

## Unprotected PCs can be hijacked in minutes

USA Today

Tue Nov 30, 7:13 AM ET

Excerpts from the article:

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.

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 Windows XP operating system, an Apple Macintosh ([news](#) - [web sites](#)) and a Microtel Linspire, which uses the Linux ([news](#) - [web sites](#)) 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 ([news](#) - [web sites](#)) 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.