Barracuda research uncovers techniques cybercriminals are using to make business email compromise attacks more convincing

New report looks at why these low-volume attacks are so costly, and how to protect your business from these targeted threats

Sydney, 22 November 2019 – Barracuda, a trusted partner and leading provider of cloud-enabled security solutions, today released a new report with key findings about business email compromise (BEC) attacks. The latest report, titled Spear Phishing: Top Threats and Trends Vol. 3 - Defending against business email compromise attacks, reveals new details about these highly targeted threats, including the latest tactics used by cybercriminals and the steps you can take to help defend your business. See the full report: www.barracuda.com/spear-phishing-report-3 The report takes a detailed look at how these crafty spear-phishing attacks use convincing impersonation, strategic targeting, careful timing, and social engineering to steal money or personally identifiable information. It also tackles how organisations can use advanced detection techniques, security awareness training, and other strategies and solutions to successfully prevent these costly and damaging attacks. Fresh insights on targeted attacks Barracuda's research reveals insights into how these targeted attacks are impacting businesses and the approaches cybercriminals are using to try to make them more persuasive. 91 percent of BEC attacks take place on weekdays, with many being sent during typical business hours for the targeted organisation to make them more convincing. The average BEC attack targets no more than six employees, and 94.5 percent of all attacks target less than 25 people. 85 percent of BEC attacks are urgent requests designed to get a fast response. BEC attacks have high click-thru rates. One in 10 spear-phishing emails successfully tricks a user into clicking. That number triples for BEC attacks that impersonate someone within the organisation. In the past 12 months, the average amount lost per organisation due to spear-phishing attacks was $270,000. "Attackers continue to find new ways to make BEC attacks more convincing, ultimately making them more costly and damaging to businesses," said Don MacLennan, SVP, Email Protection, Engineering and Product Management, Barracuda. "Taking the proper precautions and staying informed about the tactics cybercriminals are using will help organisations defend themselves more effectively against these highly targeted attacks." Resources: Get the full report: www.barracuda.com/spear-phishing-report-3 Read the blog post: https://blog.barracuda.com/2019/11/21/report-defending-against-business-email-compromise-attacks/ Get the first two volumes: Get Spear Phishing: Top Threats and Trends, Vol. 1 - Best Practices to Defeat Evolving Attacks Get Spear Phishing: Top Threats and Trends, Vol. 2 - Email account takeover and defending against lateral phishing attacks About Barracuda At Barracuda, we strive to make the world a safer place. We believe every business deserves access to cloud-enabled, enterprise-grade security solutions that are easy to buy, deploy and use. We protect email, networks, data and applications with innovative solutions that grow and adapt with our customers' journey. More than 150,000 organisations worldwide trust Barracuda to protect them — in ways they may not even know they are at risk — so they can focus on taking their business to the next level. Get more information at barracuda.com. Barracuda Networks, Barracuda and the Barracuda Networks logo are registered trademarks or trademarks of Barracuda Networks, Inc. in the U.S. and other countries.

Contacts

Emma Keen
+61 2 8905 0995
mailto: emma@einsteinz.com.au
Karen Terranova
+61 2 8905 0995
mailto: admin@einsteinz.com.au
Antoinette Georgopoulos
02 8905 0995
mailto: