



E-MAIL | JS ONLINE | TMJ4 | WTMJ | WKT1

Web search



Network Features



JSOnline MILWAUKEE JOURNAL SENTINEL

Journal Sentinel Services

Classifieds

OnWisconsin LIVE

AdFinder

Yellow

News Articles: Advanced Searches

Search



Subscribe to the Milwaukee Journal Sentinel online

JS Online Features

TECH

ON WISCONSIN : JS ONLINE : TECHNOLOGY :

E-MAIL | PRINT THIS STORY



Milwaukee expert uncovers serious Web vulnerability

By ADAM BERGSTROM abergstrom@journal sentinel.com

Posted: April 20, 2004

A Milwaukee computer security expert's research has helped discover a potential for serious Internet traffic-flow vulnerabilities.

Left unchecked, hackers could disrupt Web surfing, e-mail and other forms of electronic communication.

Paul Watson, who works for Rockwell Automation's Information Security Group, has been working with the British government's National Infrastructure Security Coordination Centre.

The organization released information Tuesday addressing flaws that could allow hackers to knock computers off-line and disrupt vital traffic-directing devices, called routers, that coordinate the flow of data among distant groups of computers.

"It's a vulnerability that everyone has known about but never really talked about," Watson, 35, said in an interview.

The flaw affects the Internet's "transmission control protocol." Watson said he identified a method to reliably trick personal computers and routers into shutting down electronic conversations by resetting the machines remotely.

Previously, experts 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

NEWS

- Metro | Waukesha State | Editorials
- Traffic | Weather
- Obituaries | More...

SPORTS

- Packers | Badgers
- Packer Insider
- Bucks | Brewers
- Marquette | Preps
- Golf | More...

BUSINESS

- News | Technology
- Stocks | Investing
- Finance | More...

ENTERTAINMENT

- Dining | Movies
- Arts | Calendars
- Music & Night Life
- More...

FEATURES

- Lifestyle
- Food & Home
- Real Estate
- Health & Fitness
- Wheels | Travel
- Interactive Chats
- Photo of the Day

Special Features:



Need Help?

- Searching Archives
- Wireless Access
- Site Topics

MAI

- [AdFinder](#)
- [Jobs](#)
- [Cars](#)
- [Real Est](#)
- [Rentals](#)
- [Personal](#)
- [General](#)
- [Buy & S](#)
- [Contests](#)

Table of Contents

Contact Staff

Subscriptions

attempts, which can be accomplished within seconds.

"Exploitation of this vulnerability could have affected the glue that holds the Internet together," said Roger Cumming, director of the National Infrastructure Security Coordination Centre.

In the United States, the Department of Homeland Security issued its own cyber-alert hours later, warning that attacks "could affect a large segment of the Internet community." It said normal Internet operations probably would resume after such attacks stopped. Experts said there were no reports of attacks using this technique.

Routers continually exchange important updates about the most efficient traffic routes between large networks.

Continued successful attacks against routers can cause them to go into a standby mode, known as "dampening," that can persist for hours.

Watson began his research after attending a conference where he heard experts from Cisco Systems Inc. say it wouldn't be practical to use this method to attack Internet traffic flow.

"I didn't agree on one of the issues they covered," Watson said. "So I went outside to the pool and began doing my own research."

Watson completed his research in November. He sent it to the two men from Cisco Systems who gave the presentation, seeking their input.

"They said to me, 'Wow, we really dropped the ball on this one,' " Watson said. "Cisco contacted me immediately and asked if they could do more research to corroborate the results."

Watson and Cisco Systems contacted the Computer Emergency Response Team at Carnegie Mellon University in Pittsburgh, a group that works with manufacturers of Internet equipment on security matters. When the team didn't respond to the request, Watson and Cisco went across the Atlantic and called on the British officials.

"They got back to us immediately," Watson said.

Since then, the group has been feverishly working with more than 150 Internet equipment companies to fix the problems before Watson presents his findings at the annual CanSecWest Internet security conference in Vancouver, British Columbia, on Thursday.

Watson predicted that hackers would understand how to begin launching attacks "within five minutes of walking out of that meeting."

The Associated Press contributed to this report.

From the April 21, 2004 editions of the Milwaukee Journal Sentinel

[BACK TO TOP](#)

[News Articles:](#) [Advanced Searches](#) [Search](#)  [Subscribe to the Milwaukee Journal Sentinel - enter online](#) JS Online Feat

© [Copyright 2004](#), Journal Sentinel Inc. All rights reserved.
Produced by [Journal Interactive](#) | [Privacy Policy](#)

Journal Sentinel Inc. is a subsidiary of [Journal Communications](#).