NY Times site inaccessible, Twitter problems also

MARTHA MENDOZA, AP National Writer

SAN JOSE, California (AP) — Readers who tried to click on the New York Times' website got nothing but error messages for several hours during the site's second major disruption this month, and people also had trouble accessing Twitter. A hacker group calling itself the "Syrian Electronic Army" claimed responsibility.

Within minutes of Tuesday's attack, the New York Times quickly set up alternative websites, posting stories about chemical attacks in Syria. "Not Easy to Hide a Chemical Attack, Experts Say," was the headline of one. The service was restored early Wednesday.

"Our Web site was unavailable to users in the United States for a time on Tuesday," the newspaper said in a post on its website. "The disruption was the result of an external attack on our domain name registrar, and we are at work on fully restoring service. We regret if this has caused you any inconvenience."

The cyberattacks come at a time when the Obama administration is trying to bolster its case for possible military action against Syria, where the administration says President Bashar Assad's government is responsible for a deadly chemical attack on civilians. Assad denies the claim.

"Media is going down ..." warned the Syrian Electronic Army in a Twitter message before the websites stopped working, adding that it also had taken over Twitter and the Huffington Post U.K.

Times spokeswoman Eileen Murphy said the disruption was caused by a "malicious external attack" that affected its website and email, while Twitter spokesman Jim Prosser said the viewing of images and photos was sporadically affected. Huffington Post U.K. did not respond to requests for comment.

Both Twitter and the Times said they were resolving the attack, which actually hit an Australian company that registered their domain names, Melbourne IT.

Theo Hnarakis, chief executive of Melbourne IT, the world's sixth largest registrar of Internet domain names, said the security breach occurred at a major-U.S.-based global reseller, or domain agent, where the hackers launched a "spear phishing attack" within the past week to steal the log-in details of the New York Times and Twitter domains.

Hnaraski declined to name the reseller, which is a major Melbourne IT client.

"This activist group used a very, very sophisticated spear phishing attack," Hnarakis told AP. " They sent very dubious emails to staff of one of our resellers whose area of expertise is looking after the domain names for major corporates including the

New York Times."

"Unfortunately, a couple of the staff members of the reseller responded by giving their email log-in details; the group were able to search their emails for sensitive information that included the user name and password for the New York Times, and from there it all cascades," Hnarakis said.

"We don't put this down to a technical failure. We put it down to human error where someone has inadvertently provided their information and from there, a major a site like the New York Times was down for several hours," he added.

The hackers had also tried to hack into Twitter.com, but failed because that domain was protected by an optional secondary security feature offered by MelbourneIT for the past two years. Times had opted not to have the same level of security.

"If they had had the security option turned on, they wouldn't have been affected," MelbourneIT chief technology officer Bruce Tonkin said.

"We do have a security mechanism that would protect the names from this sort of attack," he added. "Naturally, we are reviewing security and doing an incident review and will probably add some additional security."

Tonkin said the hacker seemed to have also accessed the credentials of the Huffington Post domain, which is held by a UK registry.

"The hackers have just posted a screen shot to say they've logged into the (Huffington Post) account, but I'm not aware that they actually changed anything," Tonkin said.

Tracking the hack even further, computer forensics from security firm Renesys Corp. traced the Internet protocol addresses back to the same ones as the Syrian Electronic Army's website sea.sy, which the firm said has been hosted out of Russia since June.

A Syrian Electronic Army activist confirmed to The Associated Press that the group hijacked the Times' and Twitter's domains by targeting Melbourne IT.

"I can't say how, but yes we did hit Melbourne IT," the hacker said in an email. No further details were disclosed.

The hacker's true identity isn't publicly known, but he has long used an email address linked to the group, and a second group member has vouched for his credentials.

The Syrian Electronic Army has, in recent months, taken credit for Web attacks on media targets that it sees as sympathetic to Syria's rebels, including prior attacks at the New York Times, along with the Washington Post, Agence France-Press, 60 Minutes, CBS News, National Public Radio, The Associated Press, Al-Jazeera English and the BBC.

FBI spokeswoman Jenny Shearer in Washington said the agency has no comment on Tuesday's attack.

Tuesday's victims were hit by a technique known as "DNS hijacking," according to Robert Masse, president of Montreal, Canada-based security startup Swift Identity.

The technique works by tampering with domain name servers that translate easy-to-remember names like "nytimes.com" into the numerical Internet Protocol addresses (such as "170.149.168.130") that computers use to route data across the Internet.

Domain name servers work as the Web's phone books, and if attackers gains access to one, they can funnel users trying to access sites like The New York Times or Twitter to whichever rogue server they please. Masse said DNS attacks are popular because they bypass a website's security to attack the very architecture of the Internet itself.

"Companies spend a lot of time, money, resources and defending their servers, but they forget about auxiliary infrastructure that is integrally connected to their networks, like DNS."

Cybersecurity experts said hijacking attacks are preventable if website administrators are meticulous about what code they bring into their sites.

"As this incident illustrates, any time you integrate third-party code into your site, it presents a new attack vector for hackers. You must not only ensure your own code is secure, but you must also rely upon third parties' security practices," said Aaron Titus, a privacy officer and attorney at New York-based privacy software firm Identity Finder.

Michael Fey, a chief technology officer at Santa Clara, California-based cybersecurity firm McAfee, said that as long as media organizations play a critical role as influencers and critics, they will continue to be targets of cyberattacks.

He said the battle tactics are broad, from denial of service attacks, to targeted attacks using social engineering and to deploying information-gathering Trojans.

"Regardless of technology or tactics deployed, we should expect to see more of these attacks," he said.