16 May 2017
Herald Sun, Melbourne

Author: Paul Gilder • Section: Business News • Article type : News Item
Audience : 317,517 • Page: 22 • Printed Size: 895.00cm² • Market: VIC
Country: Australia • Words: 557 • Item ID: 775321874

Reality bytes: new hit looms for unprepared

PAUL GILDER
SECURITY

AUSTRALIAN companies have a brief window to fortify their security defences, experts say, amid fears a bigger version of the weekend's unprecedented global cyber attack is being plotted.

And small to medium-sized businesses appear most at risk, with industry figures showing 42 per cent of SMEs fell victim to a ransomware attack in the past year.

"It's not a matter of if, but when, ransomware or another type of external breach will impact your business," said Charif El Ansari, chief executive of Australian-listed data recovery provider Dropsuite.

"There are already reports of a second wave that may be coming soon if the attacks vary their original hack and send it again."

The warning comes in the wake of a ransomware attack — believed to be the world's biggest online extortion attempt — that emerged on Friday and has since struck more than 100,000 organisations in 150 countries, including British hospitals, German rail operators and Chinese universities.

The as-yet unidentified hackers behind the attack — nicknamed 'WannaCry' for the .WNCRYT file extension it applies to infected files — demanded victims make a bitcoin payment of $US300 ($405) to $US600 to recover their data.

It was reported yesterday that people who had paid ransoms had not received access to their files, suggesting any payment was futile.

The hackers appeared to target PCs with the Microsoft Windows operating system that had yet to apply an anti-malware patch issued by the tech giant in March. Reports suggest a number of smaller Australian companies were caught up in the attack.

Ian Yip, chief technology officer for Australia and Asia-Pacific at security software heavyweight McAfee, said the motivation was clearly financial. "For many companies, the financial impact from the disruption to services is going to be higher than the actual ransom, though few have gone ahead and paid it," Mr Yip said.

The level of sophistication behind the hack, blending ransomware with worm-like tactics, pointed to a criminal element rather than mischief-making, Mr Yip told *Business Daily*.

He said Australia appeared to have avoided the bulk of the attack, although any fallout may become more apparent later in the week.

"We haven't seen a high-profile incident here," he said. "Those companies that have the budget are OK; the concern is at the smaller end of town where there's not the same level of governance and people at the premises available to perform the same security checks."

Mr El Ansari said the assault should serve as a "wake-up call for every business", but most would do nothing and simply hope they would be left unscathed.

"Most are in denial that a breach will happen to them. This is highly irresponsible."


Squawk, but don't complain

16 May 2017
Herald Sun, Melbourne

Author: Paul Gilder • Section: Business News • Article type : News Item
Audience : 317,517 • Page: 22 • Printed Size: 895.00cm² • Market: VIC
Country: Australia • Words: 557 • Item ID: 775321874