypt traffic and assure visitors it's OK to enter confidential information. Companies that sell SSL certificates verify that someone trying to buy a certificate actually owns the site that certificate will be attached to.

The presence of an SSL certificate on a site is designated by a padlock in the address bar. But many people don't pay attention to whether a padlock is present or not.

Browsers do care, though, which is why this week's talks were significant.

Browsers are programmed to block sites that don't have a valid SSL certificate, or have a certificate displaying a Web address that doesn't match the address a Web surfer was trying to reach (which can indicate someone has hijacked a person's Internet session). If the sites aren't blocked, users are warned about potential danger, and have the option to click through.

The problems outlined by researchers center on a quirk in the way browsers read SSL certificates.

Many SSL certificate companies will allow people to attach a programming symbol called a "null character" into the Web address onto the certificates they receive. Web browsers generally ignore that symbol. They stop reading at that symbol when they're checking the Web address on a certificate.

The trick in the latest type of attack is that all a criminal would need to do is put the name of a legitimate Web site before that character, and the browser will believe that the site it's visiting - which is under the criminal's control - is legitimate.

The criminal could then forward the traffic onto the legitimate site and spy on everything the victim does on that site. It's a complicated attack, but it highlights a significant weakness in the very technology widely used to assure people it's safe to navigate sensitive sites.

Jon Miller, an SSL expert and director of Accuvant Labs, said he expects significant attacks against corporations using this technique in the coming months. Criminals who run "phishing" scams, in which people are tricked into visiting phony sites, will also likely latch on.

"What kind of makes this earth-shattering is these aren't the most sophisticated attacks in the world," he said. "This is going to become a huge problem."

There are signs it's already starting.

VeriSign's Callan said within hours of the talks, his company got a number of applications for SSL certificates featuring null characters, but they were denied.