AS SEEN IN USA TODAY'S MONEY SECTION, JULY 12, 2006

Cybercrooks turn to hacking many applications

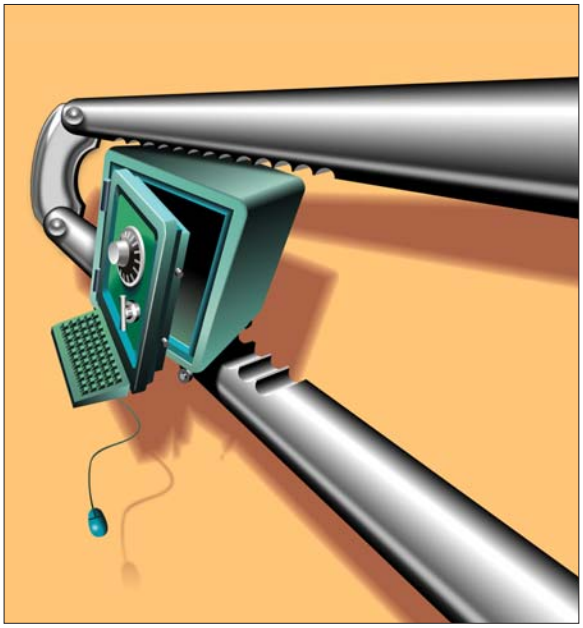
Windows no longer sole target; Macs attacked, too

By Byron Acohid
USA TODAY

SEATTLE — In a widely aired TV commercial, a hip-looking dude personifying Apple products wipes the nose of a sickly businessman representing Windows PCs, and smugly declares Apple's immunity to computer viruses.

But the ad belies an alarming shift in cyberattacks. Cyber-intruders once bent on breaking into the Windows operating system are increasingly probing for vulnerabilities in popular software applications — and not just Microsoft's.

Critical security holes have been turning up in Web browsers, anti-virus programs, word processors, spreadsheets and digital media players. "As we start to see the operating system become more secure, the criminals are moving up the application layer trying to attack Office or iTunes or RealPlayer," says Stephen Toulouse, Microsoft security response center program manager.



By Bob Laird, USA TODAY

The profit motive has never been greater for cybercrooks to take control of a PC to hijack online accounts and commit identity theft. Yet most people don't realize the degree to which their favorite software applications have come under assault, say security experts. Popular routes include:

▶ **Tainted spreadsheets.** Microsoft on Tuesday issued patches for 17 security holes — a dozen for its ubiquitous Office programs. One flaw was discovered in mid-June by a corporation. An employee had opened a tainted Excel spreadsheet attachment, which then took control of the PC, says David Cole, director of Symantec's security response center.

▶ **Web-browser bugs.** A Russian-built program called WebAttacker is being planted on websites across the Internet, says Roger Thompson, chief researcher for Exploit Prevention Labs. It checks each website visitor's browser for vulnerabilities, then uses one to take control of the PC. Cybercrooks have discovered "a rich pool of vulnerabilities" in browsers, says Thompson.

▶ **Apple security holes.** Apple has issued patches for vulnerabilities 35 times since January 2005, including 12 this year. Seven have been to fix flaws in its popular iTunes and QuickTime digital media software. The most recent iTunes patch, issued June 29, plugs a security hole that could allow an intruder to execute malicious code. Apple turned down interview requests for this story.

Apple and other software vendors are just starting to come to grips with security patches, says Scott Carpenter, director of security labs at Secure Elements. Unlike Microsoft, which has emphasized security since early 2002, Apple lacks a "well-developed process of notification and remedies," he says. "Apple's message is, 'You don't have to worry about security with a Mac,' but that's just not true."

Discussion

- Why have cybercrooks started attacking software applications?
- What tactics do cyberthieves use to steal money?
- How do Web-browser bugs operate?
- What vulnerability were iTunes users exposed to earlier this year?
- How do cybercriminals damage individuals and businesses? What effect do online crooks have on law enforcement and the economy?

Activity

Staysafeonline.org lists the "Top 8 Cyber Security Practices." They are:

- Protect your personal information. It's valuable.
- Know who you're dealing with online.
- Use anti-virus software, a firewall, and anti-spyware software to help keep your computer safe and secure.
- Be sure to set up your operating system and Web browser software properly, and update them regularly.
- Use strong passwords or strong authentication technology to help protect your personal information.
- Back up important files.
- Learn what to do if something goes wrong.
- Protect your children online.

Visit www.staysafeonline.org, and read the detailed information the site provides on each of the above tips. Next, using content from the article and the staysafeonline website, create 10 statements about online security. Half of your statements should be true, and the other half, false. Then, write a paragraph that attempts to explain cybersecurity practices to novice computer users. Include both true and false information in your work. Finally, ask a peer or a parent to review your paragraph, and identify the fallacies you embedded in it. Point out any of the inaccuracies the individual missed, and explain the correct action to take in each case.

Snapshot

USA TODAY Snapshots®

By Darryl Haralson and Robert W. Ahrens, USA TODAY

If you have a computer at home, what precautions has your family taken to make it more secure? Should the government take further steps to regulate the Internet? If so, what action would be effective, since the Net is not simply an American enterprise?

Consider all the issues involved in improving Internet security. For example, government officials and business leaders would need to agree on measures that protect free speech and free enterprise, but also deter Internet fraud. Moreover, the country would have to hire more law enforcement personnel and train them in cybersecurity. Even then, foreign criminals would be outside the reach of U.S. law. Yet, if the government, tech companies and other businesses don't take action, Internet crime will continue to cost consumers and businesses billions.

As a class, imagine that you are an advisory board appointed by the government and charged with solving the Internet security problem. Identify the first three steps you would take.