www.usatoday.com

USA TODAY

Money

SECTION B

Wednesday, September 8, 2004

IBM

IBM fellow: Stuart Parkin helped invent the technology behind what could become PLRs, or personal life recorders.

Technology

Your whole life on a tiny chip?

New kind of memory could make it so. Kevin Maney column, 5B

CONCENTRATED POWER. CONCENTRATED PRICE.

Save $150 instantly on the i830.

With built-in walkie-talkie, color screen and speakerphone. GPS-enabled. Slim enough to slip in your pocket.

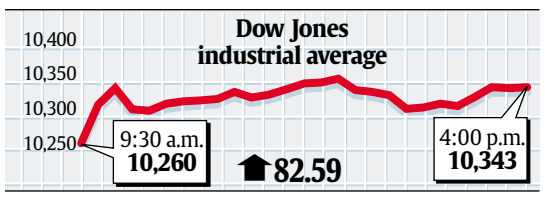
NEXTEL.COM / 800-NEXTEL9

NEXTEL. Done.

While supplies last. Final price of $249.99 is based on savings off the regular retail price of $399.99. Requires new activation and credit approval. $200 early termination fee applies, after 15-day trial period (conditions apply). Setup fee of $35 per phone, up to $70 max per account applies.

Moneyline

Tuesday markets



Index	Close		Change
Nasdaq composite	1858.56	▲	14.08
Standard & Poor's 500	1121.30	▲	7.67
Treasury bond, 30-year yield	5.01%	▼	0.05
Treasury note, 10-year yield	4.24%	▼	0.05
USA TODAY Internet 50	102.99	▲	0.78
e-Business 25	87.85	▲	0.72
e-Consumer 25	152.99	▲	0.95
Oil, light sweet crude, barrel	$43.31	▼	0.68
Euro (dollars per euro)	$1.2098	▲	0.0027
Yen per dollar	109.39	▼	1.21

Sources: USA TODAY research, MarketWatch.com

► **Market scoreboard with currencies, 6B**

GAO: Former Medicare chief should pay

Former Medicare administrator Thomas Scully should repay his government salary because of his efforts to keep a staff member from giving Congress higher estimates of the cost of a prescription drug plan, congressional investigators said Tuesday. The Government Accountability Office said federal law prohibits a federal agency from paying the salary of an official who prevents another federal employee from communicating with Congress. Bill Pierce, a Health and Human Services Department spokesman, said HHS will not ask Scully to return his salary. (Higher premiums for Medicare, 2B.)

United flight attendants call for trustee

The labor group representing United Airlines flight attendants joined another union in asking a judge to appoint a trustee to oversee the airline's bankruptcy restructuring. The Association of Flight Attendants said late Tuesday that it had filed a motion in bankruptcy court to join the International Association of Machinists and Aerospace Workers in a request that Chief Executive Glenn Tilton be replaced. The unions say United executives have lost employees' trust. United spokeswoman Jean Medina told the Associated Press: "Baseless legal filings by the AFA and IAM will not solve the complex issues facing United."

Wal-Mart CEO leads 'New Establishment'

Lee Scott, CEO of top retailer Wal-Mart Stores, vaulted to the top of *Vanity Fair*'s "New Establishment" in the magazine's 10th annual list, out today. Scott, No. 9 on last year's list, was cited for maintaining the "folksy homespun image inspired by Wal-Mart's founder Sam Walton, creating jobs and bringing low-cost goods to people who need them most." **... The Delahaye Index**, which assesses how favorably the media cover certain U.S. companies, ranked Microsoft No. 1 in positive news for the second quarter. Coverage of revenue growth and product development helped the software giant beat No. 2 Walt Disney.

Viacom merges West Coast TV groups

Viacom shook up its West Coast TV programming operations Tuesday, merging CBS Productions and Paramount Network Television and moving half a dozen executives into new posts. In the biggest move, Nancy Tellem was promoted to president of CBS Paramount Television Entertainment Group. Tellem had overseen development of CBS shows *CSI: Crime Scene Investigation*, *Survivor* and *Two and a Half Men*.

Briefly ...

Luxury retailer **Neiman Marcus** said net income hit a record $21 million, or 42 cents a diluted share, for its fourth quarter ended July 31, up 200% from $7 million, or 15 cents, a year ago. **...** **Primus Telecommunications** has agreed to pay $400,000 to settle claims by the Federal Communications Commission that it made telemarketing calls to customers on the National Do Not Call Registry. **...** Troubled rehabilitation chain **HealthSouth** named John Workman its chief financial officer. Workman, 53, most recently was CEO of U.S. Can.

Mutual fund data problem

Due to systems problems at Lipper, which provides mutual fund data to the Associated Press, the year-to-date percentage change (YTD%) column in the mutual fund tables shows the change for the year as of Friday.

Airlines: US Airways still has hope

But it needs a deal with pilots to avoid a second bankruptcy filing, possibly as soon as the end of this month. 2B

Media: FCC to fine Viacom

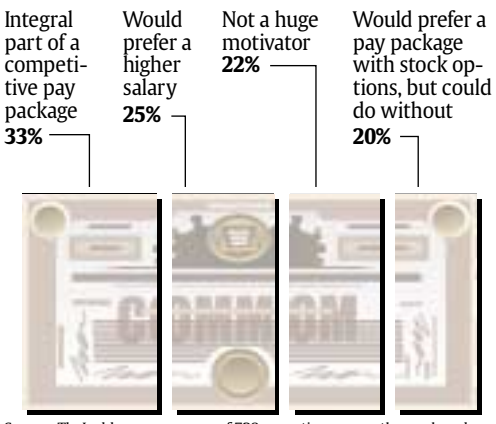
Super Bowl wardrobe malfunction is expected to draw record penalty for CBS parent. 5B

Compiled from staff and wire reports

USA TODAY .com Get business news and market data updated 24 hours a day, 7 days a week at money.usatoday.com

USA TODAY Snapshots

Workers' views of stock options



Source: TheLadders.com survey of 728 executives currently employed or searching for employment. Margin of error ±4 percentage points.

By Darryl Haralson and Bob Laird, USA TODAY

Special report: PCs under attack — Part 1

By Andy Rogers for USA TODAY

Hooked by "phishing": Heather Hall clicked on a link in an e-mail that she thought came from her bank. After an authentic-looking Web page opened, she entered personal information. Bogus charges soon appeared on her bank statement.

Are hackers using your PC to spew spam and steal?

Crooks turn profit with 'zombie' PCs

By Byron Acohido and Jon Swartz
USA TODAY

Betty Carty figured she ought to be in the digital fast lane.

Last Christmas, Carty purchased a Dell desktop computer, then signed up for a Comcast high-speed Internet connection. But her new Windows XP machine crashed frequently and would only plod across the Internet.

Dell was no help. The PC maker insisted — correctly — that Carty's hardware worked fine.

But in June, Comcast curtailed Carty's outbound e-mail privileges after pinpointing her PC as a major source of e-mail spam. An intruder had turned Carty's PC into a "zombie," spreading as many as 70,000 pieces of e-mail spam a day.

The soft-spoken Carty, 54, a grandmother of three from southern New Jersey, was flabbergasted. "Someone had broken into my computer," she says.

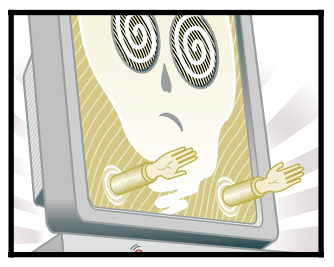
Since early 2003, wave after wave of infectious programs have begun to saturate the Internet, causing the number of PCs hijacked by hackers and turned into so-called zombies to soar into the millions — mostly in homes like Carty's, at small businesses and on college campuses. And, much like zombies of voodoo legend, they mindlessly do the bidding of their masters and help commit crimes online.

Personal computers have never been more powerful — and dangerous. Just as millions of Americans are buying new PCs and signing up for ultrafast Internet connections, cybercrooks are stepping up schemes to take control of their machines — and most consumers don't have a clue.

"We thought things were bad in 2003, but we've seen a sharp uptick in 2004. I'm worried things will get much worse," says Ed Skoudis, co-founder of consulting firm Intelguardians.

Carty's PC could have been taken over

Please see SPECIAL REPORT on 4B ►



► How cybercriminals turn PCs into zombies, graphic 3B

Coming Thursday

Fighting back

► Consumers on their own as tech firms scramble for defense.

USA TODAY .com What happens when a virus attacks? Get an animated look at tech.usatoday.com

Army might split Halliburton contract

Pieces of support orders could be put up for bid

By James Cox
USA TODAY

Halliburton's massive U.S. Army contract to provide food, housing and other support to troops in Iraq and Afghanistan might be split into smaller pieces and put up for bid, Army officials say.

The company and its KBR logistics unit have faced accusations they have overcharged for meals, fuel and other supplies. Halliburton has been a lightning rod for Bush administration foes who question whether the company has benefited from its connection to Vice President Cheney, its CEO from 1995 to 2000.

Halliburton's Army logistics contract took effect in 2001. To date, the company has been given orders for $7.1 billion in work and has been paid $4.5 billion.

The shift to smaller awards was reported Tuesday in *The Wall Street Journal*, which said the Army is frustrated about billing disputes and might impose its own cost estimates where it can't reach agreement with Halliburton.

Dan Carlson, spokesman for the Army

► U.S. deaths hit 1,000, 1A; more Iraq coverage, 5A, 11A

Field Support Command, says the move to smaller contracts would be "a normal part of the process" with no connection to billing problems.

The Army is considering the switch because the nature of logistics support in Iraq and Afghanistan has shifted from war preparation and combat to sustaining a longer-term presence of U.S. forces, he says, adding that Halliburton is "performing adequately."

Dan Briody, author of a book on the company, *The Halliburton Agenda*, says the decision "reflects the amount of political pressure and the amount of unhappiness the Army has experienced, given the auditing problems and the overcharging problems."

Halliburton spokeswoman Wendy Hall says such a characterization is "false and misleading." The company might bid on the smaller contracts, she says.

A switch to smaller components is "incredibly short-sighted," says Steven Schooner, a government procurement expert at George Washington University.

"The beauty of (KBR's) contract isn't that we were able to save a few pennies. It's that ... our troops were better fed, had better shelter, more showers, cleaner laundry and higher-quality water. All these things allow you to fight better and more quickly."

$451.5M paid in fund scandal

Invesco, AIM settle with state, federal officials

By John Waggoner
and Christine Dugas
USA TODAY

In the third-largest settlement to date in the mutual fund trading scandal, Invesco Funds Group and AIM Advisors announced a $451.5 million deal with state and federal regulators Tuesday.

The two fund companies, subsidiaries of London-based Amvescap, will pay $235 million in restitution to investors, $140 million in civil penalties and $75 million in reduced fees the next five years. Another $1.5 million will pay for attorney fees, investor education and future enforcement activities.

In contrast, Bank of America and Fleet, now merged, paid combined penalties and fee reductions of $675 million. Alliance Capital paid $600 million.

Invesco bore the brunt of the restitution and penalties, paying all but $50 million.

AIM and Invesco made the agreement in principle with the Securities and Exchange Commission and the state attorneys general of New York and Colorado.

Invesco had more than 40 arrangements with big customers, letting them dart in and out of its funds — a practice called market timing. That's not illegal, but Invesco's prospectus forbids market timing. If you do that, you can't make exceptions for big clients.

Invesco's exceptions were called Special Situations. They were not disclosed to investors or the independent members of the boards of the funds, the SEC alleged.

Market timing increases costs and dilutes gains of other investors.

"I believe this sends the strongest message yet that mutual fund companies will be held accountable for behavior that harms consumers and average shareholders," said Colorado Attorney General Ken Salazar.

"The size of the settlement is a reflection of the wrongdoing," said New York Attorney General Eliot Spitzer. He said his staff determines the amount of the restitution based on how much the market timing dilutes shareholder gains.

"The dilution was very big because of the volume of Special Situations that they permitted," Spitzer said. "Our first goal is to make investors whole, and second, we want to impose a fine to say, 'You can't get away with this.' "

AIM funds also had market-timing agreements, but far fewer than Invesco.

This action puts the total of negotiated settlements since the mutual fund scandal erupted in September 2003 at more than $3 billion. "That's $3 billion that will ultimately wind its way back to investors," Spitzer said.

A notice on the AIM funds' Internet site said: "We deeply regret the harm done to fund investors and have taken strong steps to prevent any recurrence of problems."

The companies also said they would add a 2% redemption fee to the funds most vulnerable to market timing.

Storms' one-two punch stuns Florida; will USA wobble?

By Barbara Hagenbaugh and Sue Kirchhoff
USA TODAY

Florida's economy will likely be hurt in the near term by the recent hurricanes, but it's unclear whether the national economy will be noticeably affected.

The holiday weekend arrival of Hurricane Frances was bad timing. That will make it more difficult to offset the economic losses through rebuilding, as occurs in the aftermath of many major storms.

The economy

Businesses, particularly those in the tourism and retail industries, lost money over the key Labor Day weekend as visitors canceled trips and residents hunkered down to wait out the storm. Tuesday, many businesses were still closed for lack of electricity.

Sales of batteries, canned goods and other emergency items rose before the storm but probably will not make up for the losses, such as lost ticket sales at Disney World, that piled up over the weekend and are unlikely to be recovered. Plus, with Florida already reeling from Hurricane Charley last month, Frances likely had a bigger impact than a single event would have, because some areas were battered twice.

"There's a combo effect," says Scott Brown of Raymond James & Associates in St. Petersburg, Fla.

By Richard Graulich, *The Palm Beach* (Fla.) *Post* via AP

Floating grapefruit: Crop damage in Florida.

► More hurricane coverage, 3A, 5B

All but one guest booked at the 10-bedroom Ash Street Inn in Amelia Island, Fla., canceled over the weekend, traditionally one of the busiest of the year, says owner Sam Chi. Those cancellations came after a mass of no-shows during Hurricane Charley. "It's a pretty devastating loss for us," Chi says.

Early, computer-based estimates on insured losses from Hurricane Frances range from $3 billion to $6 billion. Frances clobbered a wider geographic area than Charley and could produce more individual claims, says John Eager of Property Casualty Insurance Association of America. Insurers are expected to pay about $6.8 billion in insured property losses as a result of Hurricane Charley, making it the second-costliest hurricane in U.S. history, according to the Insurance Information Institute.

In the long run, hurricane-related construction spending will likely help make up for a large portion of the losses. But businesses are now keeping an eye on Hurricane Ivan, which was sweeping through the Caribbean on Tuesday and threatened further damage.

Nationwide, prices for some products, particularly citrus fruits and building materials, will likely rise.

Florida's position as the fourth-largest state economy in the USA might also point to a more widespread impact. But economists at Wachovia note that before the storms, Florida had one of the strongest economies in the country, putting it in a better position.

Contributing: Christine Dugas

Special report: PCs under attack

The rise of zombie computers

The Internet empowers 570 million personal computer (PC) users to exchange e-mail, browse Web sites and share files. But intruders have become highly proficient at turning Internet-connected Windows PCs into obedient "zombies." Computers using Apple or Linux operating systems make up less than 10% of the market and have generally not been attacked.

Three paths to hijack a PC

1 Sneaky path: Web browser contagions

On popular Web sites, intruders plant backdoor Trojan horses to gain full control of a PC, and spyware that tracks what the victim does on the Internet. Typically, the victim merely clicks on the Web site to get infected.

One type of spyware, called a keystroke logger, keeps track of when the user types account information on banking and e-commerce sites, then transmits that data to another zombie.

TIP: *Worms scan the Internet for PCs exhibiting Windows security holes. Enable Windows Auto-Update to automatically download the latest security patches.*

3 Scary path: Network worms

PCs often get turned into zombies with no action taken on the part of the PC owner. Malicious programs, called worms and bots, do the dirty work by continually scanning the Internet for Windows PCs exhibiting Windows security holes. Windows is riddled with such vulnerabilities. New ones turn up constantly. Once a month, Microsoft issues patches for the most worrisome. But consumers and businesses are slow to install patches.

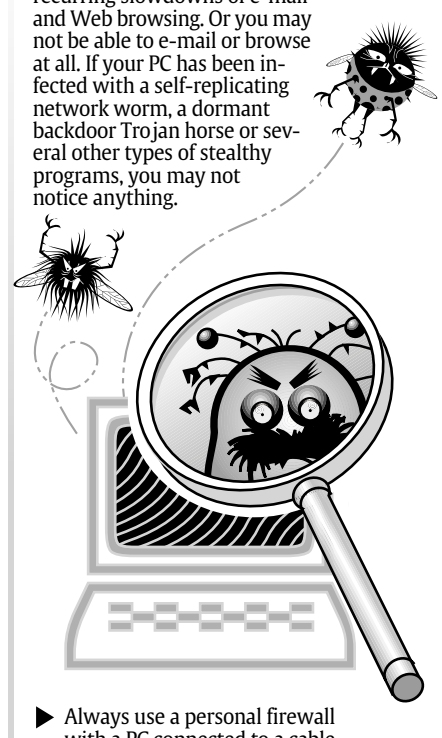
2 Easy path: E-mail viruses

E-mail messages that seduce the recipient into opening a viral attachment represent a tried-and-true way to slip malicious code past firewalls and anti-virus defenses. A recent variant of the MyDoom e-mail virus arrived in the victim's inbox with the subject line "undeliverable."

By clicking on an attached folder labeled with the PC user's own e-mail address, the victim unleashed code that planted a backdoor Trojan horse, giving the intruder full control of the PC. As with many other e-mail viruses, MyDoom also automatically e-mails copies of itself to any e-mail addresses found on the victim's hard drive.

Is your PC infected?

If your Windows PC is being used as a zombie, you may notice recurring slowdowns of e-mail and Web browsing. Or you may not be able to e-mail or browse at all. If your PC has been infected with a self-replicating network worm, a dormant backdoor Trojan horse or several other types of stealthy programs, you may not notice anything.



- Always use a personal firewall with a PC connected to a cable modem, DSL or wireless Internet service. Free ones are listed on http://www.free-firewall.org.

  TIP: *Have the personal firewall set to at least the medium level of security.*

- Buy anti-virus software, such as Norton AntiVirus, McAfee VirusScan or ZoneLabs Security Suite, and keep the subscription current. Set it to automatically check for updates.

  TIP: *New PCs typically come with a free trial subscription from Norton or McAfee. However, you must subscribe after the trial period expires to continue getting updates.*

- Enable Microsoft Windows Auto-Update to automatically download the latest security patches.

  TIP: *Follow instructions to make sure downloaded patches are also automatically installed.*

- No software vendor will ever send you patches via e-mail. If you get e-mail pretending to be a patch from Microsoft or any other vendor, delete it. Distrust all attachments. If you have even the slightest doubt, delete it without reading.

- Back up all of your important documents and folders at least once a month, more often if you can stand it. Use complex passwords and periodically change passwords and PINs.

- Beware of spyware. If you can, use the Mozilla Firefox browser. If you must use Internet Explorer (IE), set the security settings to high; this will disable multimedia features of many Web sites, but also will block a main path intruders use to plant Web contagions. And use Lavasoft's Ad-Aware or Spybot Search & Destroy anti-spyware programs.

  TIP: *Be extremely wary of counterfeit versions of Lavasoft's Ad-Aware, spelled slightly differently, that are actually spyware.*

  TIP: *To set IE security to high, navigate to tools, Internet options, security settings.*

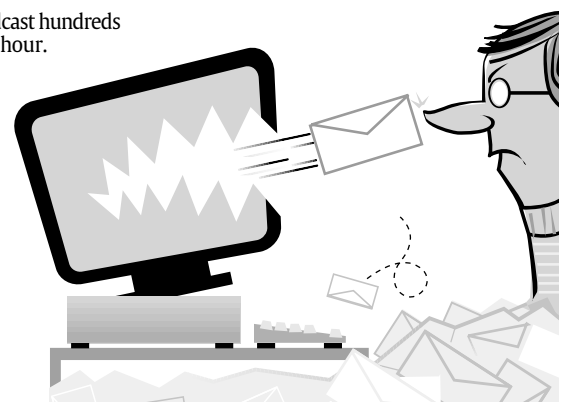
The many uses of zombie PCs

Criminals deploy zombies herded into networks of a few hundred to more than half a million compromised PCs. **Some of the nefarious activity:**

Spread spam:

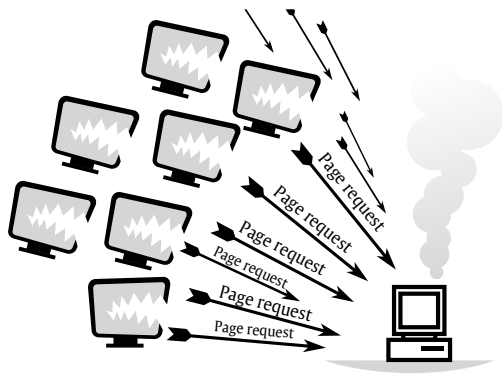
Each zombie can broadcast hundreds of pieces of spam per hour.

(A detailed how-to appears to the right)



Denial-of-service attack

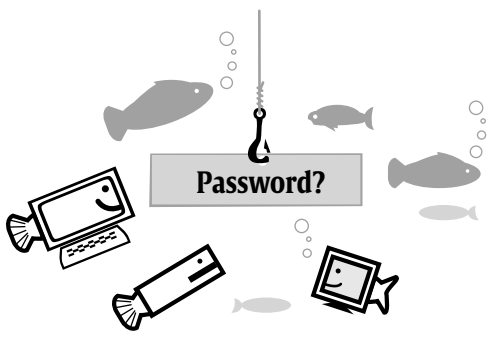
Zombie networks can be directed to swamp a targeted Web site with junk data, crippling the site. Crooks are increasingly using the threat of a denial-of-service attack to extort cash from online businesses keen to stay up and running.



Phishing scams

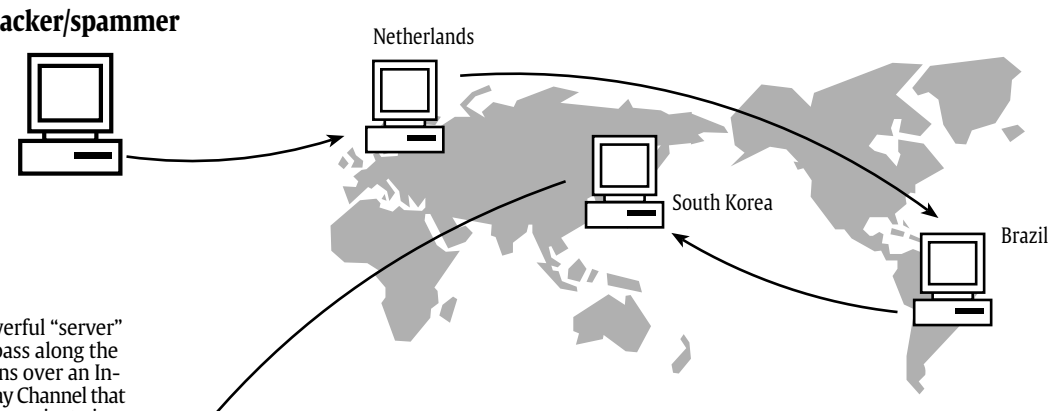
Phishing scams trick people into typing account information on counterfeit Web sites. Zombies broadcast phishing spam; they also host the bogus Web sites that collect the stolen data.

Do-it-yourself phishing kits now supply free spamming tools and bogus Web sites targeting popular online banks and merchants.



How a zombie network spreads spam

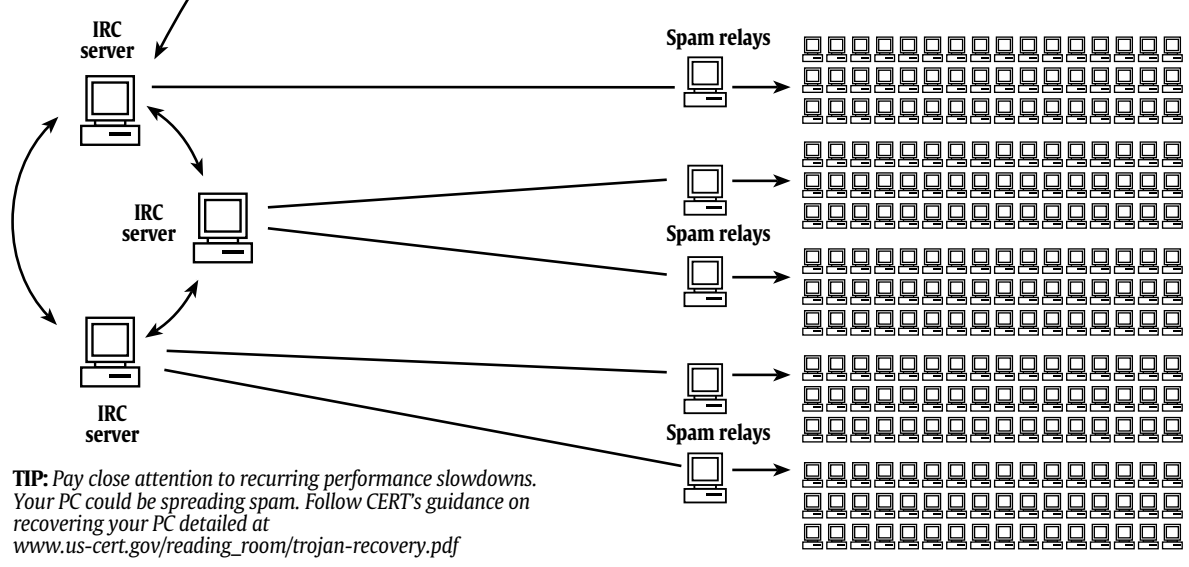
1 The spammer sends instructions for the attack to stepping-stone zombies scattered in different countries and time zones.



2 More powerful "server" zombies pass along the instructions over an Internet Relay Channel that works like a private instant-messaging service.

3 Spam-relay zombies take the instructions, using the equivalent of a buddy list.

4 Each spam-relay zombie blasts out spam to hundreds of e-mail addresses.



TIP: *Pay close attention to recurring performance slowdowns. Your PC could be spreading spam. Follow CERT's guidance on recovering your PC detailed at www.us-cert.gov/reading_room/trojan-recovery.pdf*

Sources: CERT Coordination Center, Microsoft, Gartner, University of Washington Center for Information Assurance and Cybersecurity

Researched by Byron Acohido and Jon Swartz; graphic by Dave Merrill; zombie icon by Sam Ward

Special report: PCs under attack — Part 1

Hackers blackmail some Web site owners

Continued from 1B

in myriad ways. She could have been fooled into opening a virus-infected e-mail. She might have innocently surfed to a Web page bristling with contagious code. Or she may have done nothing at all. One of dozens of network worms, voracious, self-replicating programs that pinball around the Web searching for security holes in Windows PCs, may have found one on her new PC.

Profitable attacks

Cyberintrusions traditionally have been the domain of socially inept males launching electronic attacks for fun and bragging rights, often creating a huge, if transient, nuisance for companies and consumers. But things are changing: More PCs are being taken over purely for profit.

Over the past eight months, USA TODAY interviewed more than 100 tech-industry executives, consultants, analysts, regulators and security experts who say top-tier code writers now create malicious programs mainly to amass networks of zombie PCs. They then sell access to zombie networks to spammers, blackmailers and identity thieves who orchestrate fraudulent for-profit schemes.

Most consumers are slow to grasp that an intruder has usurped control of their PC. "We have a large population that is easily tricked," says Dave Dittrich, senior security engineer at the University of Washington's Center for Information Assurance and Cybersecurity.

One measure of the swelling tide of zombie PCs: E-mail spam continues to skyrocket, with zombies driving the increase. In July, spam made up 94.5% of e-mail traffic, nearly double from a year before, says e-mail management firm MessageLabs. Postini, another big e-mail handler, estimates nearly 40% of spam now comes from zombie networks.

Using zombies to broadcast spam for Viagra or quickie loans has emerged as a huge business. Yet spreading ordinary spam is actually one of a compromised computer's more benign tasks. Bigger spoils lie in using zombies in elaborate phishing scams, in which e-mail directs consumers to bogus Web pages to trick them into surrendering personal information.

And zombie networks are perfectly suited to flood targeted Web sites with data requests, in so-called distributed denial-of-service, or DDoS, attacks. Cybercrooks use the threat of a DDoS attack to extort protection money from businesses keen to keep their Web sites running.

Few laws, few arrests

Until recently, little has been done to stop such attacks. The Justice Department's Operation Web Snare netted 160 arrests in August that could lead to more busts, offering encouraging news to cybersecurity experts who have criticized law enforcement for not doing enough. Still, detractors point out there are few federal cybersecurity laws with stiff penalties.

Federal, state and local law enforcement officials face daunting jurisdictional hurdles trying to corner, much less extradite, suspects. Chasing bad guys equipped to commit virtual crimes in several countries simultaneously has proved problematic, as has the sheer volume of incidents.

"It's easier trying to catch Osama bin Laden," says Steve Jillings, CEO of e-mail security firm FrontBridge Technologies.

Zombie victim Carty took matters into her own hands: She did research on how to clean up and protect her PC and diligently updates programs that scan her computer for various types of malicious code. Her PC now runs clean. "I had no clue at Christmas that I would become a security expert," she says.

Consumers remain seduced by the Internet's convenience. E-commerce is bigger than ever, and most casual computer users overlook safety practices. The vast majority don't use firewall software to block intruders, patch vulnerabilities or keep anti-virus subscriptions current.

"Consumers seem almost bizarrely unconcerned by security in general," says James Governor, founder of research firm RedMonk. "People will practically give out their Social Security number as easily as their phone number."

Low and slow thievery

Heather Hall can trace the start of her online banking nightmare to the day she received what she thought was a legitimate e-mail request from Bank of America asking her to click a link to a bank Web page. The 27-year-old health services worker typed in her login, password and account number.

Not long afterward, Hall noticed an unauthorized withdrawal on her banking statement for $6.50. The withdrawals increased in frequency and amounts, to as much as $108. Hall was the victim of a "low and slow" phishing scam, in which cybercriminals purposely steal small amounts of cash — sometimes as little as 20 cents at a time — to avoid detection.

Though data are scarce, experts estimate millions of dollars are being skimmed from thousands of online banking accounts. About 23.6 million people had online accounts at the nation's top 10 banks in the second quarter of 2004, up 28% from the year before, says ComScore Networks.

Sneaky cybercrooks are finding it profitable to "be patient and nick an account for a long time," says Dan Larkin, unit chief of the FBI's Internet Crime Complaint Center.

Bank of America agreed to reimburse the money stolen from Hall's account, but only after she badgered them. "They wanted me to believe it was my fault," says Hall.

Bank of America does not comment on specific cases. It reimburses victims of fraud and changes their online name and password, spokeswoman Betty Riess says.

First seen more than a year ago, phishing scams begin with e-mail messages broadcast to potential victims. The e-mail directs them, often under the guise of doing a security check, to a bogus Web page with the identical look and feel of an authentic page.

A network of zombie PCs e-mails the original request to tens of thousands of potential dupes. A separate zombie, usually a more powerful PC, often sitting in a remote country, perhaps in an obscure nook at a university, serves up the counterfeit Web page. Another zombie, in yet another country, perhaps in the basement of a small shop, stores the stolen account details and conducts the theft.

"Computer networks make this easy to do since they form a virtual world in which footprints and fingerprints are easily erased at a distance," says the University of Washington's Dittrich.

Experts say clues point to loosely organized crime syndicates, probably in Russia, Latvia, Kazakhstan and China, coordinating phishing scams with other schemes to quickly turn stolen account information into tangible booty. In what feds call one of the biggest phishing busts, a Romanian man was arrested last year and convicted for using an elaborate network of bogus Web pages and escrow accounts to fleece Americans out of $500,000.

Typically, filched financial information, such as credit card numbers, is sold on Web sites. Buyers often use card numbers to make long-distance phone calls, sign up for pornographic sites and buy computers over the Internet.

Unique phishing attacks have surged more than 10 times since January, to 1,974 in July, and show no sign of slowing. In early August, MessageLabs intercepted more than 125,000 phishing e-mails containing links to a replica of a well-known U.S. bank's Web site within the first five hours of its appearance.

U.S. banks are in a delicate position. Their customers lost an estimated $2.4 billion from phishing in the 12 months ending in April, according to market researcher Gartner. Citibank, a frequent target, warned users of a dozen examples of phishing solicitations on its Web sites in the first half of June.

Few, however, are willing to discuss such matters in detail out of fear of scaring customers and undercutting trust in online banking, in which they've invested hundreds of millions of dollars, says John Pironti, a security consultant at Unisys.

Now, free, do-it-yourself phishing kits are surfacing on the Internet. Would-be cybercrooks can choose from a dozen kits containing bogus Web sites, programming code and spam tailored toward customers of Citibank, eBay and PayPal, says analyst Chris Kraft of security firm Sophos.

The same zombie network used in phishing scams can also bombard a Web site with data requests. When that happens, no one else can get to the targeted Web site, effectively shutting it down.

Such an assault is known as a distributed denial-of-service, or DDoS, attack. Cybercrooks threaten DDoS attacks just as racketeers wave truncheons. Last January, a series of such attacks began against major Internet gambling operators in the United Kingdom. The attacks were preceded with e-mail messages demanding $10,000 to $40,000.

Some operators paid — and were immediately attacked again, according to a report from the Association of Remote Gambling Operators. The blackmail attempts continue. LadbrokesCasino.com, one of the UK's largest online gambling Web sites, recently reported coming under attack from 518,000 zombie computers.

New methods of attack

Seattle screenwriter Alex Tobias figured her laptop was immune to attacks. After all, she and her husband, Martin, a venture capitalist, worked from home a lot. To protect their home network, Martin installed top-notch firewall and anti-virus software.

Yet last fall, Alex's laptop slowed until she couldn't use e-mail or the Internet. It took extensive troubleshooting to determine that it had been turned into a spam-spreading zombie, and it took half a day to clean it up. "I don't know what she got or how she got it," says Martin. "The bottom line is she got it."

Their experience underscores the notion that there are many ways for malicious code to slip past firewalls and anti-virus programs. E-mail viruses, for instance, rely on tricking the victim into opening an infectious attachment. Another widely used tool is harder to fight: direct planting of contagions, known as "come-and-get-it" viruses, on popular Web sites.

Such contagions commonly lurk on peer-to-peer sites, where music and movies are exchanged. They trick the computer user into giving up personal information, and they can activate other invasive programs unseen by the PC owner.

Web contagions are turning up on high-traffic Web pages across the Internet. Most do the basics: plant a back-door Trojan horse and turn over full control to an intruder who might be sitting half a globe away.

Some have begun implanting spyware called keystroke loggers, which are designed to notice whenever the PC user types anything that looks like account information. It grabs the information and sends it to a zombie computer for storage and risk-free access by the crooks.

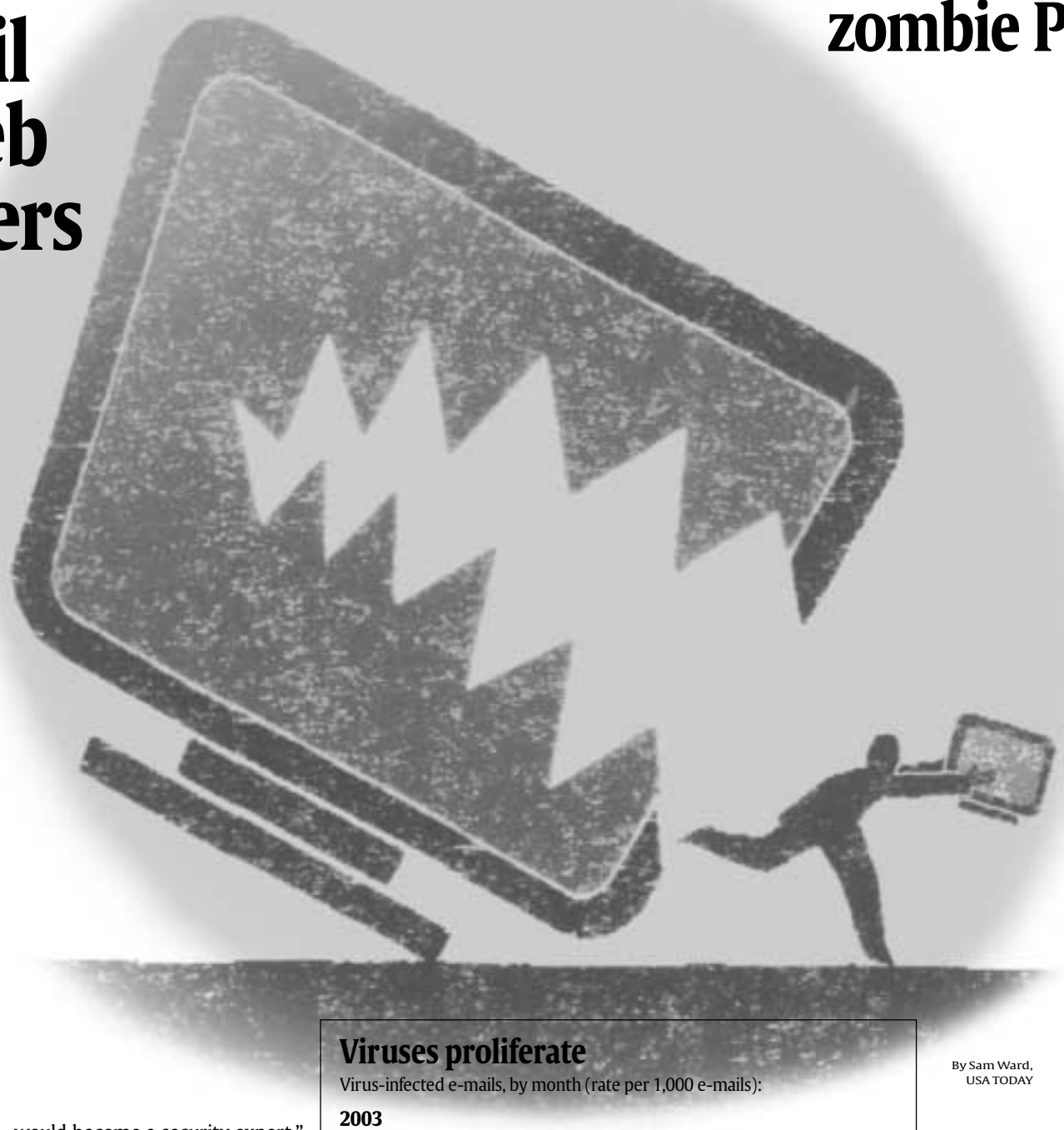
The scariest type of attack is one most consumers aren't aware of. Scores of sophisticated programs, called worms and bots, continually scour the Internet for Windows PCs with security holes. There are hundreds of Windows vulnerabilities, and new ones turn up regularly. Microsoft issues software patches, or fixes, each month for the most troublesome. But most home users, and many businesses, don't keep up to date on patches.

Consumer outrage needed

Not long ago, securing the Internet meant cleaning up after so-called script kiddies, youths who use pre-written malicious code, available free on the Web, to pull digital pranks. But security has metastasized into an almost fatalistic endeavor. "Hackers can do almost anything with a compromised PC, and there isn't much we can do about it," says Keith Lourdeau, deputy assistant director of the FBI's Cyber Division.

That will change only as tech suppliers who profit from the Internet simplify networks and collaborate on implementing universal security standards that may run counter to their current business strategies. Many experts say such a shift is at least five years away. The one thing that could make tech suppliers move more quickly is consumer outrage.

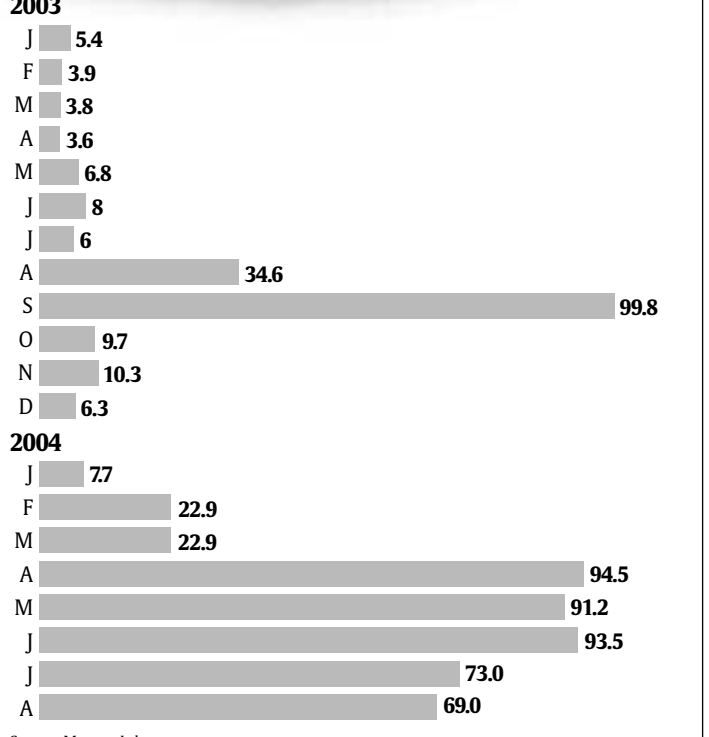
"Consumers should demand what they do of other utilities," says Kip McClanahan, CEO of security firm Tipping Point. "When I pay my water bill, I expect my water to be drinkable out of the tap. Today, when you pay your Internet bill, the data you get is not consumable."



By Sam Ward, USA TODAY

Viruses proliferate

Virus-infected e-mails, by month (rate per 1,000 e-mails):



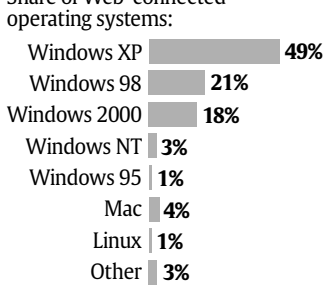
Source: MessageLabs

Number of computers worldwide connected to the Internet
(in millions)

Homes	240
Small firms	102
Midsize-to large companies	148
Government agencies	33
Schools	47

Source: IDC
Note: Figures are 2004 global estimates

Intruders mainly attack ubiquitous Windows PCs
Share of Web-connected operating systems:



Source: Google Zeitgeist

By Karl Gelles, USA TODAY

Going price for network of zombie PCs: $2,000-$3,000

By Byron Acohido and Jon Swartz
USA TODAY

In the calculus of Internet crime, two of the most sought-after commodities are zombie PCs and valid e-mail addresses.

One indication of the going rate for zombie PCs comes from a June 11 posting on SpecialHam.com, an electronic forum for spammers. The asking price for use of a network of 20,000 zombie PCs: $2,000 to $3,000. Such networks typically are used to broadcast spam and phishing scams and to spread e-mail viruses designed mainly to create yet more zombies.

Zombie networks can be sophisticated. Last fall, a small Internet service provider asked cybersleuth Don Bowman to find out which of its 70,000 subscribers were broadcasting spam. Its network was generating so much spam, other ISPs threatened to blacklist it.

Bowman discovered that e-mail would blast from 20 PCs for a brief period. After a pause, another fire-hydrant-like surge gushed from a different group of 20 PCs. On average, each machine disgorged 630 pieces of e-mail an hour. "It wasn't natural," says Bowman, chief software architect for security firm Sandvine. "No one can type that fast."

His conclusion: An intruder was deploying squads of zombies in rotating waves. Why? Probably so the unwitting zombie owner would tolerate performance slowdowns that came and went — and investigate no further.

To put a zombie network to work, an attacker needs a list of targets in the form of e-mail addresses. Lists can be purchased from specialists who "harvest" anything that looks like an e-mail address from Web sites, news groups, chat rooms and subscriber lists. Compiled on CDs, such lists cost as little as $5 per million e-mail addresses. But you get what you pay for: Many CD entries tend to be either obsolete or "spam traps" — addresses seeded across the Internet by spam-filtering companies to identify, and block, spammers.

Valid e-mail addresses command a steep price. In June, authorities arrested a 24-year-old America Online engineer, Jason Smathers, and charged him with stealing 92 million AOL customer screen names and selling them to a spammer for $100,000.

Recent e-mail viruses have begun probing for new ways to flush out valid e-mail addresses from search sites such as Google and Lycos.

Gain in polls gives stocks 'Bush bounce,' but it may not last

By Adam Shell
USA TODAY

NEW YORK — A big post-convention bounce in the polls for President Bush could add up to a bullish bump for the stock market.

Markets Stocks, which have struggled most of the year, partly because of uncertainty caused by the neck-and-neck race between Bush and Sen. John Kerry, enjoyed solid gains Tuesday. Some analysts said the Dow Jones industrial average's 83-point gain to 10,343 was sparked by polls showing Bush, benefiting from the momentum of last week's Republican convention, has extended his lead.

Stocks have moved upward since late July, at the same time the Kerry campaign, under attack from critics, lost traction after the Democratic convention.

A USA TODAY/CNN/Gallup Poll taken Friday through Sunday showed Bush had stretched his lead from 2 percentage points to 7 points. Other polls showed an even wider margin for Bush.

While some traders say it is too early in the campaign to guarantee a Bush victory, they predict stocks will likely fare better if Bush can cement his status as front-runner. "There is no doubt the Wall Street heavyweights want Bush to win," says Don Straszheim, founder of Straszheim Global Advisors, an independent research firm. Working in Bush's favor:

Bush's poll results vs. Dow's close

Bush margin[1]	Dow close
Tuesday +7	10,343
Aug. 27 +2	10,195
July 23 -1	9962

1 — In percentage points
Source: USA TODAY research

▶ **Friends in the trading pits.** Wall Street is predominantly conservative when it comes to economic theory, which makes Bush's stance on economic issues, such as his belief in lower taxes and less government interference, more palatable to investors than Kerry's views.

▶ **Historically, stocks do better when the incumbent wins.** Why? "There's less uncertainty about what the president will do and will not do," says Bruce Bittles, chief investment strategist at R.W. Baird.

For example, investors know that if Bush is re-elected, he will push to make permanent the tax reductions on dividends, capital gains and payrolls that he successfully passed in 2003. In contrast, Kerry favors repealing those cuts.

▶ **A so-so economy.** The economy, which hasn't been creating nearly enough jobs to make the voting public happy, also hasn't been putrid enough to anger voters and make the economy "the" issue in the campaign. That's a plus for Bush, because "bad" economies favor the challenger.

"There are good features about the economy and bad ones," Straszheim says. "This is more like an average economy. And when the economy is average, the public tends to focus on non-economic issues in their election calculus, such as terrorism, Iraq and leadership." On these issues, voters favor Bush.

Still, even if stocks continue to enjoy a post-convention "Bush bounce," it might not last. Don't count Kerry out just yet. "We would not be surprised if the horse race continues to be tight up until Election Day," warns Smith Barney investment strategist Tobias Levkovich.