Breaking News: McAfee Reveals Details of Global Financial Fraud Ring -Operation High Roller

So far, McAfee estimates the criminals have attempted somewhere between â‚¬60 million and â‚¬2 billion in fraudulent transfers from at least 60 banks.

This fraud empire, dubbed Operation High Roller, has reached banking systemsworldwide, and is comprised of at least a dozen groups that use active andpassive automated transfer systems to steal high value transactions from highbalance accounts. The Operation High Roller attacks have impacted thousands ofevery class of financial institution: credit union, large global bank andregional bank, using smaller and less detectable automated transactions. OperationHigh Roller Report available for download here.

AUSTRALIAN INFORMATION & INTERVIEW OPPORTUNITIES: For localinformation about Operation High Roller activity specific to Australia, we haveMcAfee Asia-Pacific CTO Michael Sentonas and McAfee Enterprise SolutionsArchitect Sean Duca available for interview or comment. Also available tocomment on implications of this criminal activity is Alastair MacGibbon,Director, Centre for Internet Safety, University of Canberra. To enquireabout these opportunities, please contact Spectrum on 02 9954 3299 or mcafee@spectrumcomms.com.au.

LOCAL QUOTES:

We need to remember that criminals are agnostic when it comes to the colour of money. This latest series of coordinated, highly automated attacks moves quickly through multiple continents, scale easily and suggests collaboration across multiple criminal specialists. The size and resources of the bank does not seem to matter either: global banks, regional banks, credit unions have all been impacted and targeted. Michael Sentonas, Chief Technology Officer Asia Pacific, McAfeeThe fraudsters objective in these attacks is to siphon large amounts from high balance accounts, and this campaign indicates that cybercriminals are evolving and becoming increasingly scalable. The success of these attacks is reliant on several factors and therefore there are several chokepoints: the end point needs to be compromised (phishing), bank monitoring systems need to be fooled, and crooks still need to extract money from mule accounts. - Alastair MacGibbon, Director, Centre for Internet Safety, University of Canberra.IMAGES: Spokesperson photos http://www.flickr.com/photos/spectrumpr/sets/72157630292982028/with/7445749304/

REPORT detailing the financial fraud ring operation, dubbed OperationHigh Roller:

http://www.mcafee.com/us/resources/reports/rp-operation-high-roller.pdf

Operation High Roller INFO & UPDATES: To keep abreast of the latestblogs related to this, please go to blogs.mcafee.com

Kind regards,

The Spectrum Team

Contacts: Richelle Gillett or Jessica Tubnor

Phone: 02 9954 3299

Email: mcafee@spectrumcomms.com.au