AVANTGARDE

PR Contact:

Louis Cheng
A&R Partners for Avantgarde
650-762-2814
lcheng@arpartners.com

FOR IMMEDIATE RELEASE

Automated "Bots" Overtake PCs Without Firewalls Within 4 Minutes

Experiment Reveals How Different Platforms Protect Against Internet Attacks

SAN FRANCISCO, Calif., November 30, 2004 – Avantgarde today released a study that showed that automated "bots," worms and other threats pummeled six computer platforms over a two-week period with 305,955 total attacks. Results also revealed that an inadequately protected computer fell victim to an actual compromise within four minutes of first plugging into the Internet. The study, conducted in partnership with security consultant and reformed hacker Kevin Mitnick, analyzed the security performance of commonly-used computer platforms against Internet attacks in the wild when running on the default security settings designated by vendors. The study revealed that Linspire (Linux) and Microsoft Windows XP Service Pack 1 with the free Zone Labs ZoneAlarm firewall received the fewest number of Internet attacks throughout the two week experiment. The regular Windows XP Service Pack 1 system without a third-party firewall was the most vulnerable, and was successfully compromised by an attack within four minutes of first plugging into the Internet.

Six different computer platforms were tested in the experiment to simulate the possible computer environments used in an average small office or home office – Microsoft Windows Small Business Server 2003, Microsoft Windows XP Service Pack 1, Microsoft Windows XP Service Pack 1 with ZoneAlarm, Microsoft Windows XP Service Pack 2, Macintosh OS X 10.3.5, and Linspire (Linux). The computers were connected to the Internet for two weeks without any adjustments to the preconfigured security settings from the manufacturer. The objective was to analyze the amount of time each computer platform can exist on the Internet before being compromised, the number of attacks experienced while on the Internet, the number of successful compromises achieved by the attacks, and the type of attacks most commonly seen.

Results revealed that the Linspire computer and the computer running Windows XP Service Pack 1 with ZoneAlarm were the most secure and experienced the fewest number of Internet attacks, without ever being compromised throughout the experiment. These two machines were the most effective at reducing the visibility of the computer from Internet hackers while online and preventing Internet attacks from successfully loading arbitrary malicious code without permission. While receiving more attacks, the Microsoft XP SP2 machine and the Macintosh OS X 10.3.3 were not compromised by the attacks. The Windows XP Service Pack 1 was repeatedly compromised—with the first attack occurring just four minutes after plugging into the Internet—and Windows Small Business Server 2003 was compromised eight hours after plugging into the Internet.

AVANTGARDE
Marketing & Design

665 Third Street
№ 329
San Francisco
California
94107 · USA

T +1.415.281.9196
F +1.415.281.9197
avantgarde.com

"The majority of home PCs are running some form of Windows-based platform and it is important for them to know that the moment they connect to the Internet, they are almost immediately under some form of Internet attack," said Marcus Colombano, partner at Avantgarde and co-investigator of this experiment. "Windows XP Service Pack 1 with ZoneAlarm was the most secure machine out of all the Windows-based systems tested due to its ability to stealth a computer while online and block unauthorized access. In addition, this third-party firewall contains an important feature that asks users for permission when a program attempts to access the Internet, a feature not included in Windows XP Service Pack 2."

"This experiment underscores the need for consumers to have a personal firewall enabled every time they go online because of automated attacks that are consistently launched on the Internet," said Kevin Mitnick, co-investigator and founder of Mitnick Security Consulting LLC, a security consulting firm. "Owners of Microsoft's Service Pack 2 already have an integrated inbound firewall but to be adequately protected, a personal firewall with inbound and outbound traffic blocking capabilities is essential. This capability can be found in several third-party firewall products, some of which are free and publicly available. If computer users fail to install a firewall onto their home PC, it's just a matter of time before they get hacked."

Malware such as spyware, worms and Trojan horses, can be transferred through e-mail, instant messages, peer-to-peer programs and routine Web browsing. Once loaded onto a computer, these threats have the ability to monitor a user's online activities, capture keystrokes to steal credit card numbers, financial data, usernames and passwords, and communicate this information back to a hacker.

About Avantgarde

Founded in 1994, Avantgarde is a marketing communications firm with a strong foundation in strategic planning, development and tactical implementation. Co-founder Marcus Colombano draws from his experience and expertise in networking and consumer electronics to help technology clients with all critical facets of their communications efforts. For more information about Avantgarde, visit the company's website at www.avantgarde.com.

About Kevin Mitnick

Kevin Mitnick is a security consultant to corporations worldwide and cofounder of Defensive Thinking, a Los Angeles-based consulting firm (defensivethinking.com). He has testified before the Senate Committee on Governmental Affairs on the need for legislation to ensure the security of the government's information systems. His articles have appeared in major news magazines and trade journals, and he has appeared on *Court TV*, *Good Morning America*, *60 Minutes*, CNN's *Burden of Proof* and *Headline News*. Mitnick has also been a keynote speaker at numerous industry events and has hosted a weekly radio show on KFI-AM 640 Los Angeles.

# # #