



Search: Articles-last 7 days for [] Go



Register or Log In. Member Benefits

Back to Home >

Mon



email this print this license this

Posted on Sat, Apr. 24, 2004

- News
 - Mercury News
 - Top of Wires
- Columnists
- Research
- Financial Markets
- Public Markets
- Venture Capital
- Personal Technology
- SV Life
- People
- Valley News
- Hot Topics
- Careers
- Events
- Archives
- Contests
- Search
- Features
 - VC Survey
 - Salary Survey
 - SV 150

Tech sleuth tracked down Net flaw just for the `thrill'

By Dan Lee
Mercury News

Paul Watson is still digesting his flash of Internet fame this week, when he became the talk of the cybersecurity world.

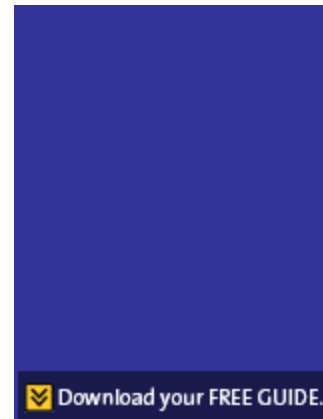
The independent security researcher from Milwaukee became a tech celebrity of sorts after the British government Tuesday made public his research exposing a flaw in a core Internet technology that could allow hackers to shut down large portions of the global network.

The flurry of security bulletins and media coverage in recent days was the climax in a tale of how one man's tinkering rippled across the globe, gaining the attention of national governments and hundreds of high-tech companies and Internet service providers.

``I'm really just shocked and amazed at the response," said the 35-year-old Watson, who presented his research Thursday at the CanSecWest computer security conference in Vancouver, British Columbia.

Watson's brush with tech fame began anonymously in Las Vegas in late July, when he attended a presentation by two Cisco Systems scientists at a computer security conference. Watson said it was a ``fine presentation with outstanding research," but he nonetheless had lingering questions.

``It just didn't sound right," he said. ``What bothered me was no one else in the room seemed to think there was something wrong."



[First Name]

[Last Name]

[E-Mail Address]

[Company]

[Phone]

Select a State or Province

[Zip]

Please Select a Country

Please keep me up to date on other product news and Security alerts via email.



On Aug. 5, Watson wrote on his personal Web site that he planned ``to compose a de technical rebuttal."

Watson, who works as a computer security officer for industrial automation company I Automation, began devoting much of his spare time to the issue. He said he spent eve weeks of vacation holed up in his basement.

The resulting paper was ``Slipping in the Window: TCP Reset Attacks."

Computer experts said Watson's research was a new approach to a long-known vulner previously considered too complex and time-consuming for hackers to exploit. The flay or Transmission Control Protocol -- could allow people to remotely attack computer sy routers, the key devices that ferry traffic around the Internet, by tricking them to shu

Such attacks, security experts said, could temporarily cause broad lapses in Internet s chance of a breach, it was thought, was remote because a hacker would have to gues numbers within a certain ``window" of time in order to end the TCP connection -- son was considered about a 1-in-4 billion shot.

But Watson concluded that an accepted number actually could be guessed in just seve

Watson sent his findings to Cisco, the world's biggest seller of Internet routers. Early t San Jose company turned it over to the Department of Homeland Security's U.S. Com Emergency Readiness Team (CERT) and then to Britain's National Infrastructure Secur ordination Centre.

From there, computer equipment makers and Internet service providers were warned vulnerability.

``The important thing is that a significant ` number of ISPs were given time to protect ` Internet before the release of the vulnerability," said Jeff Havrilla, an Internet security U.S. -CERT.

Cisco praised Watson for his handling of the matter. ``We appreciate the high ethical by contacting our scientists," said Mojgan Khalili, spokeswoman for the San Jose comp

Independent computer researchers such as Watson are driven by some common moti being first with a discovery and spurring tech companies to fix vulnerabilities, said Alla director of SANS Institute, which provides cybersecurity training.

``There's a dynamic that plays out with all of the researchers," Paller said. ``They wz for their excellence."

Watson traces his motivations back to, well, being a dedicated geek.

``I go to work eight or 10 hours a day. I come home and spend four to six hours play computer," he said, acknowledging his wife's patience.

One of his personal Web sites reflects his passion for computers, if in an alarming-sou name ``terrorist.net," he said, has to do with his fixation on computers and nothing e said he has owned the domain name for years, and the name became a running joke : friends that was easy to remember. ``It has no connotation whatsoever to terrorism i

said.

Watson, who grew up in Indiana, said he is largely self-taught in computer science. He joined the Air Force, working on computers for NORAD, North American Aerospace Defense Command, in Alaska.

Watson said he loves attending DefCon, the annual hackers convention in Las Vegas, but he has never done anything illegal at the computer keyboard.

``It's the thrill of discovery," he said.

Contact Dan Lee at dlee@mercurynews.com or (408) 920-5425.



[email this](#)



[print this](#)



[license this](#)



© Media Income
use website content
Real Cities website

[About SiliconValley.com](#) | [About the Real Cities Network](#) | [Terms of Use & Privacy Statement](#) | [Ridder](#) | [Copyright](#)