

# Imperva backs IIA plans to quarantine zombie-infected Internet connections

SYDNEY, June 9. Data security leader specialist has backed the Australian Internet Industry Association (IIA) initiative in encouraging ISPs nationwide to adopt a new voluntary code of conduct on cyber security.

Along with educating and better protection customers, ISPs are also being asked to temporarily quarantine those users whose computers are infected by zombie malware and is generated spam. "This move is to be applauded and while it's certain to generate an outcry from some quarters, will only temporarily block an infected users' ability to generate spam. It won't affect their ability to surf the Internet or access a Webmail account," said Amichai Shulman, chief technology officer with Imperva.

He added: "The IIA says the code of conduct will give customers greater levels of confidence in the security of their Internet connections, as well as helping to reduce the levels of zombie infections actively connected to the Internet."

According to Shulman, the introduction of the new code of conduct will encourage Australian ISPs to introduce network activity detection on their platforms, so allowing to identify abnormal traffic patterns from a subscriber's IP address, and take appropriate action.

If, as seems likely, the code of conduct is adopted by Australia's ISPs, then it will almost certainly reduce the number and effects of zombie infections, which the Imperva CTO says, are usually the result of a user clicking on an email link routing to an infected Web site.

According to Shulman, his company revealed last month that hackers had started infecting Web servers with a denial of service application that effectively transformed them into zombie drones.

"As I said at the time, these servers are controlled using a simple Web application, consisting of just 90 lines of PHP code, making them highly effective for the cybercriminals, since they offer criminals more horsepower and - typically - fatter pipes for throwing out spurious traffic," he said.

"If, however, the ISPs are able to quarantine an IP address generating this type of spurious traffic, then the effects of a server-infection denial of service attack can be negated. It is to be hoped that, if Australia's ISPs adopt this code of conduct, then it makes its way up to the ISPs in the northern hemisphere."

For more on the Australian ISP code of conduct: <http://bit.ly/9P2AIG>

For more on Imperva: [www.imperva.com](http://www.imperva.com)

## About Imperva

Imperva, the Data Security leader, enables a complete security lifecycle for business databases and the applications that use them. Over 4,500 of the world's leading enterprises, government organisations, and managed service providers rely on Imperva to prevent sensitive data theft, protect against data breaches, secure applications, and ensure data confidentiality. The award-winning Imperva SecureSphere is the only solution that delivers full activity monitoring from the database to the accountable application user and is recognised for its overall ease of management and deployment. For more information, visit [www.imperva.com](http://www.imperva.com) and follow us on Twitter @Imperva.

## Media queries

Grenadine Lau

Imperva

Phone: +65.67494482

Mobile: +65.9666 1886

Email: [Grenadine.Lau@Imperva.com](mailto:Grenadine.Lau@Imperva.com)

David Frost

PR Deadlines Pty Ltd, for Imperva

Phone: +61.2.43415021

Mobile: +61 (0) 408 408 210

Email: [davidf@prdeadlines.com.au](mailto:davidf@prdeadlines.com.au)