CYBER SECURITY PRIORITIES AND CHALLENGES

REGULATORY, INDUSTRY AND ENTERPRISE PERSPECTIVES

Tony Chew

Chief Security Architect

V-Key (Singapore)

16 May 2017

CYBER SECURITY FORUM & EXPO

منتدى ومعرض الأمن الإلكتروني

The cybersecurity threat landscape has become more ominous, menacing and volatile.

No system is impenetrable, invincible or indestructible.
Security strategy: protect, detect and respond.

The biggest hacking incidents and data breaches occurred in 2015 and 2016

No password is safe from hackers.

All passwords can be broken.

CNN Money International +

Markets Economy Companies Tech Autos Video

stock tickers

Hackers Lurked in Bangladesh Central Bank's Servers for Weeks

Cybercriminals used malware, hacking tools and keylogger software to breach system,

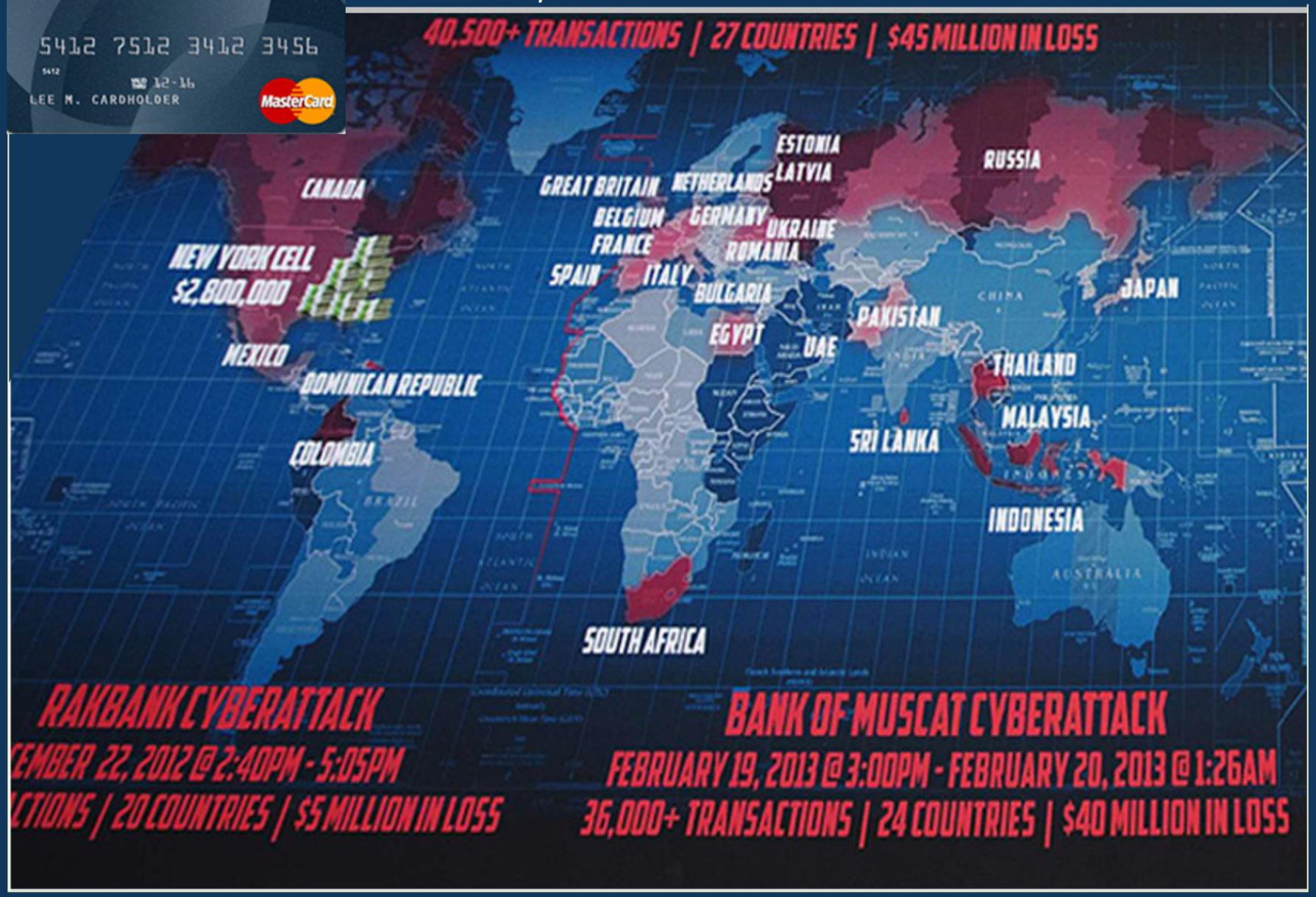
Ecuador Bank Hacked — $12 Million Stolen in 3rd Attack on SWIFT System

Friday, May 20, 2016 Swati Khandelwal

Bangladesh is not the only bank that had become victim to the cyber heist. In fact, it appears to be just a part of the widespread cyber attack on global banking and financial sector by hackers who target the backbone of the world financial system, SWIFT.

Yes, the global banking messaging system that thousands of banks and companies around the world use to transfer Billions of dollars in transfers each day is under attack.

$45 MILLION ATM HEISTS



Most USB thumb drives can be reprogrammed to silently infect computers

COMMENTS

Lucian Constantin
IDG News Service Jul 31, 2014 2:46 PM

Most USB devices have a fundamental security weakness that can be exploited to infect computers with malware in a way that cannot easily be prevented or detected, security researchers found.

2FA should be the minimum requirement for secure access controls and authentication

One-time-password and biometric access controls should be made mandatory for critical systems

Make the Chairman, CEO and EXCO jointly and severally responsible for cybersecurity and risk management

The CTO, CIO and CSO should also be held equally accountable and liable.

All banks offering online services should adopt responsible cybersecurity policies and data protection practices

All critical systems should be subject to annual risk assessment and penetration testing.

Two factor authentication (one-time-passwords & biometrics verification) should be made mandatory for all internal and external access to critical systems

Standards should be set for the adoption of defense-in-depth and multilayered security practices for all critical infrastructures, networks and systems

All wholesale and interbank payment systems should adopt the recently published SWIFT GLOBAL PAYMENT security standards.

Cybersecurity intelligence sharing and reporting of hacking incidents to regulators and affected customers should be mandatory industry practices.

Regulators and law enforcement agencies should have the power to enforce cybersecurity standards established by governments and regulators.

CYBER SECURITY
FORUM & EXPO
منتدى ومعرض
الأمن الإلكتروني

Thank You

For any enquiries, please contact us at enquires@v-key.com