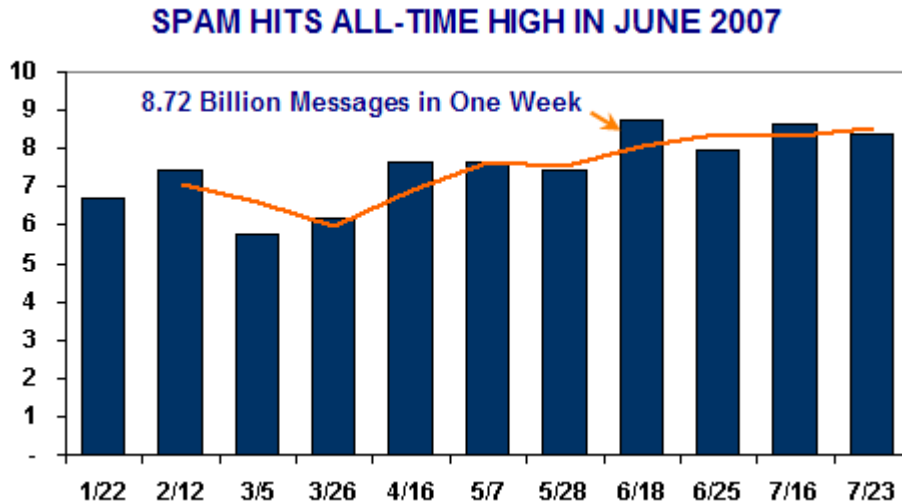


Postini Threat Advisory

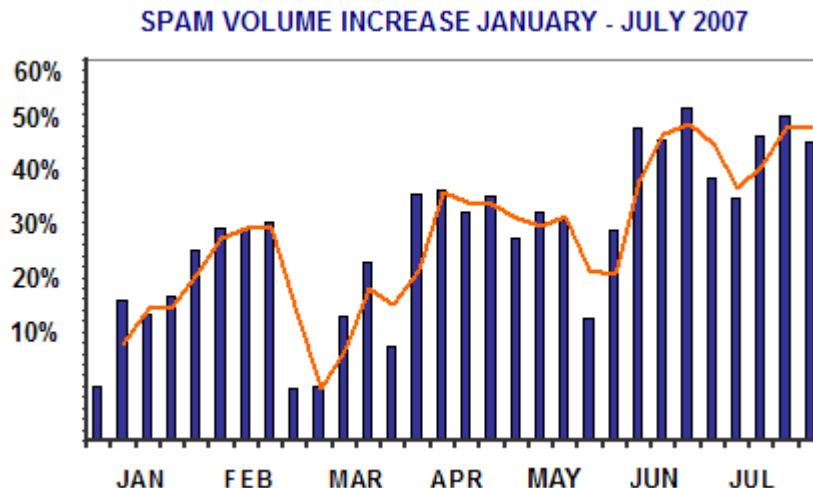
Spam Attack Update

Spam volumes set an all-time high in June, when volumes grew 51% since January 2007. In July, spam volumes dropped slightly. However, over 91% of all incoming email remains junk messages. Spammers are launching these massive attacks through the use of botnets — networks of compromised computers infected by hackers.



We also observed a significant jump in our blocking of messages with attached PDF and Excel files containing the spam "pitch." This is the result of a new tactic, in which spammers embed spam content in legitimate file types, such as .zip files and Excel files.

Image spam decreased from about 35% to about 25% of all junk messages. In terms of the total amount of spam, the use of PDF and Excel files has somewhat offset the decrease in image spam.

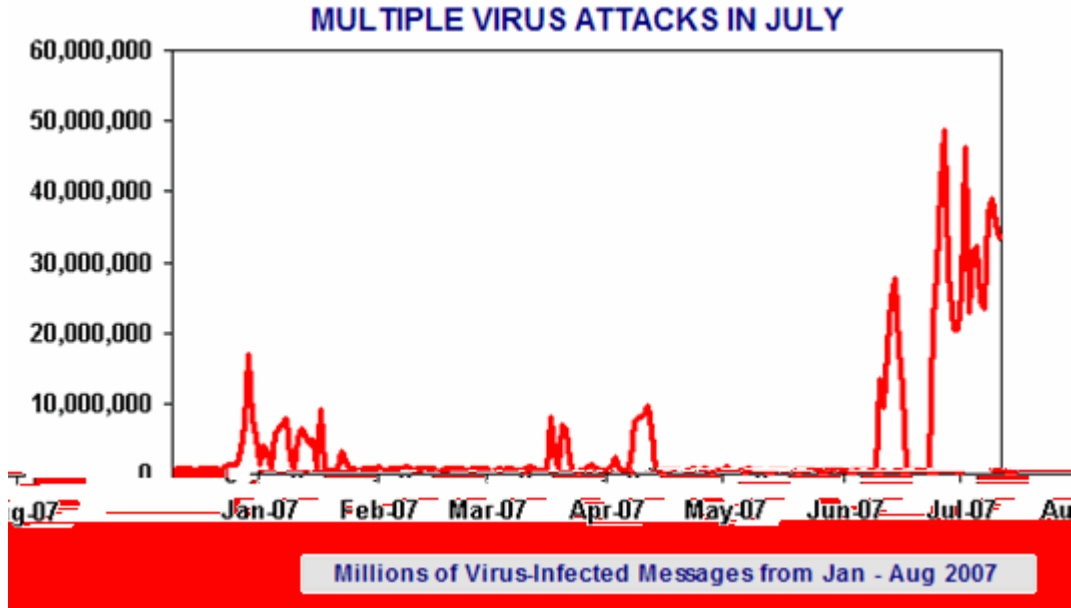


Virus Threat Update

July was the most active month for virus attacks in over two years. During a major attack from July 2-9, Postini tracked and blocked over 123 million virus-infected messages for customers. The volume of virus-infected messages was over three times larger than any attack over the past two years.

On July 16th, a new attack began that was still underway at the time of this report. Over half a billion virus-

infected messages have been sent during the course of this attack, making it over 14 times larger than any attack in the past two years.



These virus attacks are mutations of the "Storm" malware code family, which harvests computers into botnets. The "blended-attack" messages contain URLs to hacked websites that deliver the malware to the target computer. If a user clicks the link, this can secretly install a generic software downloader that allows hackers to download more malware to the user's system.

We see the hacker/spammer community rapidly evolving and specializing in delivering virus threats through email; botnets have become a commoditized resource that is available for rent. Botnets send virus-infected messages, which in turn harvest more computers into the spammer network. Botnets are largely responsible for constantly increasing spam volumes, image spam, and now PDF spam.

Postini Updates

We continually develop new security features, technology, and processes to combat the evolving virus attacks and spam tactics. Highlights of the Postini Email Security enhancements:

- Release 6.11 included improvements to Postini's operational processes which enable accelerated responses to emerging attacks. We now release filters more rapidly to counteract zero-hour spam and virus threats.
- In late August, we will release a new scanning technology that specifically targets the botnet spam and virus attacks. The Email Security service will monitor and detect spam attacks delivered through bot networks, even if the spam message is imbedded in legitimate content or valid file types.
- In a release in late August/early September, the Attachment Manager feature will filter password-protected .zip and other compressed attachments differently from standard compressed files. This helps protect against zero-hour virus threats by allowing you to bounce or quarantine password-protected .zip files that might contain hidden viruses.

Now Available: Release 6.11

Find out about the new Release 6.11 Email Security enhancements to the Message Center, Attachment Manager and more in the [Release Notes](#). A summary is also available as a [short video](#) or [slide presentation](#).

Release 6.11 also includes a new investigation feature for [Postini Message Archiving](#) and certificate validation for [Postini Encryption Services](#).

If you would like to unsubscribe, [please click here](#) | [Privacy Statement](#) | [Customer Log In](#) | [www.postini.com](#)

Postini, Inc. | 959 Skyway Road | San Carlos, CA 94070

© 2007 Postini, Inc. [Legal and Patent Notices](#). Postini, the Postini logo, Postini Perimeter Manager, Postini Threat Identification Network (PTIN), Postini Industry Heuristics, and PREEMPT are trademarks, registered trademarks, or service marks of Postini, Inc. All other trademarks are the property of their respective owners.