Security
April 13, 2009 1:36 PM PDT

Twitter cleans up after weekend worm attacks

by Elinor Mills

Twitter security engineers were cleaning up on Monday following a series of worm attacks over the weekend, including at least two credited to a bored 17-year-old.

In the first attack, which began early on Saturday, four new accounts began spreading a worm, compromising about 90 accounts, Twitter co-founder Biz Stone wrote in a posting on the **Twitter blog**.

The worms appeared to do no damage other than spread to infected users' followers and modify profile pages. You can get infected just by clicking on the name or image of someone whose account was infected.

Later that afternoon, about 100 accounts were compromised in a second wave, followed by another wave on Sunday morning, he wrote. Nearly 10,000 tweets that could have spread the worm were deleted, according to Stone.

Late on Sunday and into Monday morning, Twitter fended off another attack, he said. "Once again, we secured the compromised accounts and deleted any material that would further propagate the worm," he wrote. Stone declined an interview request from CNET News, saying he didn't have time.

The worms exploit a common vulnerability in Web applications called cross-site scripting, which allows someone to inject code into Web pages others are viewing.

In this instance, Twitter users who clicked on the name or image of anyone sending the worm messages would get infected and then send the message on to all that person's followers. Anyone viewing an infected user's profile would also get infected and pass the worm on.

Interviewed by CNET News on Sunday after the first two iterations circulated, Michael Mooney, a 17-year-old living in Brooklyn, said he created the worms out of boredom. The messages in the first outbreak included a link to rival microblogging site, Stalkdaily.com, which Mooney owns.

Mooney said in the interview that he did not plan on releasing any more worms targeting Twitter. He could not be reached for comment on Monday.

The first worm messages warned people not to go to the StalkDaily site, which would infect a Twitter user's account if they visited the site. The second worm message contained the phrase "Mikeyy" and the third referred to removing the Mikeyy worm but used "bit.ly" to add shortened URLs to messages, said Andy Hayter, anti-malcode program manager for ICSA Labs, which provides third-party validation for security products.

The most recent attack involved a message saying "Hire Mikeyy" and included Mooney's phone number, according to Graham Cluley, a senior technology consultant with security firm Sophos.

"What we're seeing was it was possible for codes to be embedded, small pieces of JavaScript, into people's profiles. This should be fairly elemental to filter out," he said.

While the attacks were mostly a nuisance, they could have been dangerous if spyware or other malware had been downloaded onto Twitter users' computers, Cluley said.

To avoid such JavaScript-based attacks, you can turn off JavaScript in your browser. Instructions for doing this **are here**. You can also use utilities such as **NoScript**, an open-source **Firefox** extension, Hayter recommended.

Users of infected Twitter accounts should also **request a password reset** and go to the **settings page** and delete any profile or other information that may have been added

during the attack. To reset colors go to the **profile design page**.

Twittercism has detailed instructions on how to tell if you are infected and how to remove the worm.

And just like e-mail users should be careful what e-mail attachments they open, be careful who you follow on Twitter, Hayter said.

Updated 4:05 p.m. PDT with Sophos comment.

Elinor Mills covers Internet security and privacy. She joined CNET News in 2005 after working as a foreign correspondent for Reuters in Portugal and writing for The Industry Standard, the IDG News Service, and the Associated Press. E-mail Elinor.

Topics: **Vulnerabilities & attacks**

Tags: **Twitter**, **cross-site scripting**, **worm**

Related

From CNET

Twitter cleans up after weekend worm attacks

Teen claims credit for Twitter worms

CNET News Daily Podcast: Assessing the electrical smart grid's risk of attack

From around the web

New Twitter Worm Lures with Promises of ... eWeek

Teen claims responsibility for disruptin... CNN - Tech

More related posts powered by Sphere