



Location: <http://www.zdnetindia.com/techzone/resources/security/stories/102264.html>.

Net's 'savior' sets the record straight

Delivering a presentation at a security confab in Canada, researcher Paul Watson, "The Man Who Saved the Internet," says it was nothing. Really.

Robert Lemos, April 24, 2004

"The Man Who Saved the Internet" says it was nothing. Really.

Paul Watson, whose research on a flaw in the way data is sent across the Net inadvertently triggered a flood of hyperbolic news reports, is finding all the attention a little strange.

"I got off the plane in Vancouver (on Tuesday), and suddenly it's a completely different world," he said. "It's crazy."

Watson's presence at [CanSecWest 2004](#) has garnered more media attention than the security conference has attracted in its previous four years. In the past 24 hours, the researcher for Rockwell Automation has fielded numerous calls for interviews from newspapers, television and radio, and a local paper even ran a front-page photo of him this week, anointing--or saddling--him with the grandiose title of Net savior.

What's crazy is this: The widely reported threat to the Internet--the threat that could let attackers bring the whole worldwide network crashing to its knees--doesn't really exist. Or at worst, it's minor.

Watson said earlier in the week that the reports were overstated, amounting to an "inordinate level of attention in respect to the amount of risk," and that because most major ISPs (Internet service providers) had already addressed the issue, the flaw could at most lead to "isolated attacks against small networks, (which) would most likely be able to recover quickly."

On Friday, Watson got a chance to further clarify the situation when he finally delivered his presentation here. "This may be anticlimatic," Dragos Ruiu, the confab's organizer, quipped before Watson spoke, "but at least we can get the real story."

The nitty-gritty on the Net threat

The flaw in the way the majority of data is sent over the Internet is interesting, but not easy to exploit. Called a Transmission Control Protocol, or TCP, session attack, the technique could allow a hacker to insert forged data or commands into the connection between two network devices or computers.

The most common version of the attack, and the easiest to perform, is a TCP reset attack, where a reset command is injected into the data flowing between two devices. The success of the attack, and the number of data packets that have to be sent by an attacker, is determined by the size of the data buffer, or window, used by the device. All an attacker has to do is send a packet with the reset command and a sequence number within the current window.

Many devices use a window that can queue up the next 16,384 packets, which gives an attacker a one in 260,000 chance of hitting the window. By sending 260,000 packets, the attacker should be able to get one into the window, and thus accepted by the device as a legitimate command.

However, the attacker also has to guess another number for the attack to work, the address, or port, used by the application to send data. There are about 48,000 legitimate ports--however, most devices use a predictable set of port numbers for certain functions. Watson estimated that an attacker trying 50 different ports could succeed, but he stressed that the requirement made the attack operating system dependent.

A device that uses a very large window of 1 billion packets and has a single, known port, could theoretically be compromised with four packets--a number that has been featured in many media reports. But such a large window is unheard of.

Two other variations of the attack, which have been largely ignored, include sending a packet requesting a new connection and sending other commands that try to hijack the session. Both are far more difficult to bring off.

One well-known security expert, who asked not to be named, created an exploit in his hotel room during the week. He found the only interesting thing about the security issue was that routers tend to use predictable source ports, not random ones, a fact that could make attacks easier.

Others concurred: The real-world value of this flaw to attackers is not great, said Sharad Ahlawat, an incident manager with Cisco Systems' product security incident response team (PSIRT). Ahlawat had come to the Canadian conference to outline how the networking giant planned to fix its products. Cisco addressed the TCP issue on Wednesday.

"On the spectrum of things we have to worry about, this is low," Ahlawat said.

He stressed that other attacks are more worrisome. Moreover, the drawback for any attacker trying to reset a TCP connection is that it becomes difficult to gauge success.

Ahlawat did see a bright side to the overreaction to the issue.

"People are looking back at the (original technical specifications)...and making improvements on standards that were created when such attacks weren't a problem," he said.

And Watson, too, saw a silver lining. He may not have "saved the Net," but he might have done something to counteract the often one-sided depiction of hackers in the press.

Watson said he hoped the issue would highlight the hard work done by old-school, "white hat" hackers, the kind who probe systems with the hope of ultimately making them safer. He had, after all, based his TCP work on theirs--many attendees could point to older security papers that had mentioned the issue, and Watson never claimed to be the first to think of it.

"I hope that all the press brings more attention to what everyone here is doing," Watson said. "I'm really tired of 'hackers' being a bad word."