Turmoil fuels 'hacktivist' attacks on Web sites

June 25 2009, By JORDAN ROBERTSON , AP Technology Writer

FILE - This Sunday, June 21, 2009, file photo shows a demonstrator carrying a sign identifying herself with Neda, a young Iranian woman shown in a video bleeding to death on the street of Tehran. She was part of a group protesting in front of the White House in support of protesters in Iran and to condemn Iran's Supreme Leader Ali Khamenei's decision to suppress the protests, in Washington. The Internet video turned the mystery woman into an instant icon of her country's opposition.(AP Photo/Alex Brandon)

(AP) -- For about 90 minutes Wednesday, visitors to the Oregon University System's Web site found themselves taken for a ride they didn't ask for. They were redirected to another site under the control of a hacker, who posted an 89-word screed criticizing the protests in Iran.

"We never cheated in elections," the site read, in black and red. The message included invective aimed at President Barack Obama and made derogatory comments about Iranian opposition leader Mir Hossein Mousavi, who claims the June 12 presidential election was rigged.

As Internet attacks go, this type isn't uncommon, and the site was quickly restored to normal. The attack also didn't appear to harm visitors' machines: The site appeared to only serve up a political message rather than a computer virus, as some hacked sites carry. Very few people were likely affected, too: The site averages fewer than 1,000 hits a day.

What the incident shows, though, is how political turmoil can spill quickly into unexpected parts of the Internet, as sites that have nothing to do with a conflict often get hijacked and turned into bully pulpits for so-called "hacktivists" bent on advancing a political cause, rather than making money.

"It's a bit like graffiti on the subway," said Graham Cluley, senior technology consultant with Sophos, a computer security software company. "Web sites that aren't properly protected are like blank subway walls. Hackers can come by and spray their political messages."

The schism in Iran over the disputed presidential election has already led to a range of Internet attacks. Some activists have been urging supporters to try to take down government sites with so-called "denial-of-service" attacks, in which the sites are flooded with so much Internet traffic that their servers buckle. Mounting those attacks can be relatively easy using widely available hacking programs.

That assault may be working: Many official Iranian sites are currently inaccessible, though it's unclear whether the outages are hacking-related. For its part, Iran has employed filtering technology to restrict what sites

people in the country can visit.

The incident at the Oregon University System, which oversees Oregon's seven public universities, is just one example of what happens repeatedly whenever a political conflict flares these days. The war in Iraq, fighting in Israel, the Beijing Olympics and the Russia-Georgia conflict all saw examples of hackers commandeering sites to push their political message.

Sites that are hacked in this way aren't necessarily targeted for their political affiliations. Instead, hackers seek them out because of security vulnerabilities in their computer networks. Those vulnerabilities can be simple to find with automated tools hackers have built to sniff out weaknesses in Web sites' programming code.

Figuring out the culprits is usually very hard, sometimes impossible, because it's easy to cover your tracks online. And unless the hackers leave some kind of hint that they're associated with a larger criminal gang, there's little chance law enforcement will get deeply involved.

"More and more people are kind of thinking this is acceptable behavior on the Internet," Cluley said. "If you're clever and smart and don't do something dumb, your chances of getting caught are probably quite small."

Oregon University System spokeswoman Diane Saunders said the school system was analyzing computer files for clues about who might be responsible. She said the hackers were able to access the site through a vulnerability in third-party software that tracks the number of visitors to the site. That vulnerability has now been fixed.

In many cases, major world events give online criminals a great opening to try and lure more victims into garden-variety Internet swindles.

Alan Paller, director of research for the SANS Institute, a computer security training organization, said hundreds of fake Web sites spring up after every big news event to try and fool people into coughing up their money or personal data, or both. Sometimes they'll take the form of fake Red Cross sites, for example, that solicit donations.

The bad guys are really good at making fake sites look real. They're also relentless advertisers: Spam volumes also surge after a big news event, with crooks trying to direct victims to sites that will infect their computers.

Paller says the effectiveness of those campaigns "is almost entirely determined by how well they exploit current news stories" and craft provocative headlines to sucker somebody into clicking on the link.

The hackers behind Oregon University System's Web site attack got noticed - for 90 minutes at least.

Associated Press writer Joseph B. Frazier contributed to this story from Portland, Ore.