HACKERS have found a way to intercept passwords for banking websites by infecting pop-up ads with a program that can install itself on computers and record user keystrokes, security experts said. The new type of threat was discovered last week by the Internet Storm Center of the SANS Institute, a collaborative effort of private security firms and university researchers.

Storm Center director Marcus Sachs said hackers apparently infiltrated advertiser servers and effectively "poisoned" certain pop-up ads to install a program that reads keystrokes and relays them to a website operated by hackers.

"The evil part of the scheme is that it has a list of about 50 banks, and if it detects that your browser is going to that bank ... it looks for login passwords, and intercepts that information before it gets encrypted," Sachs said.

He said the latest threat is a variant of "spyware" which installs programs on the computers of those browsing the Internet and can sometimes hijack browsers.

Sachs said the new type of malicious code or "malware" has a different origin from a threat reported earlier this week involving websites that are infected, but that the goal of both programs are the same - to steal banking passwords.

"We think both of these are being done by organized crime," he said.

In both cases, the websites receiving the stolen information have been shut down by Internet administrators, Sachs said.

But the two attacks highlight new risks to transmission of sensitive financial information on the Internet, experts said.

Tom Liston, a SANS analyst, said he was concerned about the new technique.

"I believe that this particular type of malware represents a huge threat to the online financial industry," he said in a posting on the SANS website.

"The approach ... makes this method of stealing identity information all the more insidious."

Sachs said that although the websites involved in the stolen data have been shut down, removing the immediate threat, "that doesn't mean the owners of that technique cant put it someplace else."

He added that users can be protected by keeping browsers and anti-virus software updated.

"This is preying on is people not keeping their software up to date," he said.

Don Rhodes at the American Bankers Association said the Microsoft browser security update from April should prevent any harm from the latest threat.
"Consumers need to be aware and pay attention to the latest developments regarding security," he said.

"Every time we hear about a significant new threat, we notify our banks about it. We may do it this time although we don't know the exact extent of that particular threat yet."

*Agence France-Presse*

This report appears on australianIT.com.au.