

Clear 58°
5 Day Forecast



- News
 - Top Stories
 - Sports
 - Business
 - Entertainment
 - Community News
 - Editorial
 - Death Notices
 - Weather
 - AP - The Wire
 - TV Listings
 - Movie Listings
 - National News
 - USA Weekend
- Classifieds
- Personals
- Best of Delco
- How to Place a Print Ad
- To Subscribe
- Business Directory
- Newsstand
- Our Newspaper
- Maps
- Directions
- Other Publications
- Sports Wire!
- Fun and Games
- Consumer Guide
- Personal Finance
- Lifestyles
- Newspapers In Education

Business for Sale

Profit from the Internet. Proven System. Business for Sale. Invest \$39,700 US. www.wsicorporate.com

Business Opportunity

Work from Home. Become financially independent. Free information Package. www.wsicorporate.com

Busin
Profit
Prove
Busin
Inves
www.w

Business

Is remote resetting a legitimate threat to Internet?

By PATTI MENGERS , pmengers@delcotimes.com

04/22/2004

Today Milwaukee mathematician Paul Watson is expected to reveal at an Internet security conference in Vancouver, British Columbia, how hackers could disrupt Internet connections worldwide by remotely resetting computers.

But local computer experts say the odds of such a disruption occurring are long and the effect on individual computer users would be minimal.

"The worst-case scenario is that the Internet would be inaccessible for periods of hours," said Swarthmore College Network Manager Mark Dumik.

Larry Pfeiffer, network engineer for the Information Technology Department at Widener University in Chester, said the vulnerability has probably existed since around 1990 when the Border Gateway Protocol, or BGP, was established for routers to connect with the World Wide Web. "This is not new, by no means. It's just a vulnerability that's out there. It's not a terrorist organization threatening to bring down the Internet. It is a hole, a vulnerability," said Pfeiffer.

Watson has predicted that hackers would understand how to begin launching attacks "within five minutes of walking out of that meeting" where he is disclosing details of the flaw he said he found in the Transmission Control Protocol or TCP, which is how computers set up connections between two points on the Internet.

"You may theoretically know how to do it but actually doing it is a lot more difficult. You'd need a whole lot more information about the traffic you're trying to disrupt between the two ISPs (Internet Service Providers)," said Dumik.

Experts previously said such attacks could take between four years and 142 years to succeed because they require guessing a rotating number from roughly four billion possible combinations. Watson said he can guess the proper number with as few as four attempts, which can be accomplished within seconds.

"What this guy claims is that the number is much less than 4.3 billion. It's still a small risk, but bigger than previously anticipated," said Dumik.

The Homeland Security Department has issued a cyberalert that attacks "could affect a large segment of the Internet community." It said normal Internet operations probably would resume after such attacks stopped.



Roger Cumming, director for England's National Infrastructure Security Coordination Centre, has said exploitation of the vulnerability could affect "the glue that holds the Internet together."

Experts said there have been no reports of attacks using this technique.

"I'm sort of discounting the likelihood of seeing something fairly significant because of this," maintained Dumik. Pfeiffer explained that the insertion of reset packets between two points on the Internet has proven valuable in terms of intrusion detection.

However, if someone has logged on to the Internet and has an open TCP connection, a hacker exploiting the vulnerability could reset the connection and log the person off, forcing the person to re-establish the connection.

"If someone does a TCP reset for example, between AT&T and Qwest, you would lose connectivity between the two, you would lose the routing protocol and it would take 30 to 40 seconds to re-establish the connection," explained Pfeiffer.

The BGP is how 134,000 routers on the Internet establish a connection with everyone on the World Wide Web and communicate with one another, said Pfeiffer. Two ISPs can have a constant connection, sharing routes.

If a reset keeps happening between two providers, BGP dampening goes into effect and the connection is put in a holding pattern, noted Pfeiffer.

"The BGP dampening sees it as unstable and puts it on standby, in a holding pattern for 40 minutes," he said. A reset on an ISP like Qwest, with multiple sites, could affect a large number of users, he noted.

"It could shut down whoever is attached to Qwest," said Pfeiffer.

Dumik said it is up to the large ISPs and major computer equipment vendors like Cisco Systems Inc., not individual users, to address the risks of the vulnerability.

Cisco executives acknowledged that their popular routers were among those vulnerable and they have distributed software repairs and tips to otherwise protect large corporate customers. There were few steps for home users to take. Officials at Microsoft Corp. said they did not believe Windows users were too vulnerable and made no immediate plans to update its software.

"A combination of new versions of software and best practices would minimize any risk from this vulnerability," noted Dumik.

He said a potential solution offered by US-Computer Emergency Readiness Team, or CERT, is that ISPs encrypt information they trade with each other to prevent hackers from inserting commands.

"It would take a lot of focused attention from someone with really sophisticated knowledge to produce a significant disruption that would interfere with Internet communication," noted Dumik.

In recent weeks, officials at some U.S. government agencies and companies operating the most important digital pipelines have fortified their own vulnerable systems because of early warnings communicated by some security organizations. The White House has expressed concerns especially about risks to crucial Internet routers because attacks against them could profoundly disrupt


online traffic.

The Associated Press contributed to this report.

©The Daily Times 2004

Reader Opinions

Be the first person to voice your opinion on this story!

Back to top 



Send us your community news, events, letters to the editor and other suggestions. Now, you can submit birth, wedding and engagement announcements online too!

Copyright © 1995 - 2004 [PowerOne Media, Inc.](#) All Rights Reserved.

[News](#) | [Classifieds](#) | [Directory](#) | [Today's Ads](#) | [AllAroundPhillyJobs](#) | [PhillyCarSearch](#) | [AllAroundPhilly](#) | [AllAroun](#)