

The man who saved the Internet

Ignored by U.S., he alerted U.K. experts to head off disaster

BY GILLIAN SHAW VANCOUVER SUN

For three months, it was Paul Watson's worst nightmare.

For a couple of weeks, it was also the world's worst-kept secret — known to 100,000 computer security experts around the globe.

But by the time the average computer user was alerted this week to a threat said to be capable of disrupting the Internet worldwide, the problem had largely been eliminated.

And when Watson, a Wisconsin computer security specialist, arrived in Vancouver Wednesday to attend a security conference, he was amazed to find that instead of being a bit player on an agenda of heavyweight security experts, his discovery of the problem is making headlines worldwide.

It all began when Watson, working in the basement computer lab in his Milwaukee home, wrote a paper describing a flaw in the Transmission Control Protocol (TCP), the core of Internet technology.

But in the hands of the wrong people, he feared, that knowledge could be used to knock computers offline and disrupt routers, the devices that direct Internet traffic.

"I was absolutely terrified of that and that's one of the reasons I waited to publish the paper," he said. "The concern is, . . . in the worst-case scenario, a sponsored effort by a politically motivated group, or hackers trying to play games with each other or carrying out a grudge. It could be traffic slowing down or it could be a complete loss of traffic. It depends on the sophistication of the attacker."

So instead of going public, Watson said, he tried for three months to alert the U.S. Computer Emergency Response Team (CERT) to the threat, but his calls and e-mails went unanswered.

Finally he went to British computer security experts, who heeded his warnings and helped spread the word that led to solutions being created to end the threat.

"For the most part it is fixed," said Watson. "The threat that affected the entire Internet is fixed."

It was the British government that first announced the threat Tuesday through its national infrastructure security coordination centre. Hours later, the U.S. Homeland Security Department issued its own cyber alert.

Details of Watson's findings can be found on the CERT website.

But his role didn't stop there.

An army of more than 100,000 security experts around the globe was mobilized to come up with the fixes. And Watson was one of the generals rallying the troops.

"I have worked quietly behind the scenes, talking to vendors and security groups, making sure everybody who needed to know did know," Watson said.

"Over the past week, more than 100,000 people around the globe have been aware of it and it has been shocking that everyone has been able to keep such a secret."

Describing the nature of the threat, Watson likened the Internet to a highway and the routers as bridges on that highway.

"This attack is like where all the bridges disappear overnight.

"People can get into their cars and be safe, but they can't get anywhere."

Unlike other Internet threats, this vulnerability can't be used on its own to access data or take over computers. It could simply disrupt traffic, causing slowdowns and total stoppages, amounting to a denial of service (DOS) attack. For companies, Internet Service Providers and others that rely on the Internet for constant delivery of data, an attack could be disruptive and even devastating.

While the threat has captured headlines because it deals with the core of Internet technology,

some security specialists feel the danger has been overblown.

"I'm kind of waiting like everyone else. I'm not taking this as the end of the world— not even close," said Ryan Purita, senior security consultant with Vancouver's Totally Connected Security, echoing a sentiment expressed by others in the industry. "It's just another denial of service as far as I'm concerned."

The U.S. CERT coordination centre is taking it seriously, though.

"The threat is real, it is a problem that has been well known for some time," said Jeff Havrilla, Internet security expert representing the U.S. computer emergency readiness team, a partnership between the U.S. Department of Homeland Security and the CERT coordination centre. "What Mr. Watson was able to observe and document in his paper was that some very important protocols . . . used to route information over the Internet rely on TCP more and more in such a way that these vulnerabilities make it easier to attack."

Havrilla said it is doubtful the vulnerability could be used to cause significant shutdowns on the Internet. although he added: "But I hope to never be proved wrong. It could take out bits and pieces of the Internet, mainly at the edges, where people rely on ISPs to get to the Internet.

"It could block the on-ramps to the information highway."

Havrilla said he couldn't comment on Watson's statement that CERT didn't respond to his warnings, although he added, "Whatever Paul is saying, I'm sure it is accurate."

Peter Bissonnette, president of Shaw Communications, said his company deals with denial of service threats on a regular basis.

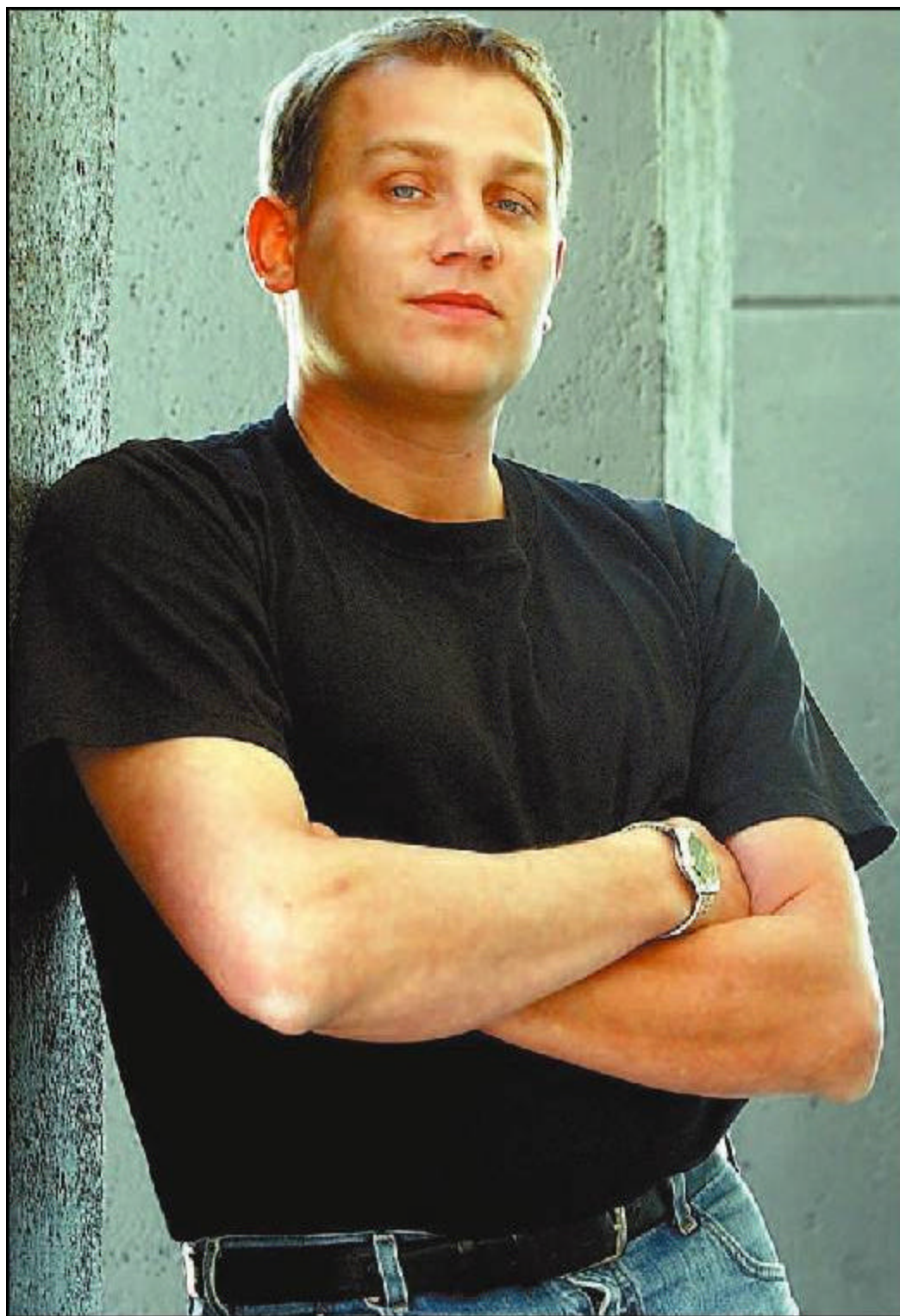
"We've been aware of the situation for the last two weeks and we have done what we have to do in order to mitigate anything happening to us," he said.

Watson, who presents his paper today at the CanSecWest/core04 conference in Vancouver, is surprised by all the attention.

"I actually felt very lucky to even get my paper published at this conference," said Watson, who is an Internet security researcher for Rockwell Automation in Wisconsin and in his spare time works with the Open Source Vulnerability Database, cataloguing security risks.

Watson said when he contacted Britain's national infrastructure security coordination centre, the British acted promptly to notify vendors, coordinate with security specialists and talk to governments around the world.

"I have a whole lot of respect for the information security professionals in the U.K.," he said.



IAN LINDSAY/VANCOUVER SUN Paul Watson says he was terrified that hackers would find out about the flaw.