Twitter hack: Made in Japan?

September 23 2010, By TOMOKO A. HOSAKA , Associated Press Writer

(AP) -- This week's Twitter attack that caused a widespread headache for the micro-blogging service appears to have been triggered by a Japanese computer hacker who says he was only trying to help.

The attack, which emerged and was shut down within hours Tuesday morning, involved a "cross-site scripting" flaw that allowed users to run JavaScript programs on other computers.

The originator is believed to be someone who uses the name "Masato Kinugawa" in cyberspace and acknowledges creating the Twitter account "RainbowTwtr" that demonstrated the vulnerability.

Through his Twitter account and personal blog, Kinugawa regularly tracks down possible computer security loopholes and notifies

companies of their existence. Earlier this year, he pointed out several scripting problems to Japanese Internet company Livedoor, which thanked him with a 15,000 yen ($177) gift certificate.

Kinugawa says he contacted Twitter about the weakness on Aug. 14 - but in vain.

"Twitter had not fixed this critical issue long after it had been notified," Kinugawa tweeted. "Twitter left this vulnerability exposed, and its recognition of this problem was low. Rather than have someone maliciously abuse this under the radar, I decided it would be better to urgently expose this as a serious problem and have it be addressed."

The account, which displayed messages in colors of the rainbow, spurred others like Australian teenager Pearce Delphin of Melbourne to spread the word about the vulnerability. "RainbowTwtr" has since been suspended.

In an e-mail to The Associated Press on Thursday, Delphin said he analyzed the code within the "rainbow tweets" and realized it could be tweaked to make a pop-up window appear just by moving a cursor over a message. Other users quickly picked up on Delphin's discovery and made their own changes, infecting unsuspecting accounts around the world.

San Francisco-based Twitter said it does not believe that any user information was compromised and that the "vast majority" of the breaches were pranks or promotions. The company said the attack began when a user, whom it did not identify, noticed a security hole and "took advantage of it."

"First, someone created an account that exploited the issue by turning tweets different colors and causing a pop-up box with text to appear

when someone hovered over the link in the tweet," the company said.

The White House's official Twitter feed - followed by 1.8 million users - was among those affected, though the offending message was quickly taken down.

Security breaches were common in Twitter's early days, but the company has since worked to beef up its vigilance and the problems have become less common. Tuesday's hack coincided with Twitter's ongoing rollout of a redesign of its website, which tries to streamline users' Twitter feeds and make it easier to see photos and videos directly on the site, without having to click on a link to YouTube or Flickr.

Twitter said it discovered and fixed this problem last month, and that a recent site update unrelated to the redesign was responsible for its return.