InformationWeek
BUSINESS INNOVATION POWERED BY TECHNOLOGY

Cyberattack Fools You Once, Evades Detection

The attacks represent a "quantum leap" for hackers in terms of their technological sophistication and pose a serious challenge to the IT community, one security firm reports.

By Larry Greenemeier, InformationWeek
June 14, 2007
URL: http://www.informationweek.com/story/showArticle.jhtml?articleID=199904381

Cyberattackers have adapted the ability of Web sites to analyze the demographics of site visitors in order to create a new breed of drive-by malware downloads that defy detection.

These so-called "evasive attacks," as labeled by Web security appliance maker and security researcher Finjan in its most recent Web security trends report, are especially sneaky because they infect visitors only once before fading into obscurity.

Here's how evasive attacks work: A malware writer finds a vulnerability in a Web site and infects that site with malware that can deliver a virus or some other malicious payload to unsuspecting site visitors. When someone visits the infected Web site, the malware identifies the visitor by his IP address, browser version, and other data. The infected site does an IP lookup to see if that visitor has already visited the site.

If the visitor is new to the site, the site will deliver its malicious payload. If the visitor has already been to the site -- and has already been infected -- "the site will actually serve the site's real Web pages and traces of the malicious code are hidden," Finjan CTO Yuval Ben-Itzhak told *InformationWeek*.

The malware restricts access to the malicious code to a single view from each unique IP address. "This can keep security vendors from developing signatures against the malicious code," he added. "It's considered evasive because you see the attack only once."

These attacks represent a "quantum leap" for hackers in terms of their technological sophistication and pose a serious challenge to the IT community, Finjan concluded in its Web security trends report for the second quarter of 2007, conducted by the company's Malicious Code Research Center. These attacks evade signature-based and database-reliant security methods.

Since the malicious code on the infected host Web site accesses its own database of IP addresses to determine whether to serve up malware or legitimate content, URL filtering, reputation services, and even search engines might mistakenly classify these polluted sites as legitimate. Meanwhile, the malicious code's payload is being used to steal sensitive financial and personal information such as bank-account details, credit-card numbers, and Social Security numbers.

The only real way to combat this new technique at this time is for businesses to patch and protect their Web sites from being compromised in the first place. Barring that, Web users need to keep their Web browser patches up to date and analyze in real time any code that Web sites attempt to install on their computers.