Shoppers fast out of gate, but slow at the turn

By Lorrie Grant
USA TODAY

Excitement on Friday as the holiday shopping season got underway cooled before the weekend's close as cautious shoppers browsed and let many deals pass.

About $13 billion was spent on Friday and Saturday, an overall 4% gain from last year's first Friday and Saturday, according to retail information firm ShopperTrak's final tally on Monday.

Retailing

The revenue gain, however, came on Friday — with $8 billion in sales, up 11% from the same day a year ago. The remaining $5 billion posted on Saturday was a 6.5% drop from the Saturday last year.

It could be just a blip. "One day is hard to judge. The decline could represent a shift in the timing of spending," says Ira Kalish of Deloitte Research.

But Saturday's weak sales proved that more retailers than Wal-Mart saw wary shoppers over the weekend.

Wal-Mart reported Saturday that very soft sales last week had forced it to cut projections for November sales growth to 0.7% from 2% to 4%. The retailer expressed disappointment with weekend sales, which some observers blamed on less promotion than last year. "A year ago, Wal-Mart broke incredible prices on consumer electronics, and this year they did not," says Britt Beemer, chairman of America's Research Group.

Wal-Mart spokeswoman Mona Williams said, "While our prices were generally as low as they have ever been, our competition was even more aggressive. We ... will move quickly to respond to what our customers have told us during the remainder of the shopping season."

Many investors moved quickly. Wal-Mart stock tumbled $2.17, nearly 4%, to end volatile trading of 23.7 million shares at $53.15.

Competition in electronics included aggressive pricing at Best Buy, Circuit City and Sears. A survey of a thousand shoppers by Beemer's research group over the weekend found 21% shopped at consumer electronics stores this year, up from 7% a year ago, while 30% went to discount stores, a drop from 41%.

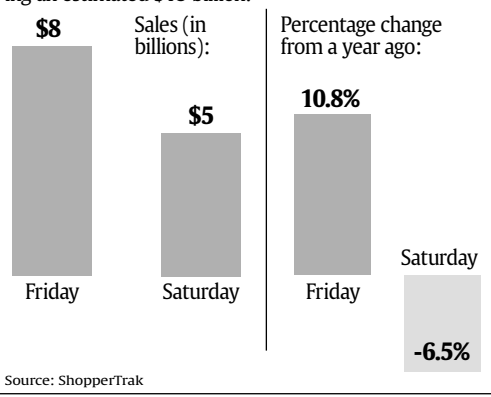
Last year also featured a brutal price war on toys among Toys R Us, Wal-Mart and Target, which has not been repeated this year. "Maybe more significantly, there was a lack of a positive traffic driver in the toy area where there appears to be no 'must have' item this year," says Todd Slater of Lazard Freres.

He and other analysts say caution and bargain hunting spread because consumers remain unconvinced that the economy is improving.

"When consumers are uncertain, they take a conservative approach," says Daniel Howard, marketing department chairman at Southern Methodist University's Cox School of Business. "It won't be reflected in not spending at all but in spending carefully. That is when, traditionally, discount stores have done well."

Holiday rush is on

Sales surged the two days after Thanksgiving, reaching an estimated $13 billion.



Source: ShopperTrak

By Adrienne Lewis, USA TODAY

Speedy computer chip for PlayStation near

By Michelle Kessler
USA TODAY

The superfast computer chip expected to power Sony's next-generation PlayStation video game system and other cutting-edge consumer electronics will be ready next year, Sony, IBM and Toshiba said Monday.

The three companies have been working on the chip, code-named Cell, since they signed a $400 million deal in 2001. They've said little about it since, causing speculation to soar in tech circles.

Monday, in promotional material for an upcoming chip conference, they broke their silence. IBM said it would start a pilot manufacturing program during the first half of next year. Although the chip was designed with PlayStation in mind, Sony and Toshiba said they expect to use the chips in other consumer products by 2006, including high-definition televisions and home entertainment servers.

Technology

The chip is expected to give the third PlayStation the ability to run games "that look like they were done in a Hollywood studio," says tech analyst Richard Doherty with researcher Envisioneering Group. Details are under wraps until February, but engineers are believed to be combining existing technology in a new way.

IBM has long made processors for Apple's Macintosh line of PCs. The new chips are expected to have four of these processors lashed together, Doherty says. That would give the system four "brains" that could handle four different tasks. In a football video game, for example, one chip could render the stadium, another two could create the players, and a fourth could track the ball. The chip's design is "very ambitious," says IBM spokesman Chris Andrews.

That's important, because video games are growing increasingly sophisticated. Future games will use artificial intelligence so characters can react to a player's moves, for example. "Gamers are one of the last niches where you can never have enough performance," says chip analyst Nathan Brookwood with semiconductor research firm Insight 64.

But gamers are also very price-sensitive, which limits the profit the new chips will generate. An Intel PC processor, for example, sells for $150 to $200, Brookwood says. A Cell chip will cost less than $100, he says.

The Cell chips are a blow to Microsoft, which is challenging PlayStation's dominance of the video game market. The Cell-powered version of PlayStation is expected in 2005 or 2006, and Microsoft is scrambling to answer with a new video game system of its own, says Dan Hsu, editor-in-chief of *Electronic Gaming Monthly*, a magazine for game enthusiasts.

Cell chips might pose a threat to Intel and Advanced Micro Devices, the two biggest PC processor makers. Their chips are often used for non-PC electronics. (Intel made an early Xbox processor, for example.) But Brookwood says the threat remains small because the chips are so specialized. Plus, the market for gaming chips is about one-tenth the size of the market for PC chips, he says.

Unprotected PCs can be hijacked in minutes

Automated cyberattacks saturate Net

By Byron Acohido and Jon Swartz
USA TODAY

SAN FRANCISCO — Surfing the Web has never been more risky.

Simply connecting to the Internet — and doing nothing else — exposes your PC to non-stop, automated break-in attempts by intruders looking to take control of your machine surreptitiously.

While most break-in tries fail, an unprotected PC can get hijacked within minutes of accessing the Internet. Once hijacked, it is likely to get grouped with other compromised PCs to dispense spam, conduct denial-of-service attacks or carry out identity-theft scams.

Technology

Those are key findings of a test conducted by USA TODAY and Avantgarde, a San Francisco tech marketing and design firm. The experiment involved monitoring six "honeypot" computers for two weeks — set up to see what kind of malicious traffic they would attract. Once breached, the test computers were shut down before they could be used to attack other PCs.

The test did not measure Web attacks that require user participation, namely spyware, which gets spread by visiting contagious Web sites, or e-mail viruses, which proliferate via e-mail attachments.

However, the results vividly illustrate how automated cyberattacks have come to saturate the Internet with malicious programs designed to take the quickest route to break into your PC: through security weaknesses in the PC operating system.

"It's a hostile environment out there," says tech security consultant Kevin Mitnick, who served five years in prison for breaking into corporate computer systems in the mid-1990s. "Attackers have become extremely indiscriminate."

Mitnick and Ryan Russell, an independent security researcher and author of *Hack Proofing Your Network*, were contracted by Avantgarde to set up and carry out the experiment.

Test results underscored the value of keeping up to date with security patches and using a firewall. Computer security experts say firewalls, which restrict online access to the guts of the PC operating system, represent a crucial first line of defense against cyberintruders. Yet, an estimated 67% of consumers do not use a firewall, according to the National Cyber Security Alliance.

The machines tested were types popular with home users and small businesses. They included: four Dell desktop PCs running different configurations of the Window XP operating system, an Apple Macintosh and a Microtel Linspire, which uses the Linux operating system.

Each PC was connected to the Internet via a broadband DSL connection and monitored for two weeks in September. Break-in attempts began immediately and continued at a constant and high level: an average of 341 per hour against the Windows XP machine with no firewall or recent security patches, 339 per hour against the Apple Macintosh and 61 per hour against the Windows Small Business Server. Each was sold without an activated firewall.

By contrast, there were fewer than four attacks per hour against the Windows XP updated with a basic firewall and recent patches (Service Pack 2), the Linspire with basic firewall and the Windows XP with ZoneAlarm firewall.

"The firewalls did their job," says Russell. "If you can't get to them, you can't attack them."

While attempted break-ins never ceased, successful compromises were limited to nine instances on the minimally protected Windows XP computer and a single break-in of the Windows Small Business Server. There were no successful compromises of the Macintosh, the Linspire or the two Windows XPs using firewalls. That pattern was not surprising, as Windows PCs make up 90% of the computers connected to the Internet, and the vast majority of automated attacks are designed to locate and exploit widely known Windows security weaknesses.

Intruders repeatedly compromised the Windows XP computer through the same two security holes used by the authors of the July 2003 MS Blaster worm and May's headline-grabbing Sasser worm, which overloaded computers in banks, hospitals and transportation systems worldwide.

To hijack the Windows Small Business Server, the attacker finagled his way into a function of the Windows operating system that allows file sharing between computers. He then uploaded a program that gave him full control.

On three occasions, intruders got as far as logging on to an Internet Relay Chat channel, signaling an intent to herd the compromised PC with other hijacked PCs to pursue illicit activities.

IRC channels work like a private instant-messaging service. An intruder in control of such a channel can send instructions to some PCs to spread spam, to others to serve up scamming Web sites, and to others to hijack more PCs.

"Downloading and using other exploits, performing denial-of-service attacks, running spam-relay tools, running identity-theft tools are all very common activities of compromised machines," says Martin Roesch, chief technology officer at tech security firm Sourcefire.

The intruder who cracked the Windows Small Business Server even uploaded a tool to prevent rival attackers from following behind him and gaining access to the system, says researcher Jon Orbeton, of anti-virus and firewall supplier ZoneLabs.

That level of sophistication shows how cyberintrusions are fast becoming an ingrained part of the Internet. Compromised PCs fueled a 150% surge in suspicious security activity per machine per day in the third quarter of this year, compared with a year ago, security vendor VeriSign said in a report in November.

The end game: illicit profits. Compromised PCs supply the computing power for cybercrooks to run increasingly diverse scams, including phishing schemes that lure victims into typing account information at counterfeit Web sites.

In the past month, the first phishing scam to plant a bogus Web link on a legitimate banking Web site surfaced. The scam was probably carried out with hijacked PCs to protect the perpetrator from detection. "It's the most sophisticated, and frightening, phishing scam we've seen," says Susan Larson, vice president of global content at SurfControl, an e-mail security firm.

By Alejandro Gonzalez, USA TODAY

Anatomy of a honeypot test

From Sept. 10 to Sept. 25, online intruders attempted to break in to six computers connected to the Internet via a broadband DSL connection 305,922 times. Attackers successfully compromised the Dell Windows XP with Service Pack 1 computer nine times and the Dell Windows 2003 Small Business Server once. No other PCs were breached.

	Total attacks	Attacks per day	Attacks per hour
Windows XP SP1	139,024	8,177	341
Apple Mac	138,647	8,155	339
Windows SBS	25,222	1,400	61
Windows XP SP2	1,386	82	3.4
Windows XP ZoneAlarm	848	50	2.1
Microtel Linspire	795	46	1.9

Source: USA TODAY research

By Marcy E. Mullins, USA TODAY

Analysis of a break-in

How intruders on Sept. 10 attacked a Dell desktop computer running the Windows XP operating system with Microsoft's Service Pack 1 (SP1), which lacked a basic firewall and recent security patches:

10:52:08 a.m. Less than four minutes from start of the test, an intruder breaks in through the vulnerability most famously exploited by last May's Sasser worm. Intruder's ensuing instructions get garbled.

11:03:30 a.m. Eleven minutes later, another intruder breaks in through the security hole exploited by the July 2003 MS Blaster worm. Ensuing instructions get garbled.

11:04:04 a.m. While the previous break-ins are still unfolding, another intruder, using a different attacking computer, breaks into XP SP1 through the Sasser hole. Ensuing instructions get garbled.

8:21:44 p.m. An intruder breaks in for the fourth time — using the MS Blaster hole. Things go smoothly. He begins uploading commands. He confirms the computer is connected to the Internet, then begins making repeated attempts to connect it to a server running an Internet Relay Chat channel, the equivalent of a private instant-messaging line.

8:22:49 p.m. The intruder successfully connects to the IRC channel, which is probably also running on a hijacked PC.

8:23:05 p.m. The intruder instructs the computer to navigate to a designated Web site, likely running on yet another hijacked PC. The compromised computer downloads a program, called ie.exe, from the Web site.

8:23:11 p.m. The hijacked PC begins scanning the Internet, poised to similarly hijack other PCs exhibiting the same unpatched security hole.

Sources: USA TODAY, Avantgarde

By Marcy E. Mullins, USA TODAY

Shore up your cyberdefenses on these three cyberfronts

If an online intruder has infiltrated your Windows PC, you may notice recurring slowdowns of e-mail and Web browsing, or you may notice nothing at all. PC users must shore up defenses on three fronts:

▸ **Operating system vulnerabilities.** Always use a personal firewall and keep security patches up to date.

As of early November, all new Windows XP PCs come with Service Pack 2, which includes a firewall and automatic patching.

Owners of Windows XP PCs purchased earlier than that should download Service Pack 2 from www.microsoft.com/athome/security/protect/default.aspx. Users of older versions of Windows can get security tips at that same Web site.

▸ **E-mail viruses.** Distrust all attachments. If you doubt it, delete it. Subscribe to anti-virus software, such as Norton AntiVirus, McAfee VirusScan or ZoneAlarm Security Suite. Keep the subscription current and set it to automatically check for updates.

▸ **Spyware.** Consider switching from Internet Explorer, a sieve for spyware, to the Mozilla Firefox browser or the Opera browser. Both are free and can be downloaded, respectively, from mozilla.org or opera.com.

If you continue using Explorer, set security settings to high and use anti-spyware software.

Sources: CERT Coordination Center, Microsoft