Cybercrime attacks rise 40 percent across Asia-Pacific with identity attacks double the global average -- revealed by latest data from ThreatMetrix

The Asia-Pacific region is facing unprecedented levels of complex cybercrime and fraud attacks, as revealed in the "2016 Q3 Cybercrime Report -- APAC Deep Dive" from ThreatMetrix®, The Digital Identity Company®.

Hong Kong, China, December 13, 2016 /India PRwire/ -- The Asia-Pacific region is facing unprecedented levels of complex cybercrime and fraud attacks, as revealed in the "2016 Q3 Cybercrime Report -- APAC Deep Dive" from ThreatMetrix®, The Digital Identity Company®.

Key highlights in the report:

- **APAC digital revolution:** Online transaction volume increased 36 percent over the previous year on the ThreatMetrix Digital Identity Network®
- **Mobile access is the key:** Mobile transactions make up 35 percent of overall transaction volume, a 44 percent increase since 2015.
- **APAC is facing unprecedented threats:** 40 percent increase year-on-year in the number of daily attacks; China revealed as the most attacked nation in the region.
- **Finance goes mobile:** Mobile transactions in financial services have almost tripled compared to last year
- **Cross-border transactions fuelling high attack rates in APAC**: Higher than average instances of cross-border transactions compared with global figures, which are more susceptible to bot attacks and location spoofing than domestic transactions

Identity attacks are having an ever-increasing impact on APAC businesses as fraudsters monetize credentials harvested from huge data breaches by testing, validating and augmenting identity data. Spikes in automated bot attacks, which are being used to carry out identity credential testing activity, are leading to attack peaks where 14 percent of all transactions are rejected as fraudulent. Identity spoofing is the most prevalent attack vector in APAC - cybercriminals are actively leveraging stolen identity data to carry out attacks on digital transactions.

"Identities are fast becoming hard currency for cybercriminals perpetrating online fraud. Many of the attacks we see in the Digital Identity Network are focused on stealing, validating, augmenting and selling identity credentials to make future attacks more lucrative," says Vanita Pandey, vice president of strategy and product marketing at ThreatMetrix. "As fraudsters leverage patched-together stolen identities, it is only in understanding the intricacies of a true digital identity that organizations can accurately detect future fraud."

Notes to Editor

About the report

The report is based on actual cybercrime attacks that were detected by the ThreatMetrix Digital Identity Network during real-time analysis and interdiction of fraudulent online payments, logins and new account applications. ThreatMetrix®, The Digital Identity Company®, is the market-leading cloud solution for authenticating digital personas and transactions on the Internet.

Download the report here.

For more information, please contact:

Ken Lam
ThreatMetrix
(L) +852-61800905

Paul Wilke
Upright Position Communications
(L) +1-415-881-7995