

This information is taken from several sources: a USA Today article on July 30, 2009, and then using Google Searches.

When Michael Jackson died on June 25, 2009, his fans mourned — and cybercriminals swung into action. Within 38 hours, they forged alliances with familiar partners to trigger global spam campaigns that capitalized on the singer's death.

That was a potent reminder of the dangers that computer-savvy lawbreakers pose in a world that increasingly depends on the Internet for communications and commerce.

"Cybercriminals hunt prey with a velocity that's impossible for legitimate businesses to match," says Patrick Peterson, Cisco chief security officer.

The attacks after Jackson's death will be fresh on the minds of about 4,000 corporate managers gathering Wednesday to discuss cybercrime defenses at the annual Black Hat Vegas security conference.

"The bad guys are very adept at using Internet technologies," says Dave Marcus, director of research and communications at anti-virus firm [McAfee](#). "And unlike the good guys, they aren't restrained by any laws or jurisdictional boundaries."

Like most large-scale cyberattacks, the Jackson spamming runs were carried out by about a dozen elite crime gangs. Each controls networks of hundreds of thousands of infected

home and workplace PCs, called bots, which they lease to clients who want to carry out scams.

Longstanding clients include sellers of non-certified pharmaceutical drugs, herbal remedies, replica designer goods and worthless anti-virus subscriptions. Their hard drives brim with e-mail and website marketing material and software to carry out online sales.

They attract attention by referring to headline news, including the election of President Obama, the swine flu outbreak — and celebrity deaths. A

"They have templates ready so all they have to do is plug in words relating to a specific event," says John Harrison, director of Symantec's security response team.

So they were all set on the Thursday afternoon when news about Jackson's death began to spread.

Trolling for hot topics

"These groups monitor news outlets, Twitter and other social-media sites to discover hot topics," says Jose Nazario, manager of security research at Web security firm Arbor Networks.

Within a few hours, a smattering of amateurish spamming attacks began to appear. But the serious botnet gangs and cyberscammers took a little more time to coordinate large-scale campaigns.

By dawn on Saturday, a top botnet gang, Waledac, had a client: a well-known online drug retailer, GlavMed.com, also known as Canadian Pharmacy, Cisco senior researcher Henry Stern says.

The Waledac gang began deploying thousands of bots to spam out millions of e-mails with Web links purportedly leading to news about Jackson, he says. But the links actually redirected recipients to websites affiliated with GlavMed that sold sexual-performance drugs and pain killers.

A few hours later, another major botnet gang, known as Rustock, also blasted out Jackson-themed spam for GlavMed's online shopping sites.

"Rustock is run by a different group of criminals, but here it was spamming the same e-mails as Waledac on behalf of a common client," Peterson says.

A week after Jackson's death, criminals out to steal sensitive data or hijack online financial accounts began to move in. A major botnet gang called Pushdo launched a large-scale spamming campaign with enticing messages including: "Who killed Michael Jackson? Visit X-Files to see the answer." A Web link followed.

Clicking on it triggered what's known as a "drive-by download." The attacking bot scans for security holes in popular applications such as Internet Explorer, QuickTime and Adobe Acrobat Reader.

Breaking in

When it finds one, it swiftly secures access to the heart of the operating system, giving botnet controllers an opening to install any programs they want, including one called a root kit that makes the opening permanent.

Pushdo's client also paid the gang to install a customized version of a malicious tool, called Zbot, that watches for when the PC user logs on to any banking website. Zbot then steals the user name and password and forwards it to the client.

As with most drive-by downloads, the Pushdo gang got a bonus. The opening created by the bot remained in place after the client's work was done, giving the gang another bot for hire.

"This was just another routine spam campaign by Pushdo, but it had a malicious twist," says Phil Hay, lead threat analyst at security firm Marshal8e6.

The PushDo Botnet Group

The Pushdo botnet has been with us since January 2007, and while it does not grab as many headlines as its attention-seeking peers such as Storm or Conficker, it is the second largest spam botnet on the planet – sending approximately 7.7 Billion emails per day, making it single-handedly responsible for about 1 out of every 25 emails sent.

There are several reasons for Pushdo's lack of notoriety – the authors have actively used several techniques to help keep its activity “under the radar.” Not only is Pushdo responsible for a huge amount of spam activity, it also is one of the primary conduits for other criminal gangs to spread their malware creations.

Waledac Spam Botnet Group – July 4th 2009, Botnet

The Waledac spam/botnet may be dwindling, but that didn't stop its disseminators utilising this weekend's 4th of July celebrations to spread malicious executables, according to [Symantec](#).

Using attention-attracting spam mail, the group enticed users to visit malicious Waledac websites, then download and install the bot. One method of achieving this was to set up spoofed 'YouTube' sites, using these of similar words:

The Compelling Case for Video Telephony in UC: Download now

"Colorful Independence Day events took place throughout the country. This year July 4th firework's shows were surprisingly amazing. The largest firework happend this Saturday. Unprecedented sum of money was spent on this fabulous show even despite crisis.

"The American Pyrotechnics Association has named South Shore's Fourth of July fireworks show as the best pyrotechnic displays in the nation. If you want to see this

fantastic show just click on the video below and press "Run".

Click the pretend video frame, however, and instead of watching a clip you'll run one or several malicious Waledac executables with names such as "video.exe", "movie.exe", "run.exe" and "setup.exe". According to [PC Tools](#), which reported the attack, the bot continues to maintain a list of peer nodes for its P2P over HTTP technology in clean XML formatted data.

Rustock botnet leads spam surge up 60 percent in 2009

Spammers have now completely recovered the capacity lost last November by the shutdown of the botnet-hosting ISP McColo and spam levels reached 90 percent of all email in the first half of 2009, according to the latest spam report from [web security](#) firm Marshal8e6.

From January to June 2009, spam email surged by 60 percent, with 40 percent of spam coming from the Rustock botnet of compromised PCs, the report said.

Bradley Anstis, director of Information Technology at Marshal8e6, said Rustock has specialized in image spam and spoofing HTML templates from legitimate newsletters and inserts to lend spam the appearance of professional, legitimate email. Image spam spiked to account for 10 percent of all spam, he said.