Twitter is hacked tuesday morning
Riva Richmond

Twitter was overrun with posts on Tuesday morning that used a programming flaw to play pranks, distribute porn and spread worms to unsuspecting users.

The problem was confined to Twitter's old Web interface, and did not affect the new interface that Twitter is gradually rolling out or the company's mobile applications. Security experts said that a JavaScript command in the offending posts included a command, "onmouseover," that caused messages to pop up and Web sites to open automatically when a mouse hovered over it. The script in some cases also caused a user to forward the offending link, spreading it virally to their followers and the rest of Twitter.

Twitter didn't immediately respond to a request for comment, but it posted a message on its status page saying: "We've identified and are patching a XSS attack; as always, please message @safety if you have info regarding such an exploit." At 9:50 Eastern time Twitter said it had fixed the flaw. (XSS is short for "cross site scripting" and refers to Web-application flaws that enable hackers to inject scripts into Web sites.)

Later Tuesday, Twitter Security Chief Bob Lord said in a blog post that the site patched the flaw used in the attack a month ago, but that a recent update "unknowingly resurfaced it." At 5:54 Eastern time, a user notified Twitter of the security hole, and Twitter fixed it by 10:00.

"Users may still see strange retweets in their timelines caused by the exploit," Mr. Lord said. "However, we are not aware of any issues related to it that would cause harm to computers or their accounts. And, there is no need to change passwords because user account information was not compromised through this exploit."

Among the pranks was one that apparently ensnared Sarah Brown, wife of the previous British prime minister, Gordon Brown. A link on her Twitter page redirected visitors to a hard-core Japanese porn site, according to a blog by Graham Cluley, an expert at the security software maker Sophos. Mr. Cluley said there were tens of thousands of dodgy links circulating on Twitter.

The first worm of this kind appears to have been launched Tuesday morning by Magnus Holm, a Norwegian Ruby programmer who uses the Twitter handle @judofyr. His post contained only a link, which had the embedded command "onmouseover," a JavaScript command that caused the link to be automatically Tweeted by anyone whose mouse cursor touched it. In an e-mail, Mr. Holm said he created the worm "because I wanted to experiment with the flaw," which he says was already being exploited by others. "The purpose was simply to see if it was possible to create a worm."

His worm turned the text in the post into black blocks to hide the dangerous text. Mr. Holm said his worm spread to at least 200,000 users. That, he wrote, "really surprised me! Because it was very easy to delete the Tweet that contained the worm, I expected that everyone would just delete it the moment they realized that they've been 'infected.' "

Mr. Holm described his worm as "harmless," but it appears to have inspired more malicious attacks by others. One such worm, which entirely took over victim's computer screens, appears to have been started by a Twitter user called @matsta. Matsta's Web site contained the 1980s singer Rick Astley's music video for "Never Gonna Give You Up" with an added message: "Rick is dancing because he just lost the game." Other attacks, including the first worm to strike the iPhone, launched in November 2009, also paid tribute to Mr. Astley. In rebel-Web parlance, clicking to see Mr. Astley is known as being "rickrolled." Twitter has since disabled @matsta's account.

A more malicious worm "downloaded some nasty code from a Russian server," Mr. Holm said, a fact that suggests cybercrime organizations might have joined the action.

The programming XSS flaw the attacks exploit is believed to have been discovered by Masato Kinugawa, known on Twitter as @kinugawamasato, who on Sunday claimed to have also discovered a similar flaw in Twitter's new Web interface. Last month's flaw, was rediscovered Tuesday morning and reported to Twitter by Mario Heiderich, a German freelance Web developer.

Cross-site scripting flaws exist in seven out of 10 of all Web sites, according to WhiteHat Security, a firm specialized in Web site security. Social networks have periodically contended with worms that exploit them since the Samy Worm struck MySpace in October 2005.

Security experts have been recommending that Twitter users avoid the Web site and instead use a third-party Twitter client like TweetDeck to access the service. Using a JavaScript blocker, such as the NoScript ad-on for Firefox, offers protections from attacks of this kind.

Fonte: The New York Times, Sept. 21th 2010. Disponível em:<www.nytimes.com>. Acesso em: 22 set. 2010.