

Kiwi's Defcon contest challenges AV vendors

Results of competition will be wake-up call to users and vendors

BY ROB O'NEILL | AUCKLAND | TUESDAY, 19 AUGUST, 2008

EMAIL PRINT

DMZ Global's senior security engineer, Simon Howard, had global antivirus software vendors studying his every move at the legendary Defcon hacker conference, held in Las Vegas last week.

Howard ran a competition called the "Race to Zero" in which teams of security pros had to modify nine samples of malware and exploit code to evade anti-virus software from 10 leading vendors.

One team completed the task in just under two-and-a-half hours, but failed to win the contest as two samples did not pass muster when its modified samples were reverse-engineered for judging.

Two other teams also completed the task on the first day and the eventual winner was judged to be a team from security consultancy Mandiant.

The results will be a wake-up call to users as well as vendors.

"Pattern or signature-based anti-virus is dead," Howard told *Computerworld* on his return to New Zealand last week. "While a lot of people have behavioural technology, it has not made it into the enterprise space yet."

Howard says adoption of behavioural anti-virus technology needs to be accelerated.

For home users there is a message as well. Howard says while behavioural screening is included in some consumer anti-virus packages it often needs to be activated separately, rather than through the default boxes provided on installation.

Howard says consumers often get new technologies ahead of enterprises as this market is used as a sounding board for development before enterprise packages are released.

He says the need to manage pop-up information — to provide meaningful information and alerts to users — is a major challenge.

Another solution is whitelisting, where only known good software is allowed on a system. However, Howard says anti-virus systems should still be in use.

Howard wasn't the only Kiwi attending or presenting at Defcon. He says two consultants from Security-Assessment.com also attended, as well as Ben Hawkes, who studies Windows security.

Hawkes will be presenting at the Kiwicon 2k8 conference, to be held at Victoria University's Pipitea campus, on September 27 and 28.

According to the programme, he will explore the cutting edge of heap exploitation theory and practice on Windows Vista.

"The focus is on finding previously unknown attack vectors resulting from memory corruption on the heap. These include techniques for controlling execution flow, by attacking only the heap implementation and not the application itself, and techniques for attacking the application in conjunction with the heap. Additionally, several design changes to further improve the security of the Vista heap will be suggested," the event programme says.

The heap is the component in charge of dynamic memory management and is used to some extent in every Windows Vista process.

DMZ Global is a security management company owned by TelstraClear.

SHARE THIS STORY WITH:



LATEST NEWS

Sinclair to leave Renaissance

Telecom result helped by \$27m compensation payment

Gen-i awarded datacentre contract with Air New Zealand

FRY UP: They may be watching you

Five govt agencies engage with Public Records Act

Telecom revenue down, but some improvement seen

BOOKMARK THIS LINK FOR THE COMPUTERWORLD WHITEPAPERS

We're building 'IT' so you can come and research, starting with the subject most critical to all — Security.

SUBSCRIBE



Computerworld is New Zealand's only specialised information systems fortnightly. Subscribe now for \$97.50 (24 issues) and save more than 37% off the cover price!



SIGN UP



Get the latest news from Computerworld delivered via email. Sign up now

CLICK HERE FOR MORE INFORMATION

MOST POPULAR

READ COMMENTED EMAILED SHARED

- Netbook failure rate disappoints major user
- Canterbury University signs alliance with Microsoft
- File-sharing bill could extend surveillance culture - Bott
- How to roll out full disk encryption on your PCs and laptops
- Ernie Newman resigns

WHITE PAPERS

On Common Ground: Where Compliance and Data Protection Overlap

Automation Makes Perfect: Taking the Time Crunch Out of IT Compliance with Automation

POPULAR EVENTS

Excellence in the Use of ICT in Government Award 2010 Award

The Sustainable 60 Awards

The Sustainable 60 Workshops

SPONSORED LINKS

Local and International news Enterprise ICT must know info

NZ's most trusted tech advice Free NZ Delivery

Asigra Partner of 2010 Asigra Partner of the Year 2010, Asigra Experts, Free Online Quote!

Free Online Backup Trial Successful Businesses Use KinetiCD Powered by DDB. Get a 2 Week Trial

What's My Timeshare Worth Instant Quote with No Obligation! Over 10 Years of Experience.

CodeBlue - the new wave NZ's leader in proactive monitoring and IT services