THE AUSTRALIAN

Telstra backs Melbourne Cofense cyber security centre to defend Asia Pacific

EXCLUSIVE

By **JARED LYNCH**, REPORTER

4:50PM DECEMBER 31, 2020 • 19 COMMENTS

Telstra is backing a new centre to be built in Melbourne aimed at combating a sharp increase in sophisticated cyber attacks — some from foreign powers — across the Asia Pacific region.

The centre will aim to prevent phishing, or malicious emails, infiltrating Australia and the region's biggest businesses, who are also battling their own war in securing talent to prevent unwarranted cyber intrusions.

Telstra's venture capital arm, Telstra Ventures, has backed the company behind the centre — US-based Cofense, which is based near the CIA's headquarters in Virginia.

It is part of Telstra Venture's $US100m ($131m) bet on more than a dozen cybersecurity start-ups to bolster defences for big business, as attacks from criminals and foreign powers increase in volume and scale.

The Melbourne facility will replicate similar Cofense phishing-fighting centres located in Britain, India and the US, but be tailored to risks within the Asia Pacific region.

It follows a suspected Russian hack of US government agencies and private businesses across the globe that festered for months, going largely undetected by the Trump administration and cybersecurity firms until two weeks ago.

Cofense founder and chief executive Rohyt Belani told The Australian that spear phishing, using business email compromise (BEC), had cost business more than $US26bn ($34bn) over the past four years, with attacks showing no signs of abating.

Mr Belani said while most companies were running phishing simulation software to train their employees in preventing attacks, a more proactive approach was needed.

“You can reduce susceptibility. But we weren’t quite happy with saying ‘great you brought susceptibility rates down from 45-50 per cent to 5 per cent’ because there is still residual risk and what do you do about the 5 per cent?” Mr Belani said.

Part of the solution was installing a button in Outlook and other email platforms for people to report suspicious emails to aid early detection by cyber security experts. That button now has more than 29 million unique deployments globally, Mr Belani said, and is growing by about 100,000 per week.

“What we found was it is a tremendous source of crowdsourced data on suspicious emails. The challenge is how do you find the needle in the haystack.

“There are lot of suspicious emails being reported — some benign, some are spam, some are legitimate emails, and then there are the few that are malicious in nature.

“We created a suite of software to help members of security operations teams take this barrage of reports from an organisation and separate the signal from the noise.”

But Mr Belani said even some of the biggest corporations were facing talent constraints in securing cyber security experts, making it difficult to act on the deluge of suspicious email reports — even when they were sorted.

And this is when Cofense went from software developer to a managed service offering.

“It allowed organisations to outsource the problem of detecting phishing attacks that have bypassed their perimeter controls, their gateways ... and essentially remove the threat from their environment.

“We’ve done this for about three years in other parts of the world. We started in the US and now have phishing defence centres in the UK, Ireland and India as well. It’s just been a natural progression.”

The Melbourne centre will initially employ at least three cyber security experts, with the hope of building it out to a similar staffing levels of the US and UK centre, which employ about 20 and 10 people respectively.

Despite the lean operation, Mr Belani said the phishing defence centres (PDCs) were backed by the Cofense Research and Threat Intelligence teams and a "global network of more than 25 million people searching for and reporting suspected phish".

"By alerting an organisation or taking action right away, Cofense can prevent a successful large scale attack. In fact, the PDC team have identified and stopped attacks in less than 10 minutes," he said.

"We are excited about our new PDC location in Australia. It further enhances our commitment to our presence in the region, which includes expanded resources, staff and regional support. We believe that Human Intelligence will always be greater than Artificial Intelligence, and when combined with our automation technology, Cofense's intelligence delivers unparalleled protection for organisations."

The attack this year on US companies and government departments began as early as March when customers of SolarWinds, a US network-management company, began unwittingly installing malicious software as part of a routine and seemingly benign update issued for a software product known as Orion, according to the company.

The company said in its SEC filing that its Microsoft Office 365 email systems had been compromised and that this incident "may have provided access to other data contained in the company's office productivity tools".

The US Commerce and Treasury, Homeland Security and State departments, and the National Institutes of Health and the State Department were all hacked as well.

Russia's foreign-intelligence service is suspected of being responsible. The same group has been linked to cyber espionage campaigns in the past, including an intrusion of multiple agencies, among them the State Department and White House, during the Obama administration.

The Russian Embassy in Washington denied responsibility and said the allegations were "unfounded attempts of the US media to blame Russia".

Meanwhile, investigators are still assessing the overall fallout.

Additional reporting: Dow Jones News Wires

JARED LYNCH, REPORTER

Jared Lynch is a business reporter with a career spanning 15 years across national publications. Jared is based in Melbourne and writes on agribusiness, healthcare and gaming. He also has extensive experience i... Read more

More stories on this topic

- Foxtel, Telstra extend AFL deal
- Telstra sells Velocity business
- Uniti takes No. 2 spot after $140m Telstra fibre buy

Topics

Telstra

{"success":false,"message":"Widget not found"}