



## TECHNOLOGY INSIGHTS

These are our own opinions.

We have no commercial arrangements with vendors.

For more reviews, please contact TECHNOLEDGE.

**T** +61 2 9909 0246  
**E** [info@technoledge.com.au](mailto:info@technoledge.com.au)  
**W** [www.technoledge.com.au](http://www.technoledge.com.au)

## Conficker Worm and Swine Flu What do they have in common?

### The pig that flew

Both threats have been vastly exaggerated by the media, and by the authorities charged with internet security and public health respectively. Early in May, the World Health Organisation was ready to declare the Swine Flu a full-on pandemic. At the time, the tally was 19 confirmed deaths world-wide, and some 800 infections.

It turned out to be just another flu, yet Australia's stocks of antivirals were exhausted before the country recorded a single case of swine flu. Our Health Minister had to order more Tamiflu and Relenza from drug makers doing summersaults all the way to the bank. In the first two months, 100 people died from the swine flu worldwide. In any two months, 600 people die from ordinary flu in Australia alone.

### The worm that grew legs

Conficker turned out to be just another worm, despite headlines like *'Conficker worm threatens April Fools' chaos'*, accompanied by the picture on the right. *'World waits as Conficker worms into action'* was another.

No, it wasn't just the media, as you can see from headlines like *'Conficker's next move a mystery to researchers,'* with the by-line *'Impossible to know what massive botnet will do April 1, researchers say.'*



### Experts Clueless, Public Panics

The massive botnet was already 8 million strong, according to security software vendor F-Secure, and growing. 'Security researchers are in the dark,' Computerworld's Greg Keizer wrote on March 24, 'about what will happen next week when the newest variant of Conficker, 2009's biggest worm by a mile, begins trying to contact its controllers.'

As the worm reportedly infiltrated the French government's naval systems – forcing the French to ground their warplanes – and the British Parliament's computer network, experts were aghast at the breadth of the worm's reach. Soon, there were hushed warnings of an impending 'digital Pearl Harbor.'

Just why these experts couldn't figure out what this worm would do, despite using harvested samples to infect their test PCs and observing their behaviour, is a very good question. It's obvious that they didn't have a clue and decided to play it safe like the WHO with the swine flu – better safe than sorry, right?

Bruce Schneier, a down-to-earth security expert, said that Conficker's 1 April deadline was just the kind of event humans tend to overreact to. 'It's a specific threat, which convinces us that it's credible. It's a specific date, which focuses our fear. Our natural tendency to exaggerate makes it more spectacular, which further increases our fear. Its repetition by the media makes it even easier to bring to mind. As the story becomes more vivid, it becomes more convincing.'

<http://www.guardian.co.uk/technology/2009/apr/23/conficker-panic>

## The Morning After

April 1 passed without incident, and soon we had the experts and security vendors telling us that this did not mean that Conficker was no longer a threat. The public doesn't like being taken for a ride and, perhaps for a rare moment, clearly saw the PC security business for what it is: a giant scam. A recession-proof giant scam because people think they mustn't skimp on security any more than they would skimp on the tyres of the family car.

The companies who make so much money from security software and services, and all the experts who make a good living from the bits they pick off the vendors' backs like those birds that feed on Rhinos, have a vested interest in keeping us permanently panicked. In that state, we'll renew that licence when it runs out next month and gladly pay the price. If we think we're being ripped off, we may have second thoughts.

Computerworld added another twist when it reported: 'Mainstream media hype leading up to the Conficker worm's April 1 software update may have distracted people from legitimate cyber threats, the U.S. Federal Bureau of Investigation's head of cyber security said Thursday.'

[http://www.computerworld.com.au/article/300670/conficker\\_hype\\_problem\\_says\\_fbi\\_cyber\\_chief?eid=-6787](http://www.computerworld.com.au/article/300670/conficker_hype_problem_says_fbi_cyber_chief?eid=-6787)

## Never say Die

The worm refused to go away, though, or perhaps the security experts didn't want to let it die. While the hype slowed dramatically after April 1, much like it did in the days after we entered a new millennium when the forecast catastrophe failed to eventuate, the worm kept turning. 'Conficker Worm Still Lurking, Threat Remains,' said a June 29 headline.

A month later, at the Black Hat security conference in Las Vegas, an F-Secure virus researcher stirred the pot again. 'The gang behind Conficker are no fools,' said Mikko Hypponen. 'They know their stuff, they know coding, development cycles, crypto and they are clever and they are watching us, their enemy in the security industry.' Needless to say, the IT media jumped on the story hoping to retrieve some of its damaged reputation.

The swine flu did a lot better in the same period, with the case load growing rapidly across Australia, which soon had the Health Minister warning that the worst case scenario death toll could be as high as 6,000. One expert said it could exceed 10,000 unless a vaccine became available.

By early August, with spring temperatures rising across the country, the nationwide death toll stood at 74 and the more responsible reporters conceded that the victims had died 'with' the swine flu, not from it.

## The Bottom Line

Don't pay more attention to the media or the experts than they deserve. Install decent Internet security software and spam filters, tighten up your browsers and make sure that you and your staff follow the road safety rules when you're out on the internet highway. We have a few resources for you on these subjects here: <http://www.technoledge.com.au/resources-straight-talk.htm>

And if you're worried that you might have caught this bug, known as Conficker or Downandup, here's a simple way to find out for sure: go to the first link below and run the free Sophos endpoint assessment test, which will identify any security issues on your PCs.

<http://www.sophos.com/products/free-tools/sophos-endpoint-assessment-test.html>

If it looks like one of your PCs has caught the bug, here's a free removal tool from the same source <http://www.sophos.com/products/free-tools/conficker-removal-tool.html>

# # #