Trends in Internet security

This story on the Web
- Flash page
- Non-Flash page
- Get the X-Force® 2007 Trend Statistics report (3.12MB)

Protect your network
- IBM Internet Security Systems

Address security threats
- Threat mitigation services
- Ethical hacking

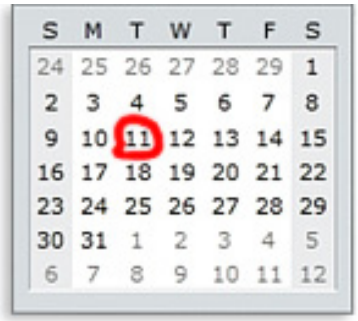
Safer architecture
- Internet security architecture
- Network security assessment

Where to go for more
- Expertise and solutions for strong IT security

Stay on top of innovation
- More Ideas from IBM

Insights and resources for
- CIOs
- Business Executives

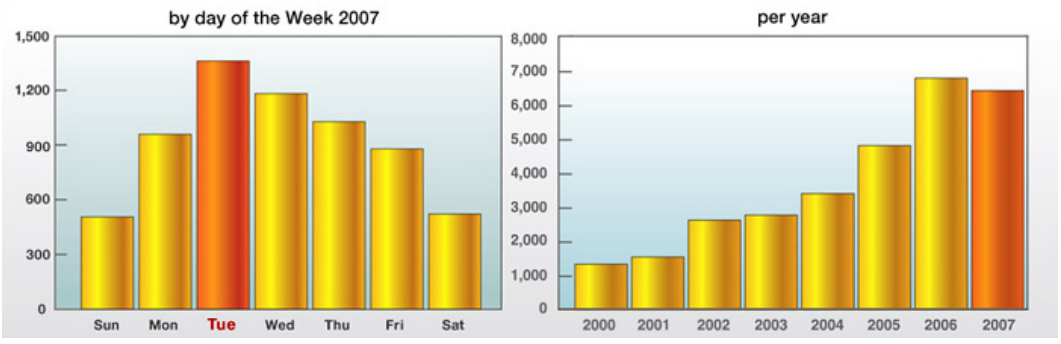
Patch tuesday



Pay attention to the calendar the next time you're asked by your computer to download a software update. There's a good chance it's the second Tuesday of the month, known by IT security experts as "Patch Tuesday." That's the day when many information technology vendors publicly announce newly discovered vulnerabilities in their software releases. These vulnerabilities might allow a hacker to take control of your machine, download your data, or even overwrite your system -- unless you install the patch.

Vulnerabilities Disclosed

Thanks to Patch Tuesday, more vulnerabilities were publicly disclosed on Tuesdays than on any other day of the week in 2007, with Wednesday coming in a close second. That's according to the research of IBM Internet Security Systems, which also found that 2007 was the first year in which fewer vulnerabilities were reported than in the previous year.



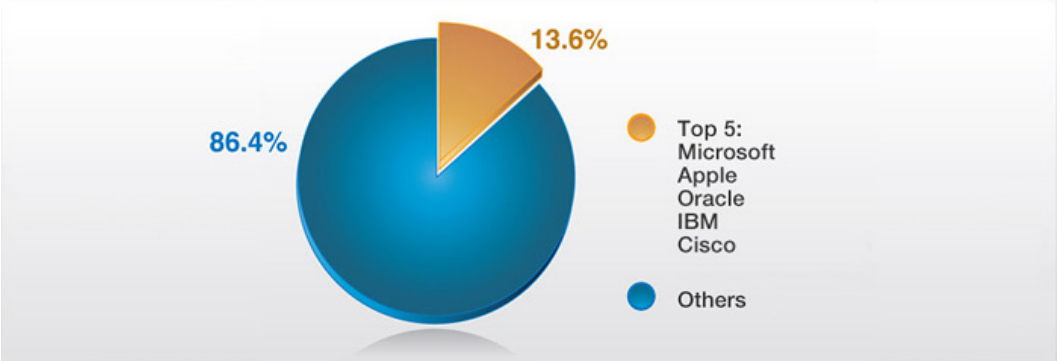
X-Force 2007 Trend Statistics

In their recent X-Force 2007 Trends report, they talk about the wide variety of online threats and vulnerabilities that raised their ugly heads last year. It's a fascinating look at the kind of Internet activity most of us wish would just go away, and which computer security experts work round the clock to thwart -- if they can.

Those threats range from garden-variety spam in your inbox to identity theft and hacker attempts to access computer systems remotely.

Accountability for Vulnerabilities 2007

A major focus of the report tracks the trends in these security vulnerabilities discovered and reported by software vendors themselves. As the X-Force statistics show, the top 5 software vendors — Microsoft, Apple, Oracle, IBM and Cisco — accounted for only 13.6% of the vulnerabilities reported in 2007.

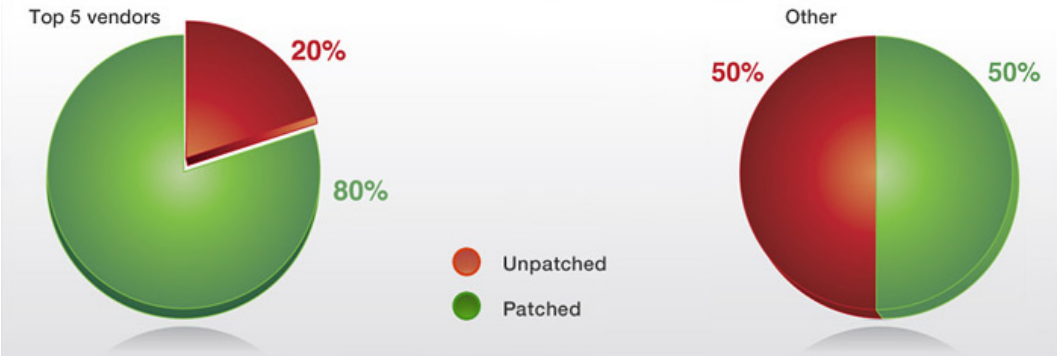


Patched vs Unpatched Vulnerabilities 2007

And four-fifths of their reported vulnerabilities were able to be repaired with a software patch.

Unfortunately, of the remaining vulnerabilities reported from other vendors, only half could be secured through such a patch.

Some of these security vulnerabilities are attempts exploit your Web browser, which the X-Force report covers in detail.



Critical Browser Vulnerabilities 2007

According to IBM Internet Security Systems, there's even an underground market in software toolkits for hackers to use to create new kinds of Web browser exploitation attacks. The latest trend is for hackers to lease these software development toolkits so they can get a piece of the action with an even smaller initial investment. In an irony that was probably expected, however, X-Force analysts now suspect that many of these same hacker tools are themselves subject to widespread piracy in that community.

What is "spam"?

spam (noun): Unsolicited e-mail, often of a commercial nature, sent indiscriminately to multiple mailing lists, individuals, or newsgroups;.junk e-mail

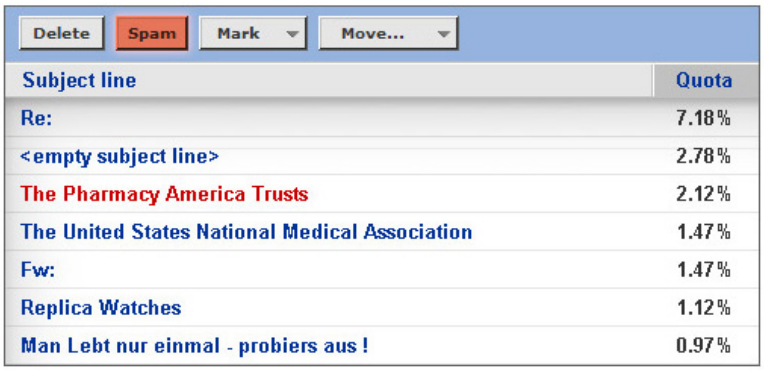
spam (transitive verb): 1. To send unsolicited e-mail to. 2. To send.(a message) indiscriminately to multiple mailing lists, individuals or .newsgroups.

— The American Heritage Dictionary of the English Language, 4th ed.

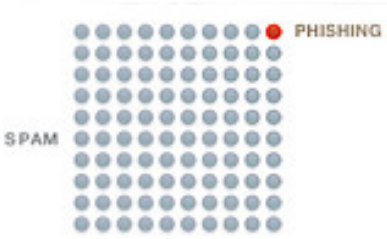
Everyday spam e-mails remain the network annoyance most of us are familiar with. And on an average day, IBM Internet Security Systems analyzes 150,000 unique spam messages. They found that, in 2007, 15% of the Internet's spam messages came from e-mail servers in the United States, followed by servers in Russia, Germany, and South Korea. But most spam is controlled by automated programs often called "bots" — and these can be manipulated remotely from any country, regardless of where the server is located.

Most popular subject lines for spam, late 2007

Often the subject line can be a clue before you open the e-mail -- but even those subject lines can range anywhere from an empty field to random offers for "replica watches." Offers for prescription pharmaceuticals and advertising masquerading as an e-greeting card were also popular techniques of spammers.



What is “phishing”?



By the end of 2007, 1 out of every 100 spam messages was something even more nefarious: an attempt to get someone’s personal information to commit identity theft, an illegal activity otherwise known as “phishing,” spelled with a “p-h.” This is a growing trend in consumer fraud and computer hacking, as many phishing expeditions try to trick consumers into turning over their financial information.

Most popular subject lines for phishing, late 2007

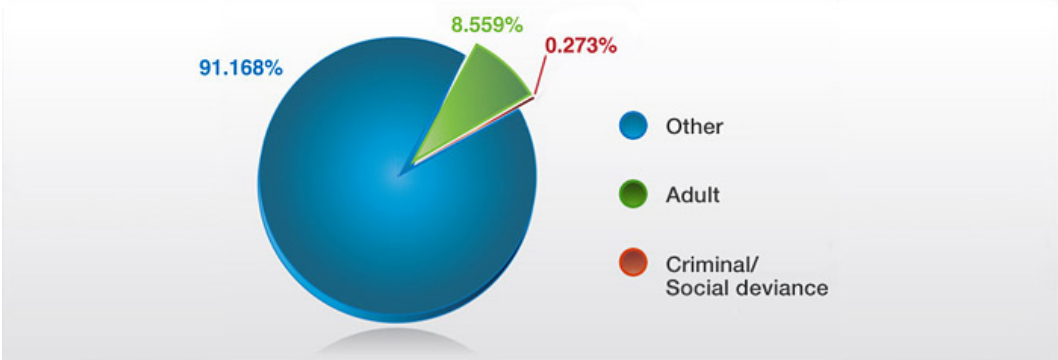
These e-mails often use subject lines or a return address that try to look like a real security alert from your bank or brokerage firm. Or, increasingly, they’ll try to link you to a Web site they’ve set up to look like a legitimate bank but which is actually a front for a criminal operation.

Delete | Spam | Mark | Move...

Subject line	Quota
<empty subject line>	22.21%
Account Security Measures!	3.86%
Important Notice-E*TRADE FINANCIAL Corp	3.21%
Important notice!	2.01%
Volksbanken Raiffeisenbanken AG: 02/11/2007	1.94%
Security Measures!	1.82%
Citibank Account Security!	1.77%

Distribution of Web content, late 2007

The other bane of many people’s experience online is all the undesirable content you can come across on the Web without even trying. There’s some good news to report in those trends, at least. In 2006, unwanted or undesirable content — such as pornography, criminal activity, or hate speech — accounted for one-eighth of all the content on the Web. But by the end of 2007, that number had dropped to less than a tenth.



Trends in cybercrime and online threats

IBM Internet Security Systems has noted a disturbing rise in the sophistication of attacks by criminals on Web browsers worldwide. By attacking the browsers of computer users, cybercriminals are now stealing the identities and controlling the computers of consumers at a rate never before seen on the Internet.

Underground brokers are delivering tools to aid in obfuscation, or camouflaging attacks on browsers, so cybercriminals can avoid detection by security software. In 2006, only a small percentage of attackers employed camouflaging techniques, but the rate of attacks using such camouflage tactics soared to 80 percent during the first half of 2007, and reached nearly 100 percent by the end of the year.

These and other trends were reported by the IBM Internet Security Systems X-Force team in their 2007 Trends Report. Download the report here.

IBM Corporation
New Orchard Road, Armonk, NY 10504