RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Minimizing the Threat of Mobile Banking Cybercrime

SESSION ID: MBS-T10

Paul J.S. Oliveria

Technical Communications Manager
Trend Micro Incorporated


Back
Photograph Check Front
Make sure the entire check is inside the blue box and touch the camera icon when you are ready. Your iPhone will take the picture when the phone is steady.

KrebsonSecurity

In-depth security news and investigation

BLOG ADVERTIS

17 Double Cashing With Mobile Banking

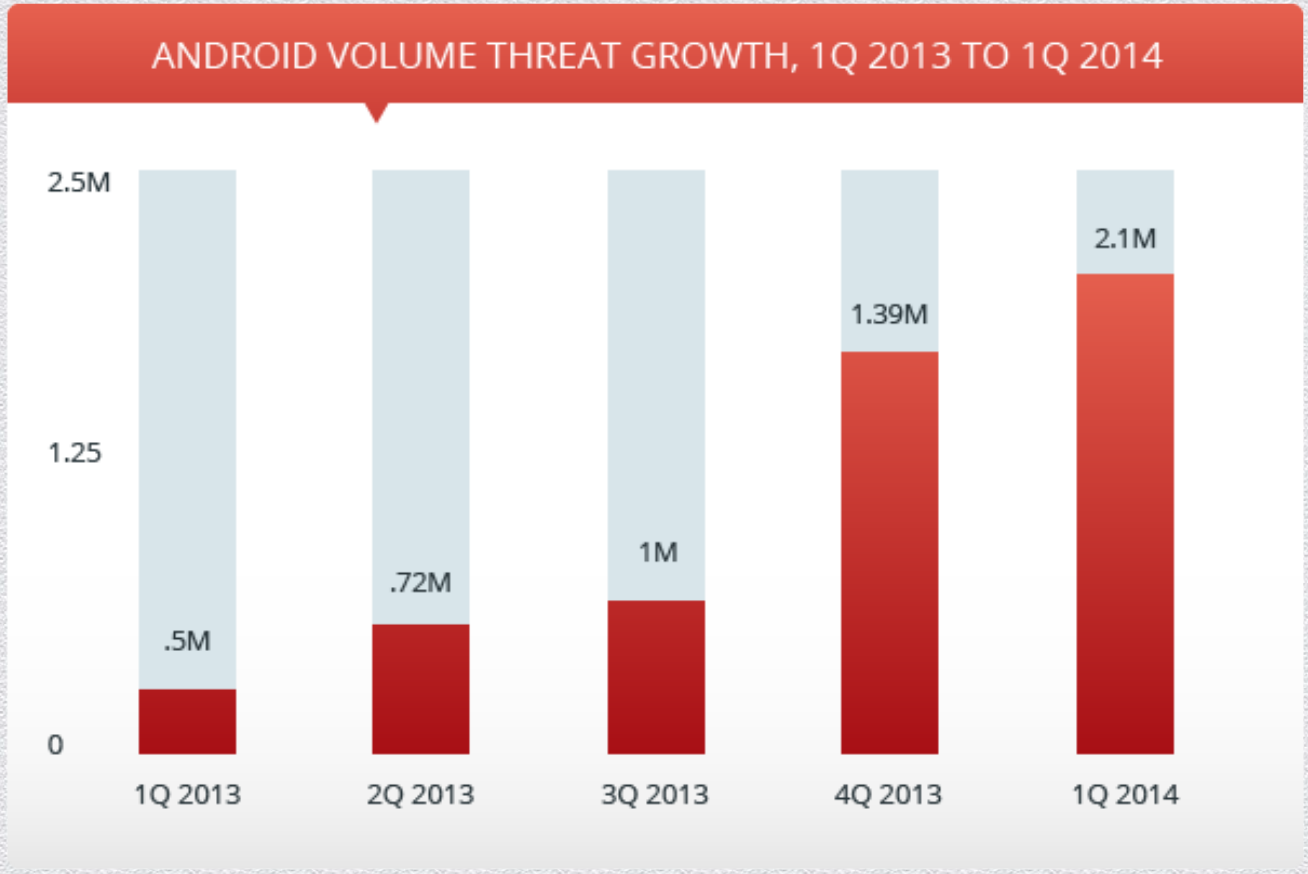
JUN 13

The case of a Kentucky man arrested this month for using mobile banking to steal thousands of dollars from a local supermarket chain highlights the security loopholes that thieves can exploit in mobile check deposit schemes being deployed by financial institutions across the country.

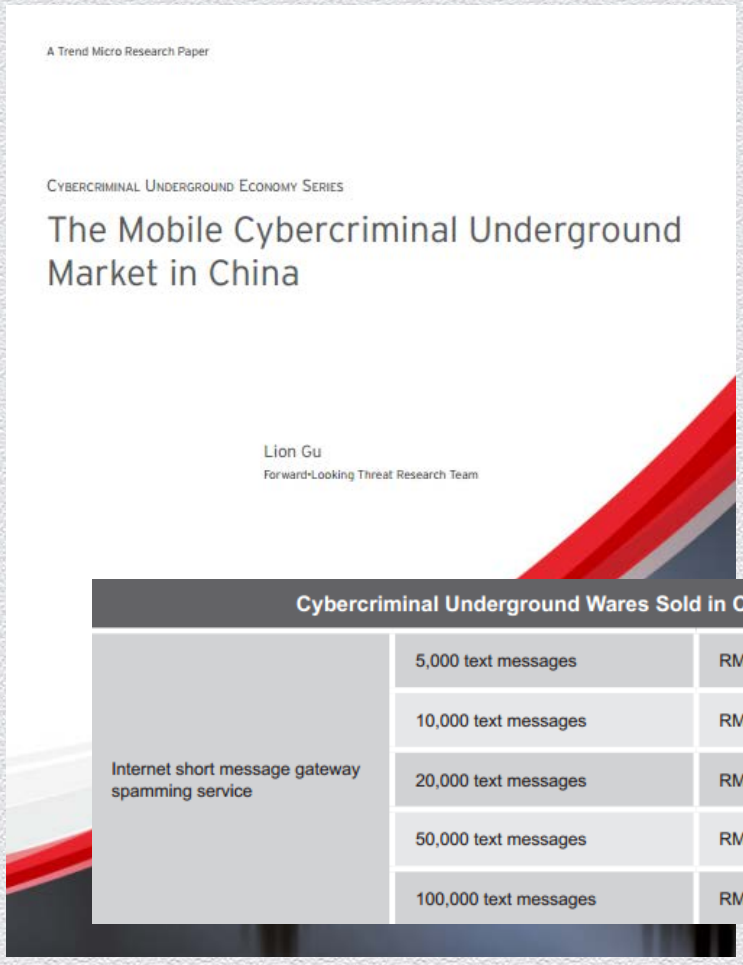
Louisville, Ky. based news station **WDRB Inc.** carried a story last week about a local man who was arrested after allegedly using mobile banking to steal more than $12,000 from multiple Kroger stores.


Everything is coming up mobile

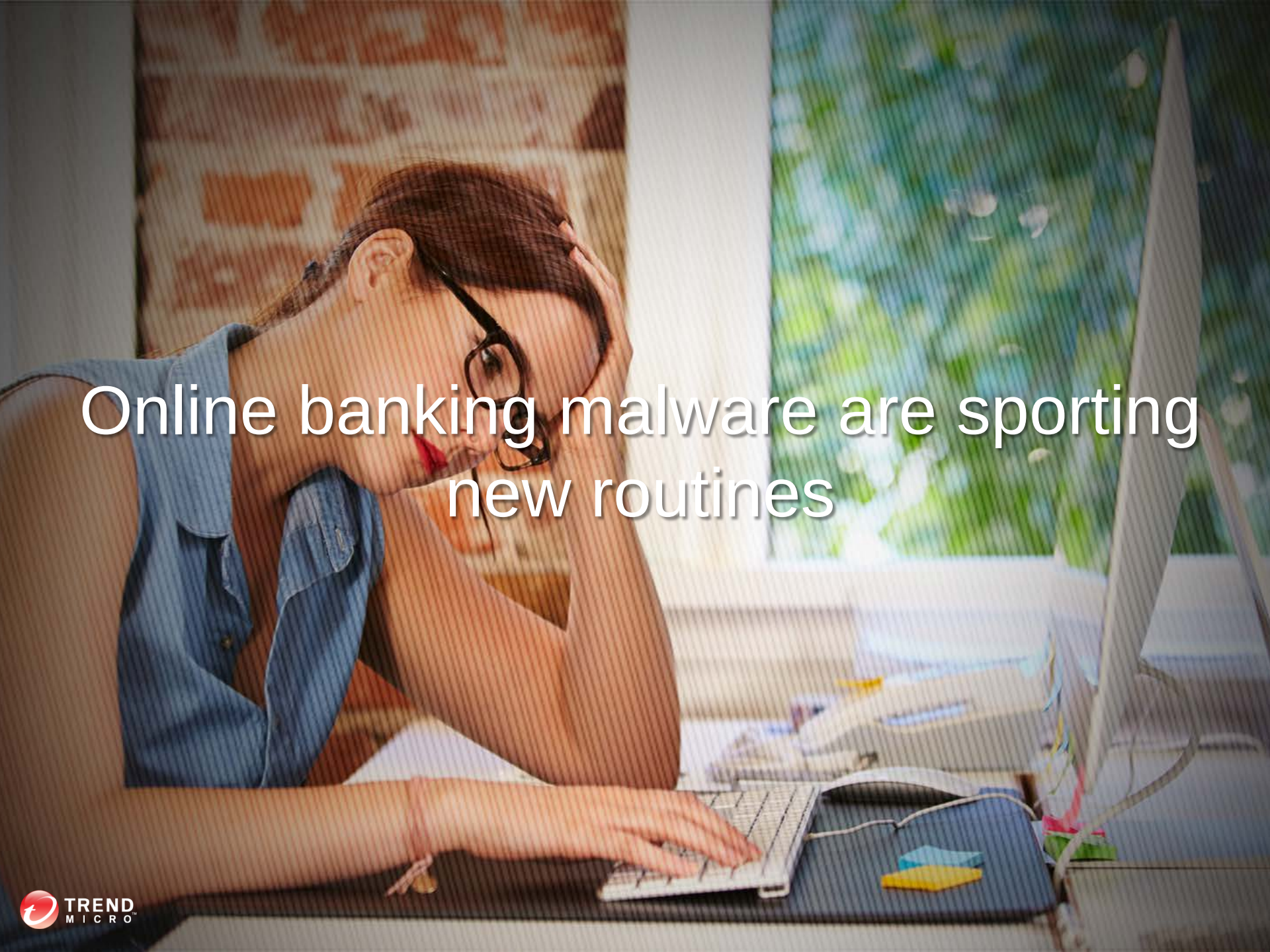
Android Threat Volume

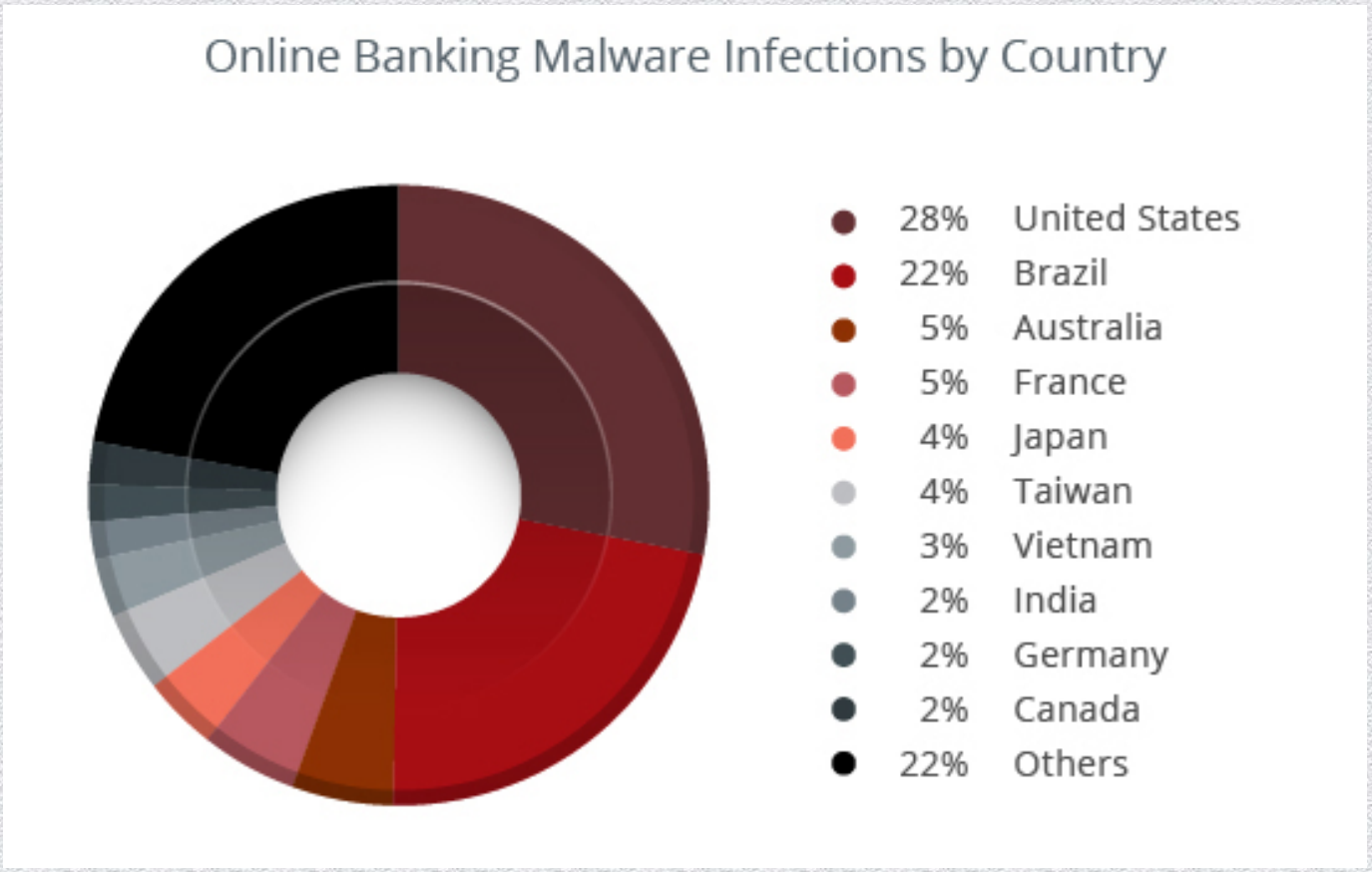


Mobile Cybercriminal Underground



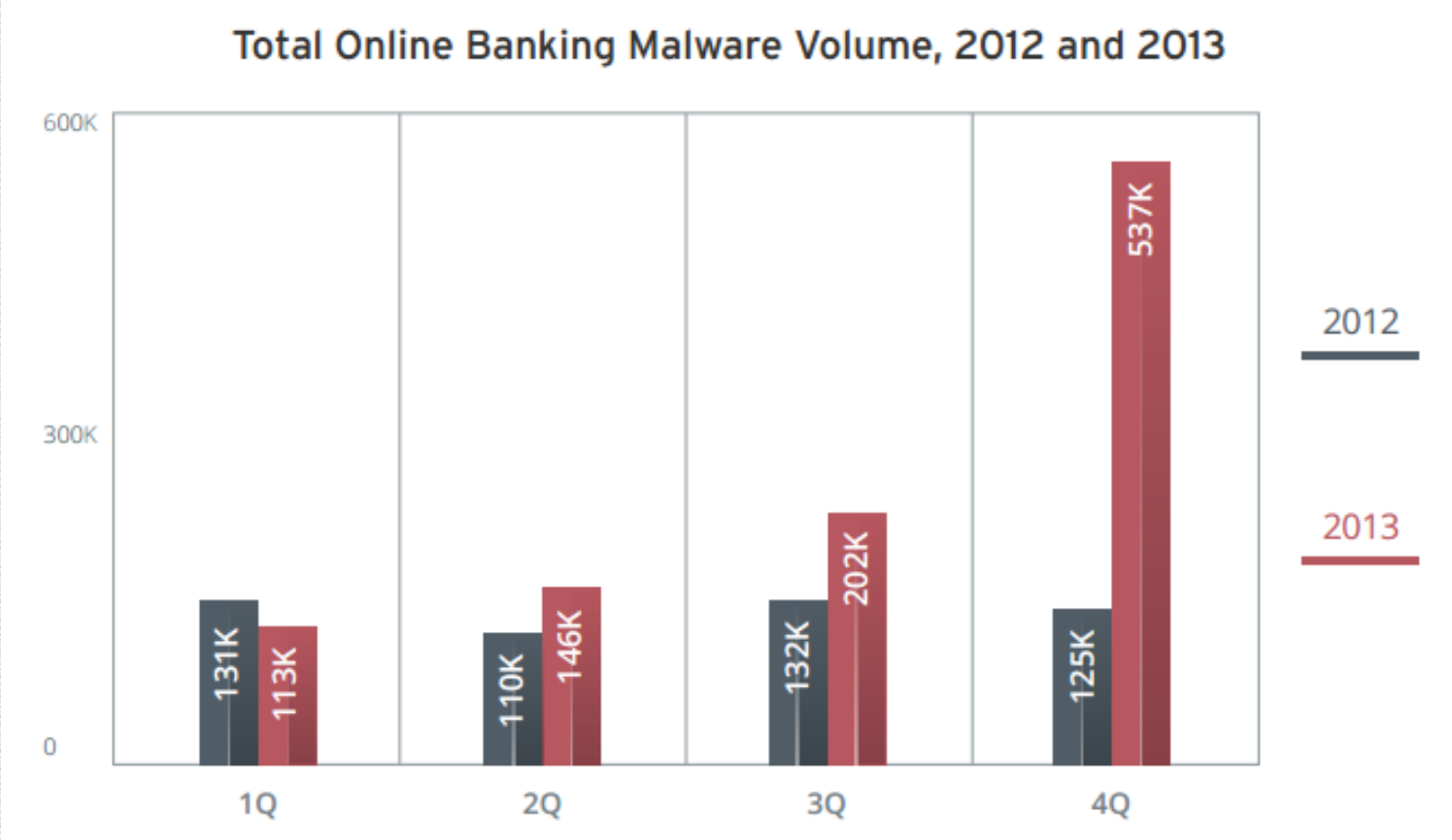
Cybercriminal Underground Wares Sold in China		
Internet short message gateway spamming service	5,000 text messages	RMB 300 (~US$50)
	10,000 text messages	RMB 400 (~US$65)
	20,000 text messages	RMB 700 (~US$115)
	50,000 text messages	RMB 1,500 (~US$250)
	100,000 text messages	RMB 2,800 (~US$460)


Online banking malware are sporting new routines



Online Banking Infections by Country

Based on 2013 Trend Micro Smart Protection Network Data



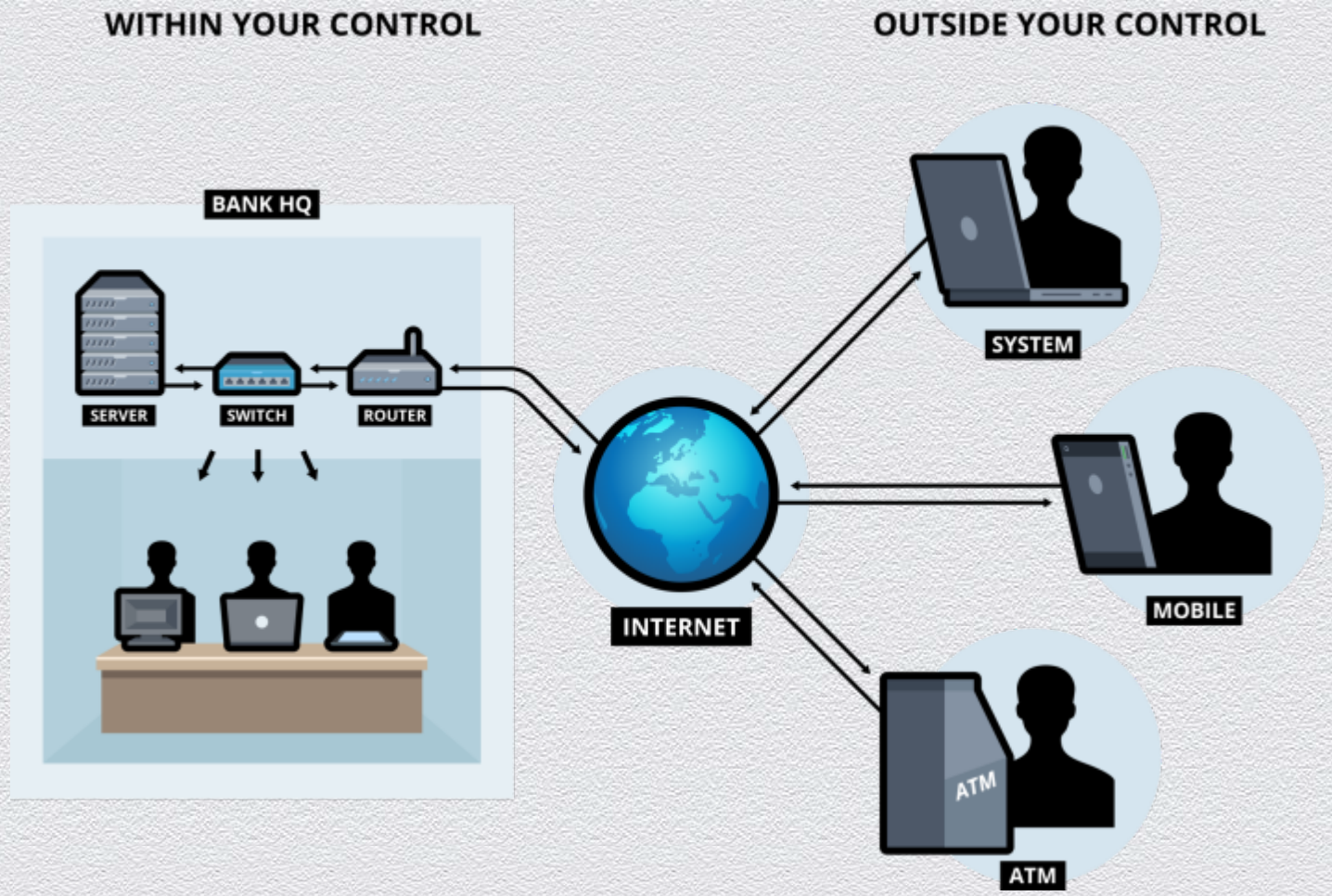
Total Online Banking Malware Volume 2012 vs. 2013

Based on 2013 Trend Micro Smart Protection Network Data

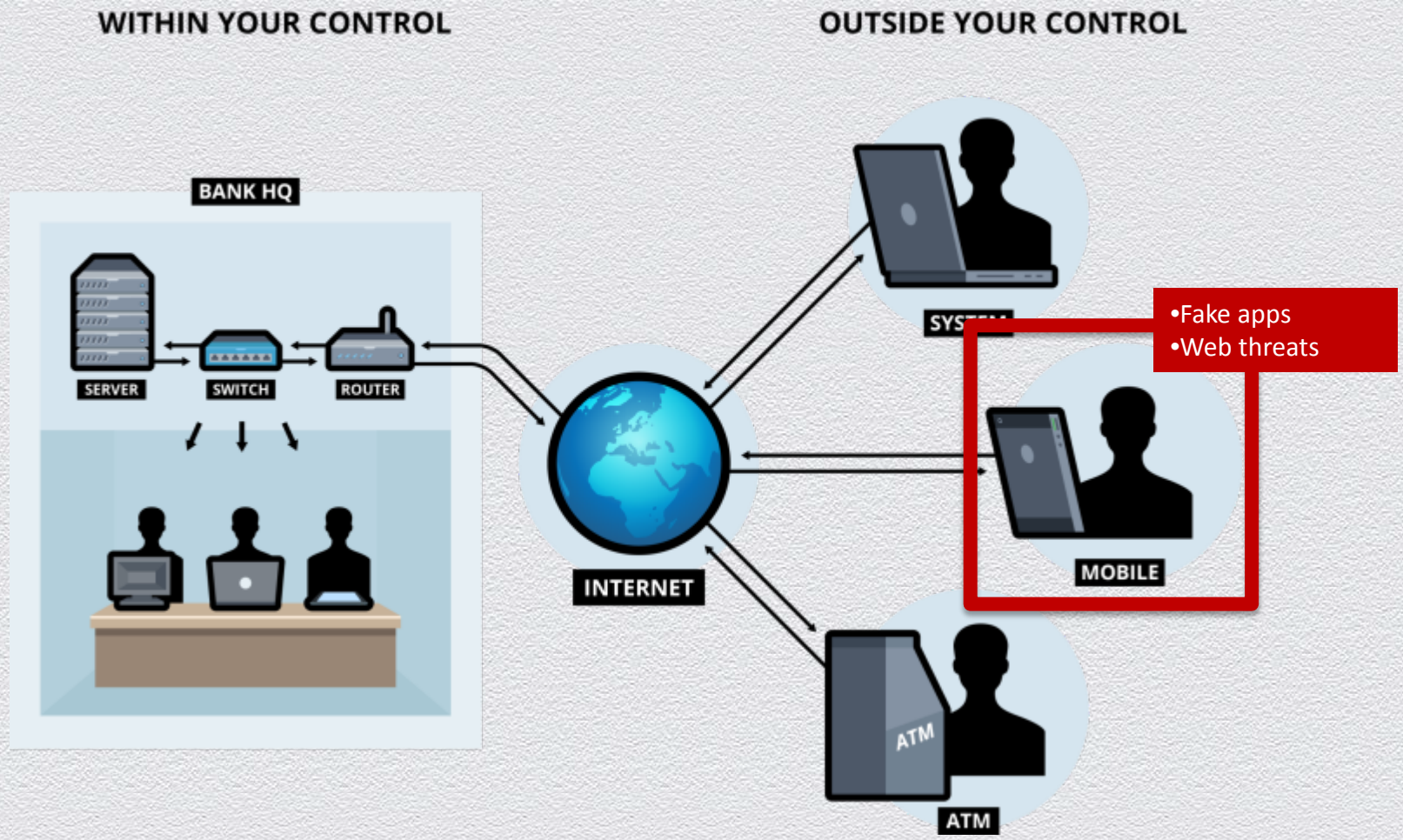

Mobile + Banking = A Perfect Storm

Security Risks in Mobile Banking

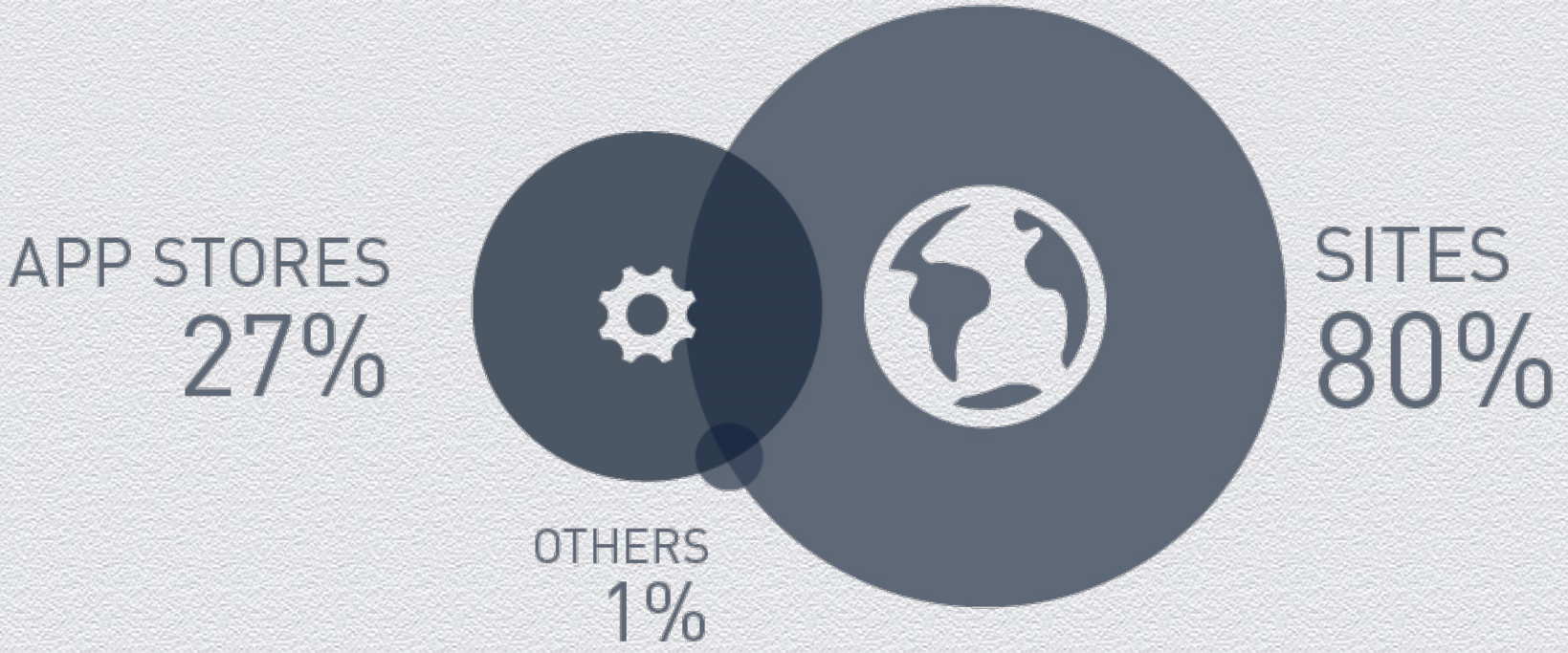
Entry Points for Security Threats



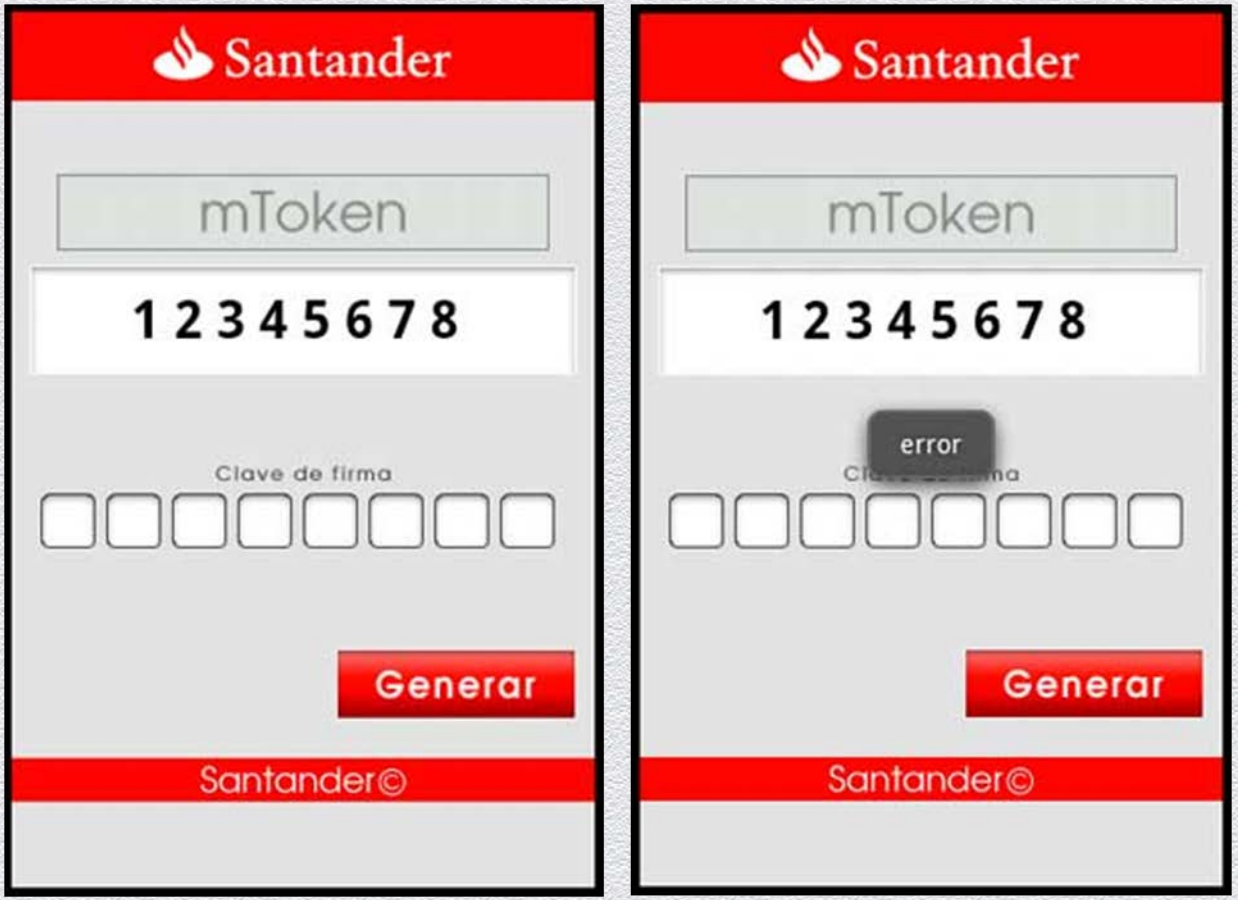
Entry Points for Security Threats



Where Users Stumble Upon Malicious Apps

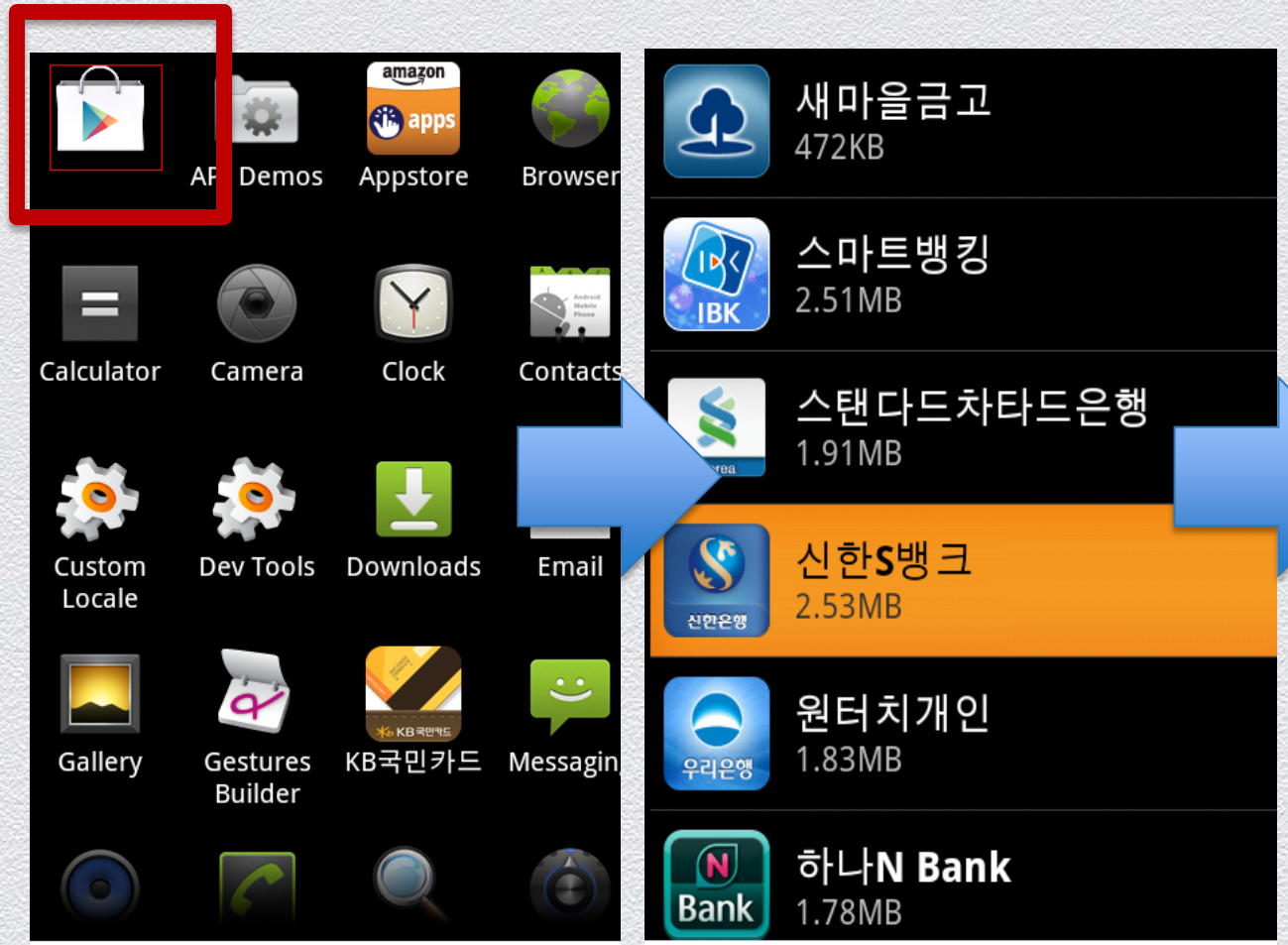


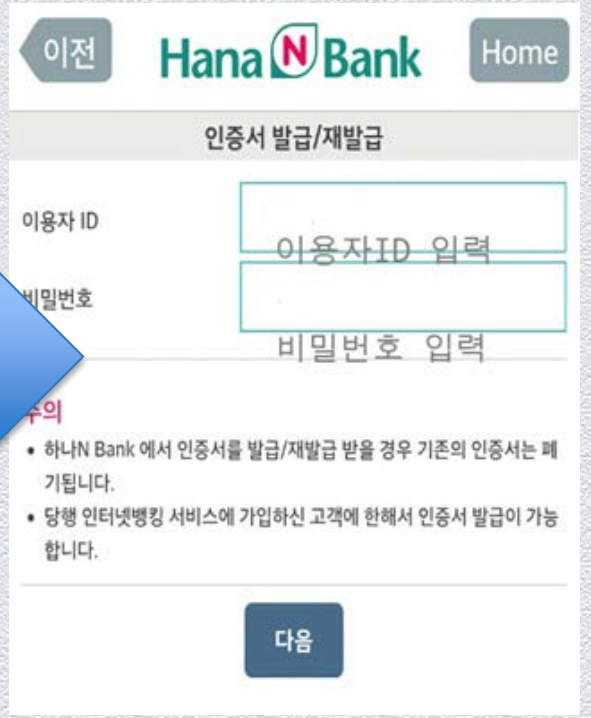
Fake Banking Apps



- Fake token generator app steals bank password and sends user and device information (e.g., SMS, contact lists, etc.) to a remote server.

Fake Banking Apps





“Trojanized” Banking Apps

InformationWeek
DARKReading CONNECTING THE INFORMATION SECURITY COMMUNITY

Home | News & Commentary | Authors | Slideshows | Video | Radio | Reports | White Papers | Ev

ATTACKS/BREACHES | APP SEC | CLOUD | ENDPOINT | MOBILE | PERIMETER | RIS

VULNERABILITIES / THREATS

8/6/2013
10:58 AM

Mathew J. Schwartz
News

Connect Directly

4 COMMENTS

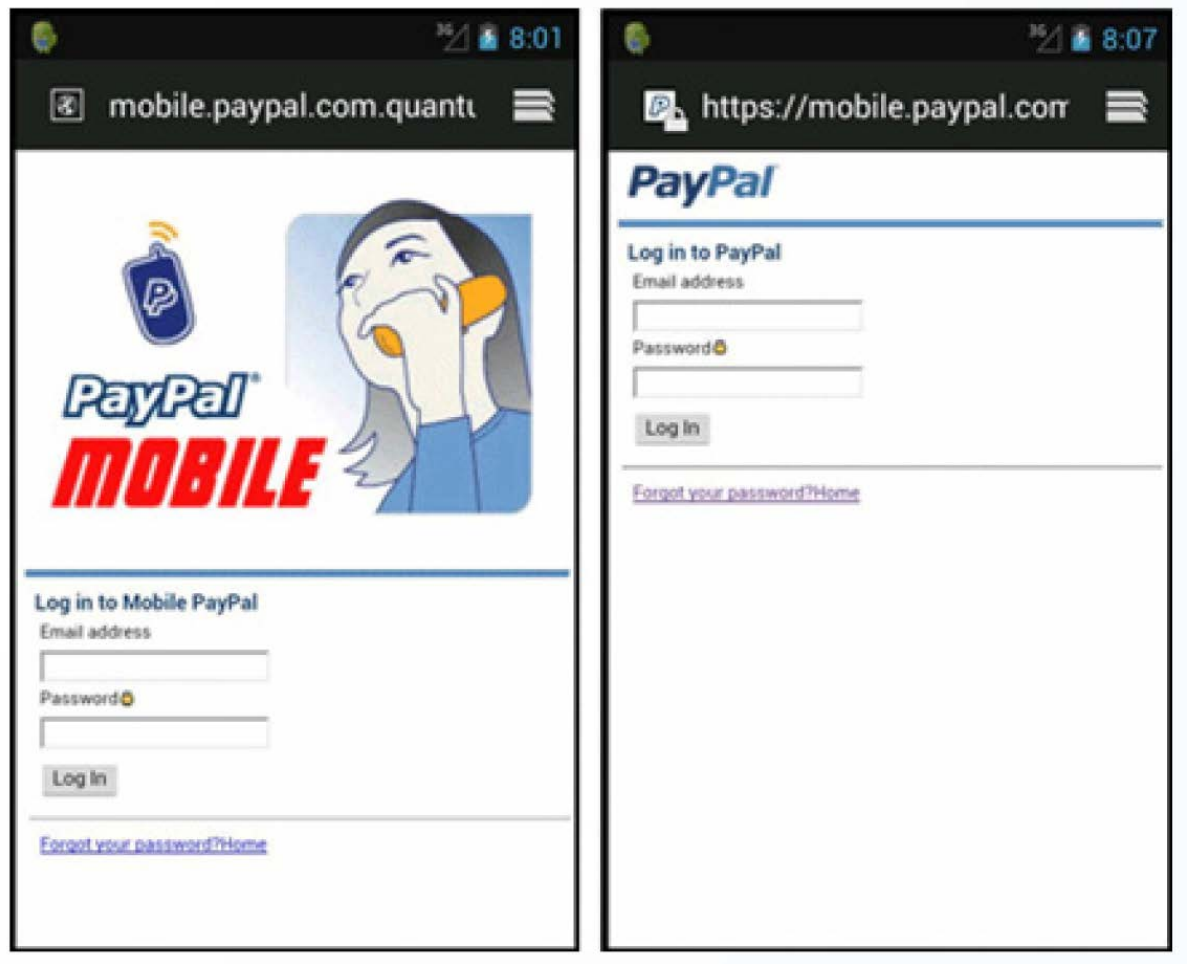
Android Trojan Banking App Targets Master Key Vulnerability

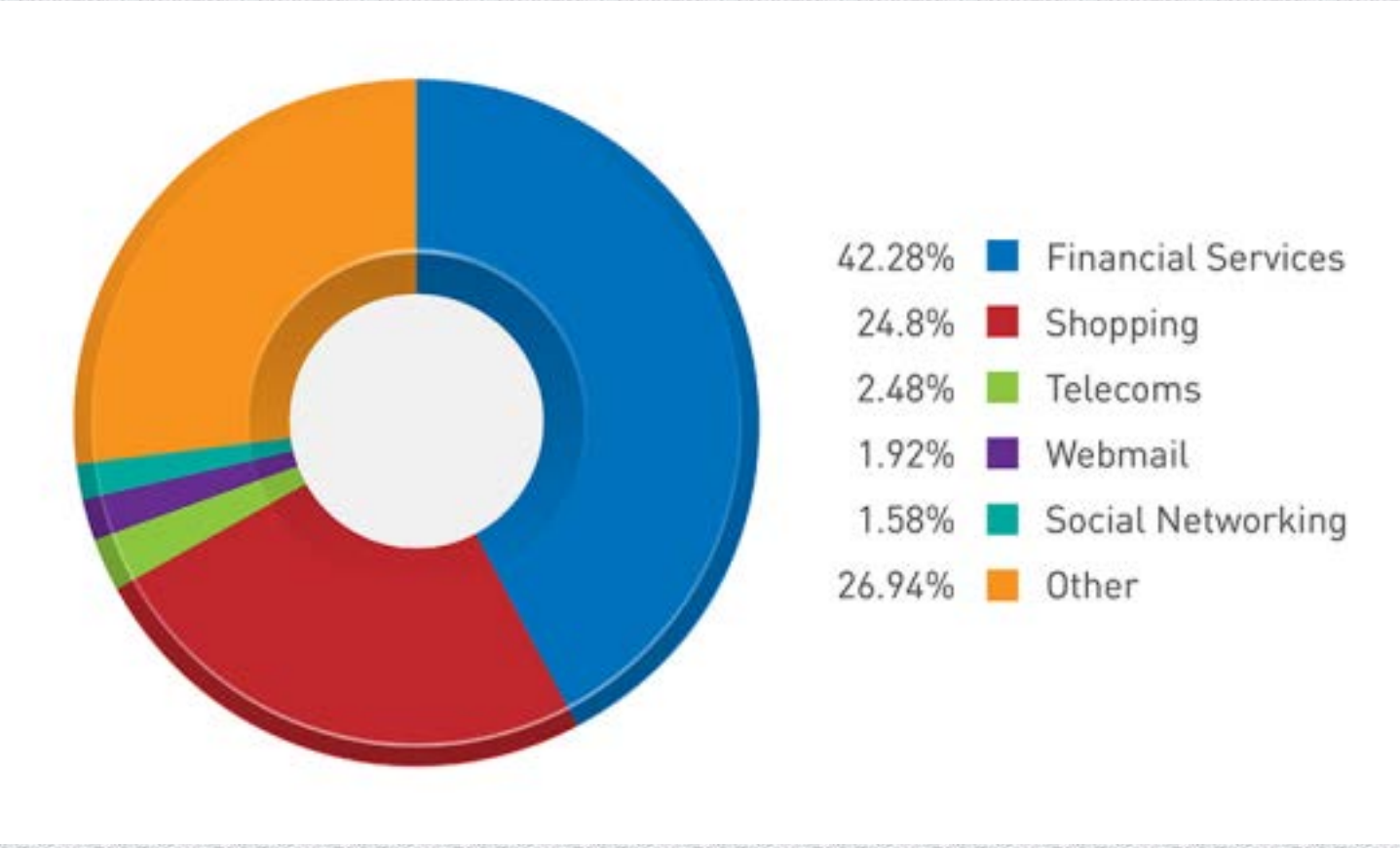
Sluggish Android updates put users at risk. Could rising public awareness of the flaw lead carriers and device makers to patch more quickly?

Security researchers have spotted a legitimate banking app for Android smartphones and tablets that has been "trojanized" using the so-called master key vulnerability. That flaw, which affects all versions of Android prior to version 4.2.2, can be used by attackers to inject malicious code into a digitally signed, legitimate Android app.


Apps are just one piece of the puzzle. Threats continue to transition from PC to mobile with help from malicious URLs.
Facebook
Twitter
Messenger

Mobile Phishing



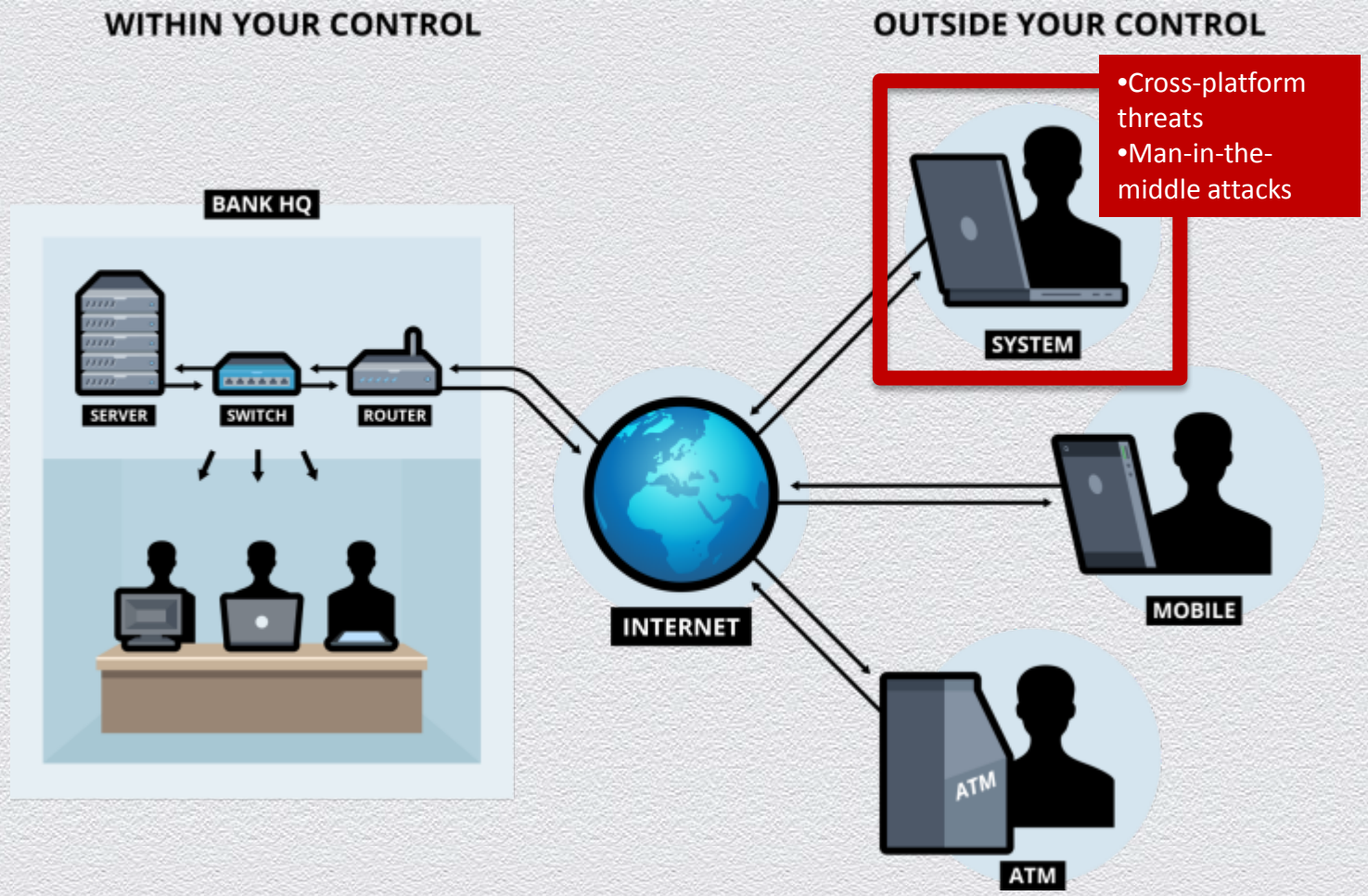


Distribution of Mobile Phishing URLs

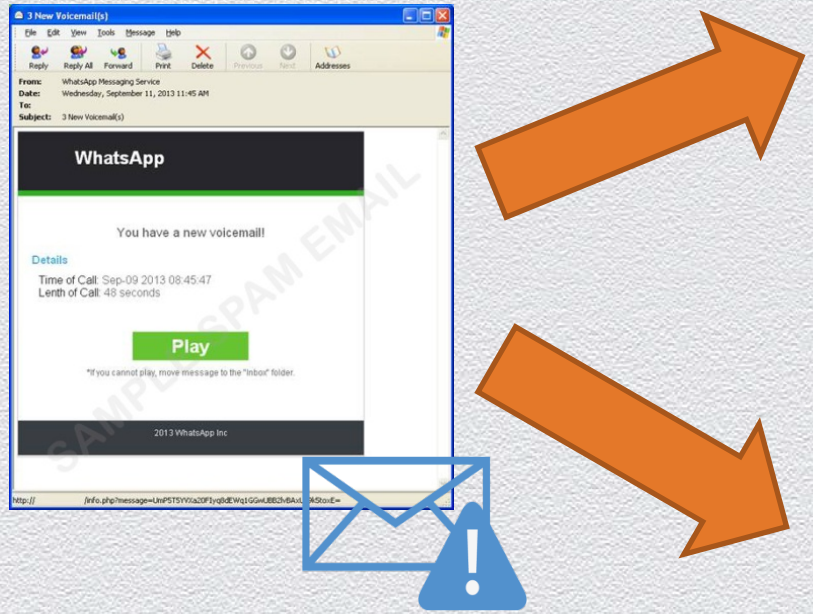
More than 40% of mobile phishing sites target financial services

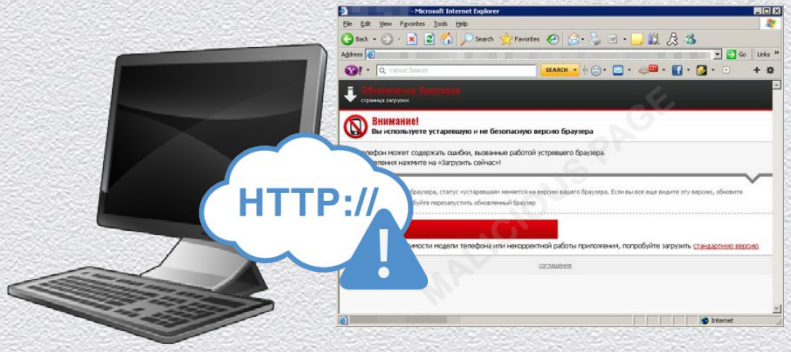
Mobile Phishing

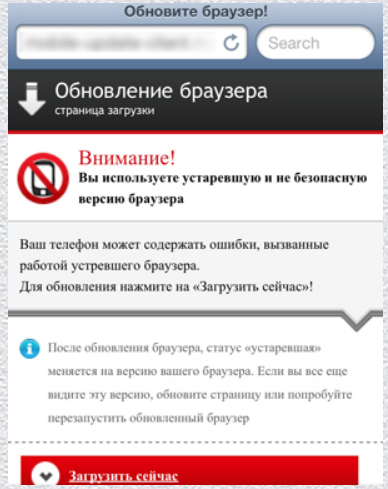
Entry Points for Security Threats



Cross-Platform Threats





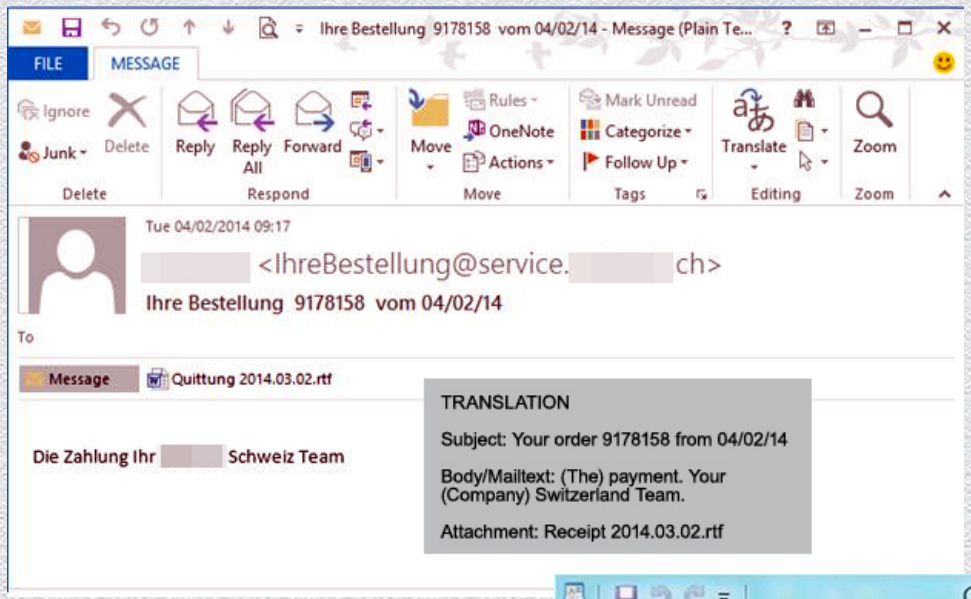


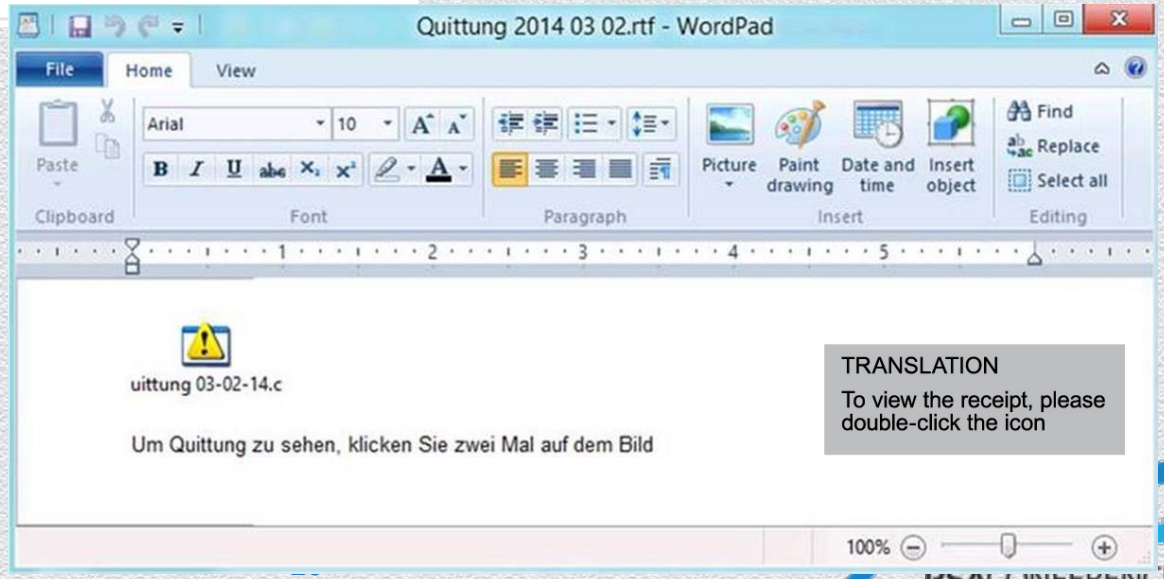
Cross-Platform Threats

Man-in-the-Middle Attacks

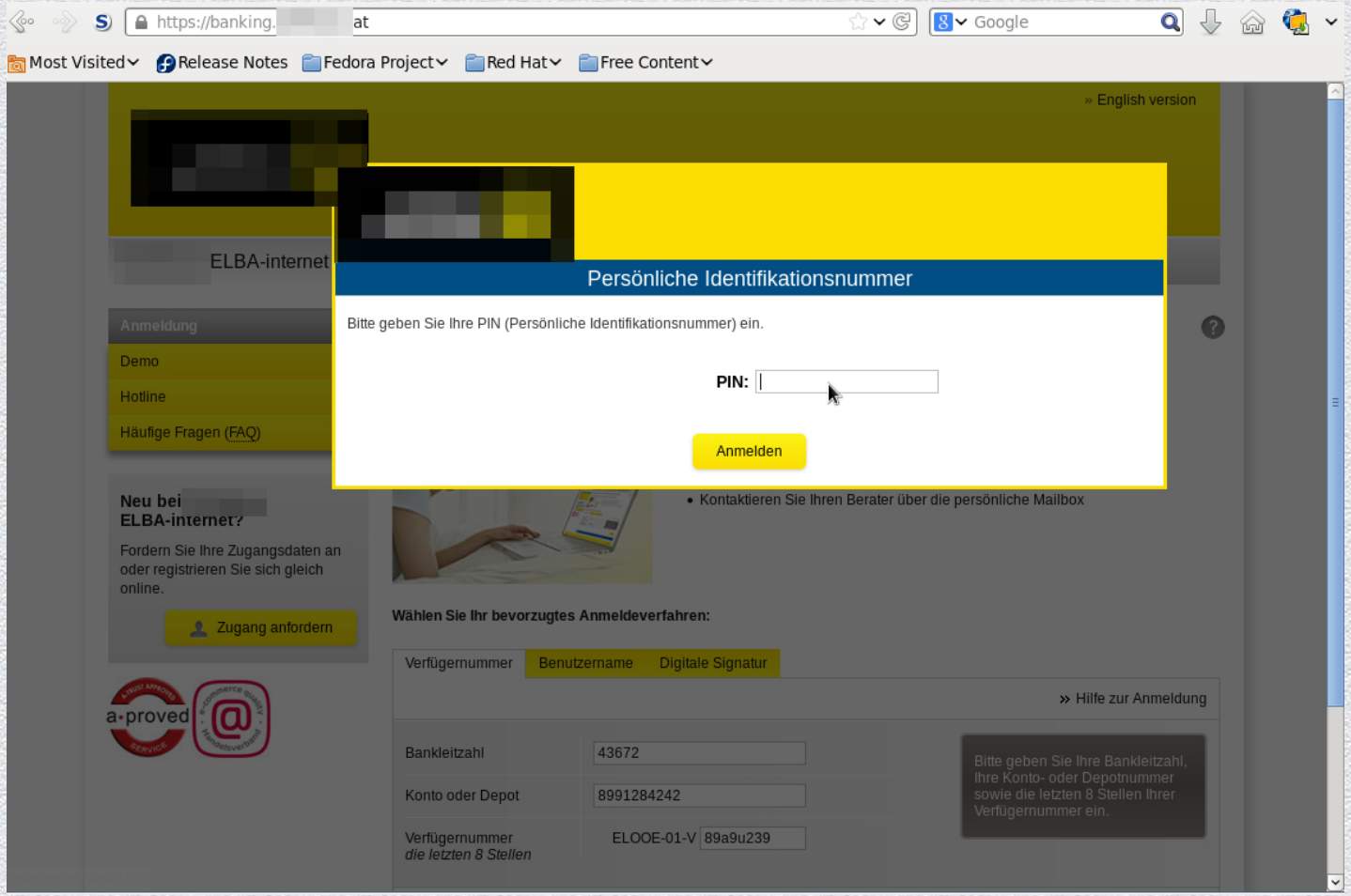
ZITMO and PERKEL

Operation Emmental

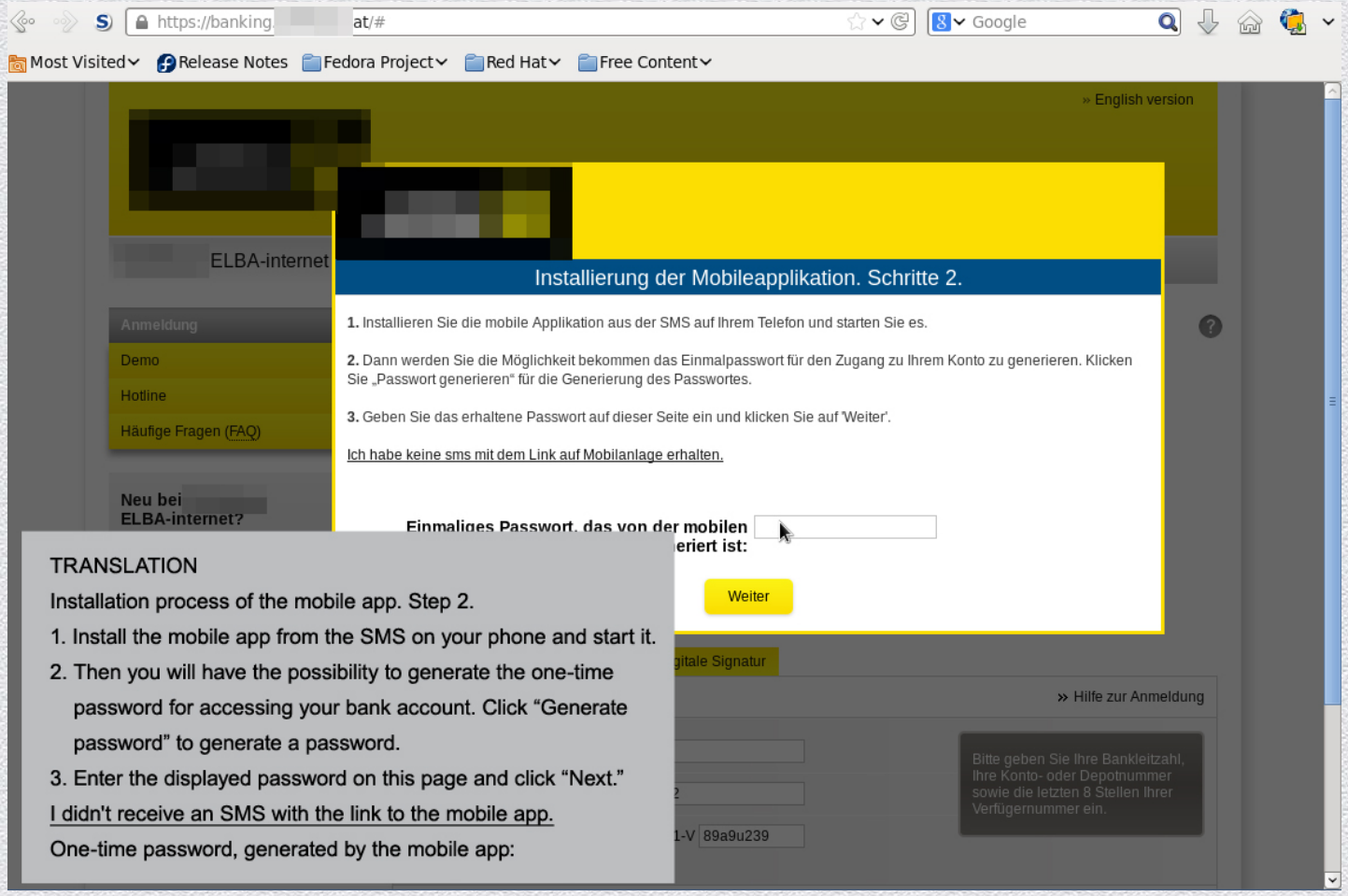




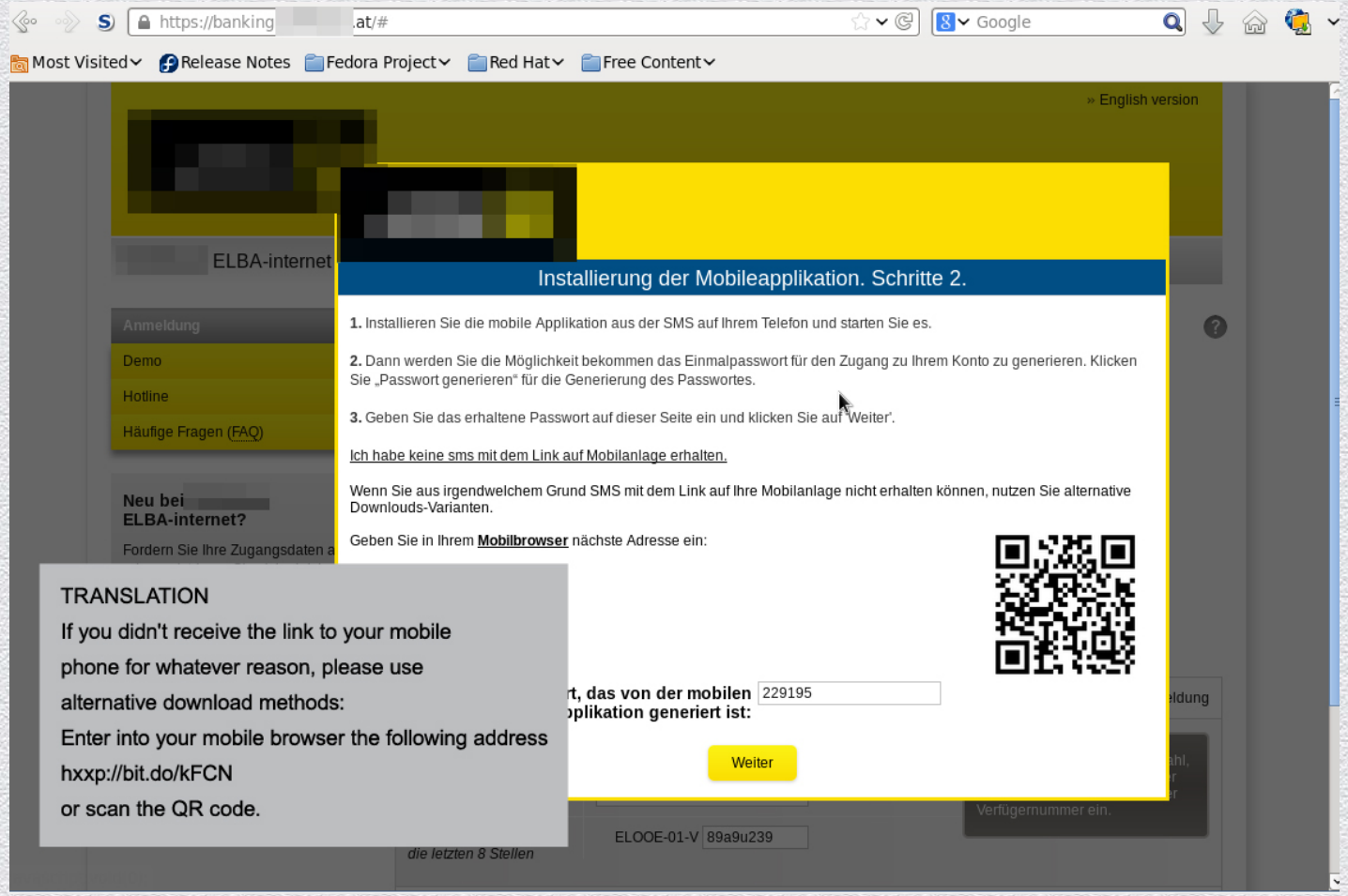
Operation Emmental



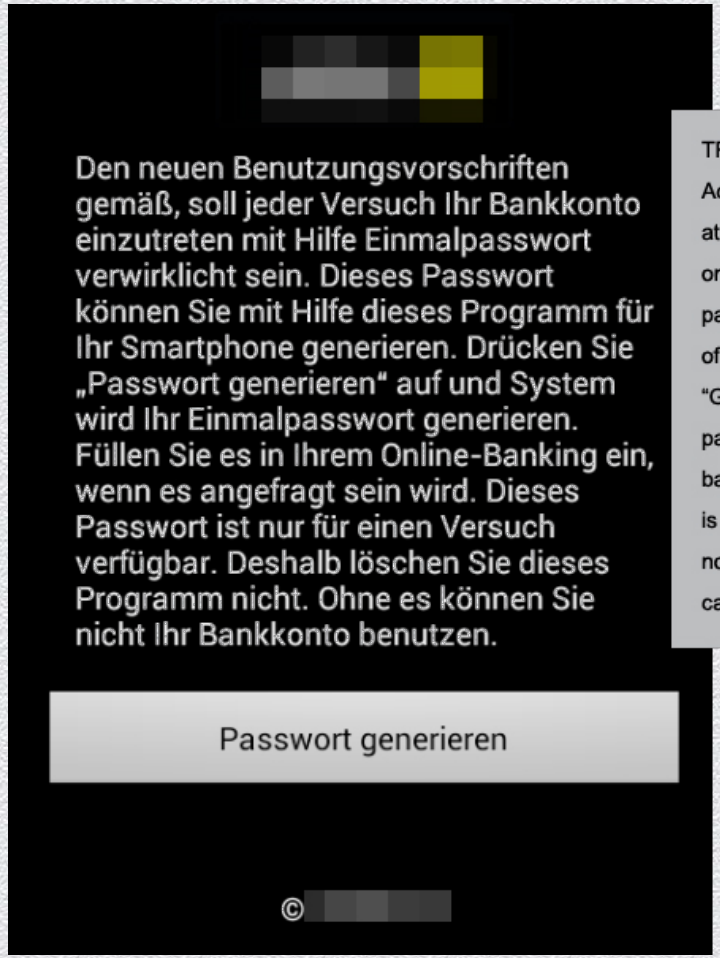
Operation Emmental



Operation Emmental



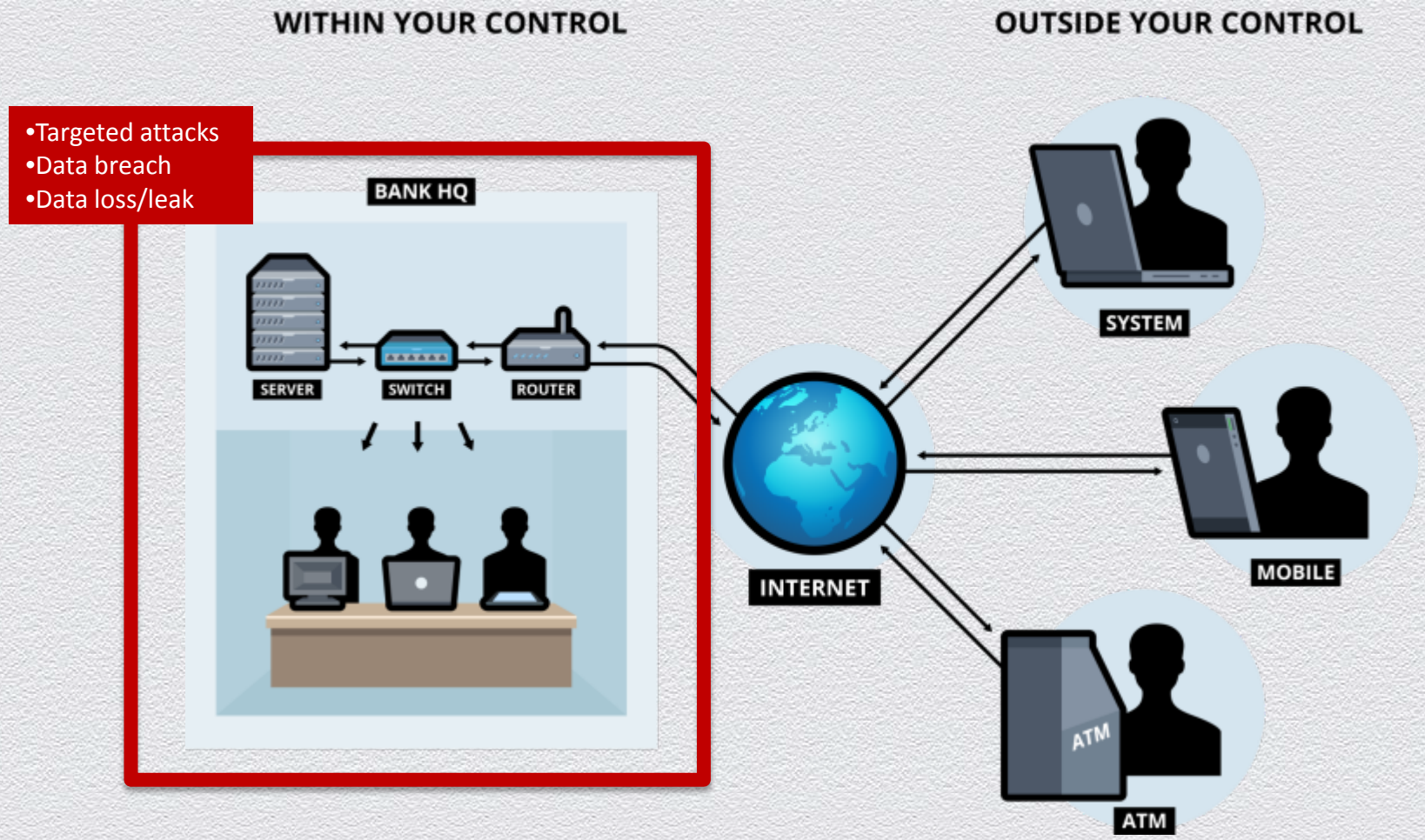
Operation Emmental



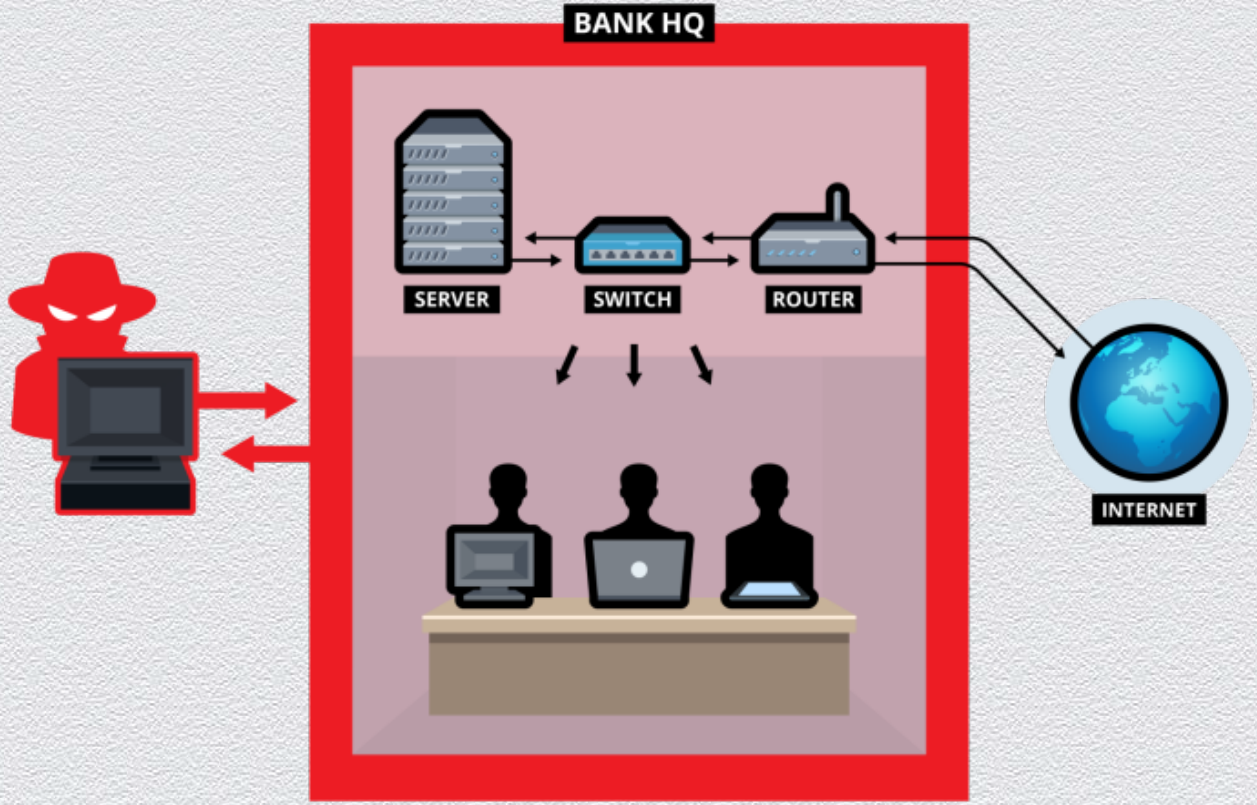
TRANSLATION

According to the new policy, for every attempt to log into your bank account a one time password is needed. This password can be generated with the help of this app on your smartphone. Click on "Generate password" to generate a password. Enter it into your online banking, if asked to do so. The password is only valid for one attempt. Therefore do not delete this app. Without this app you cannot use your online banking anymore.

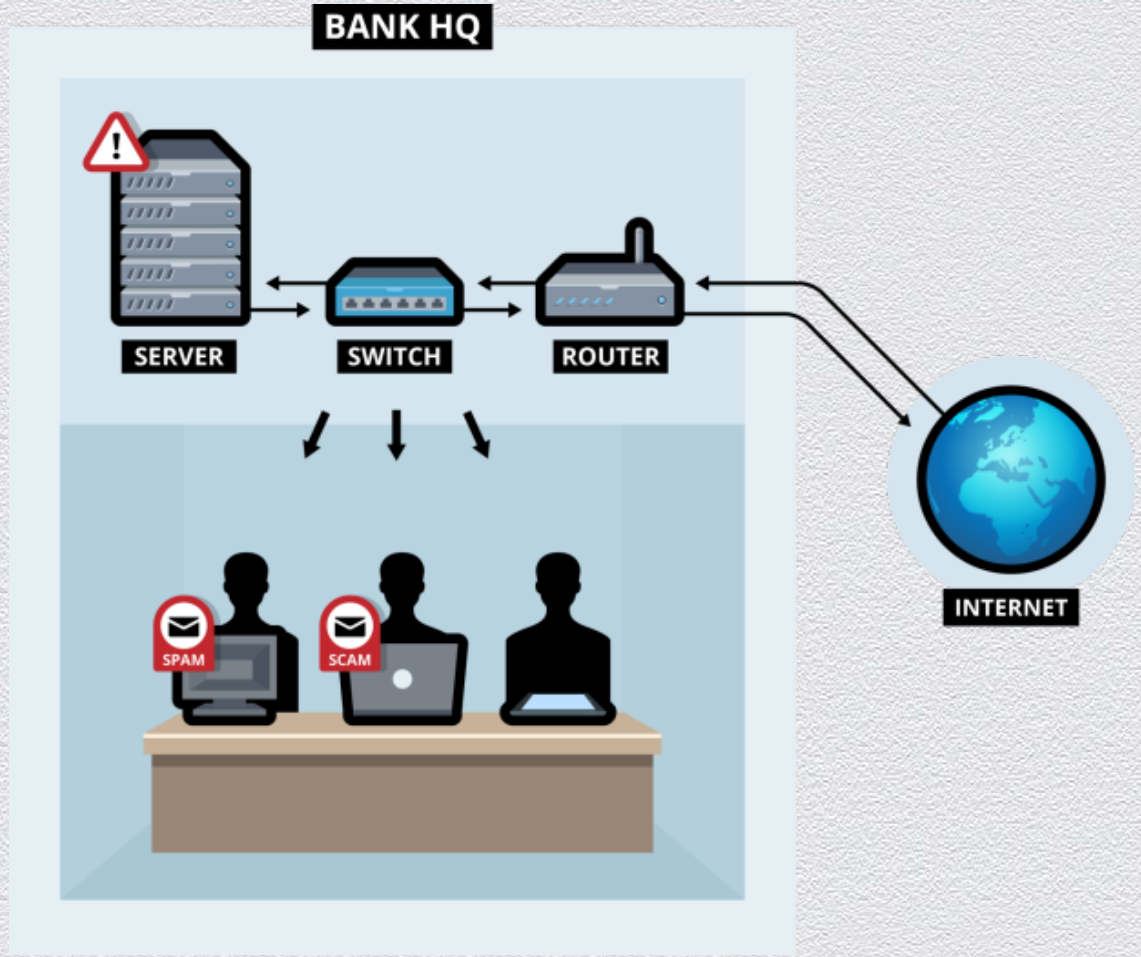
Entry Points for Security Threats



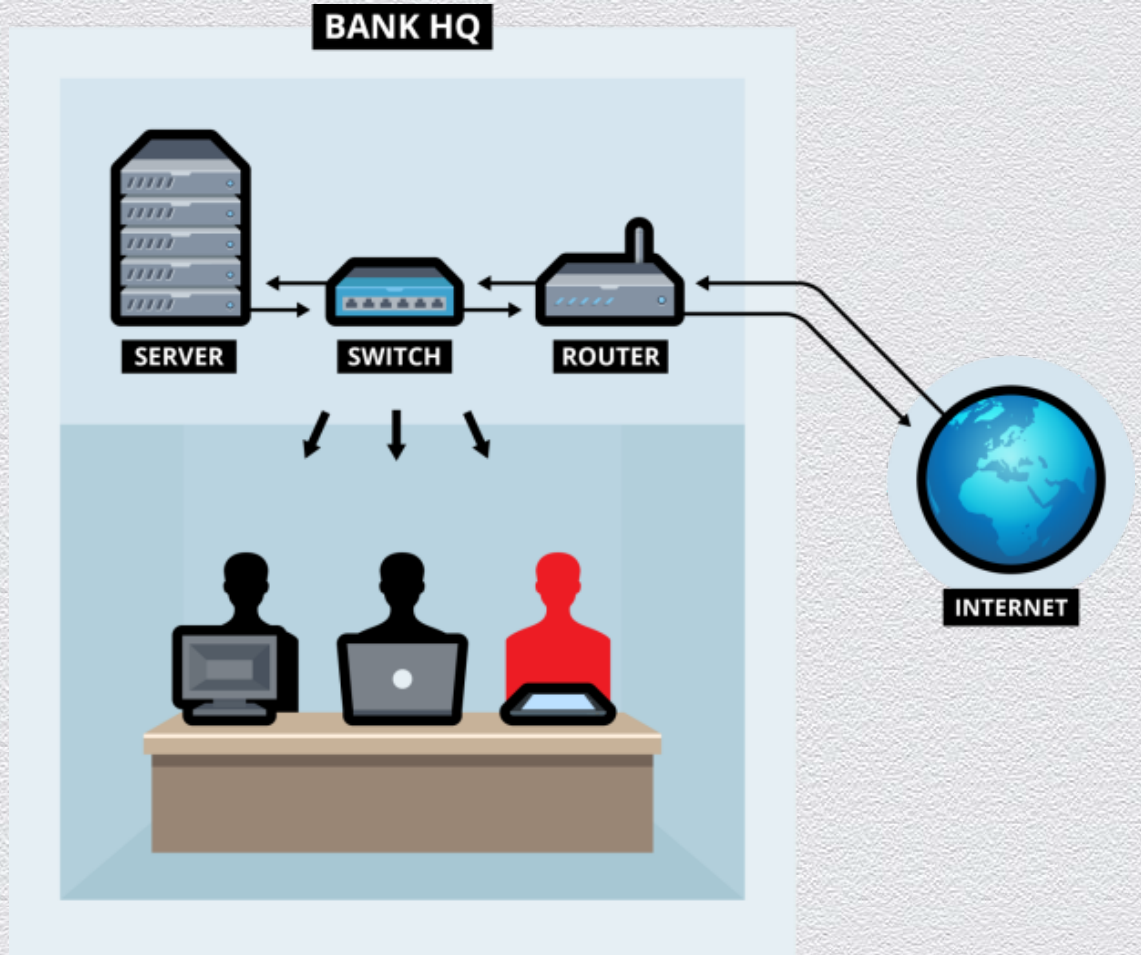
Security Threats to Enterprises: Targeted Attacks



Security Threats to Enterprises: Data Breach



Security Threats to Enterprises: Data Leak/Loss



InformationWeek
DARKReading CONNECTING THE INFORMATION SECURITY COMMUNITY

Home | News & Commentary | Authors | Slideshows | Video | Radio | Reports | White Papers | Ev

ATTACKS/BREACHES | APP SEC | CLOUD | ENDPOINT | MOBILE | PERIMETER | RIS

VULNERABILITIES / THREATS

12/12/2013
08:10 PM

Kelly Jackson Higgins
News

Connect Directly

0 COMMENTS
COMMENT NOW

Weak Security In Most Mobile Banking Apps

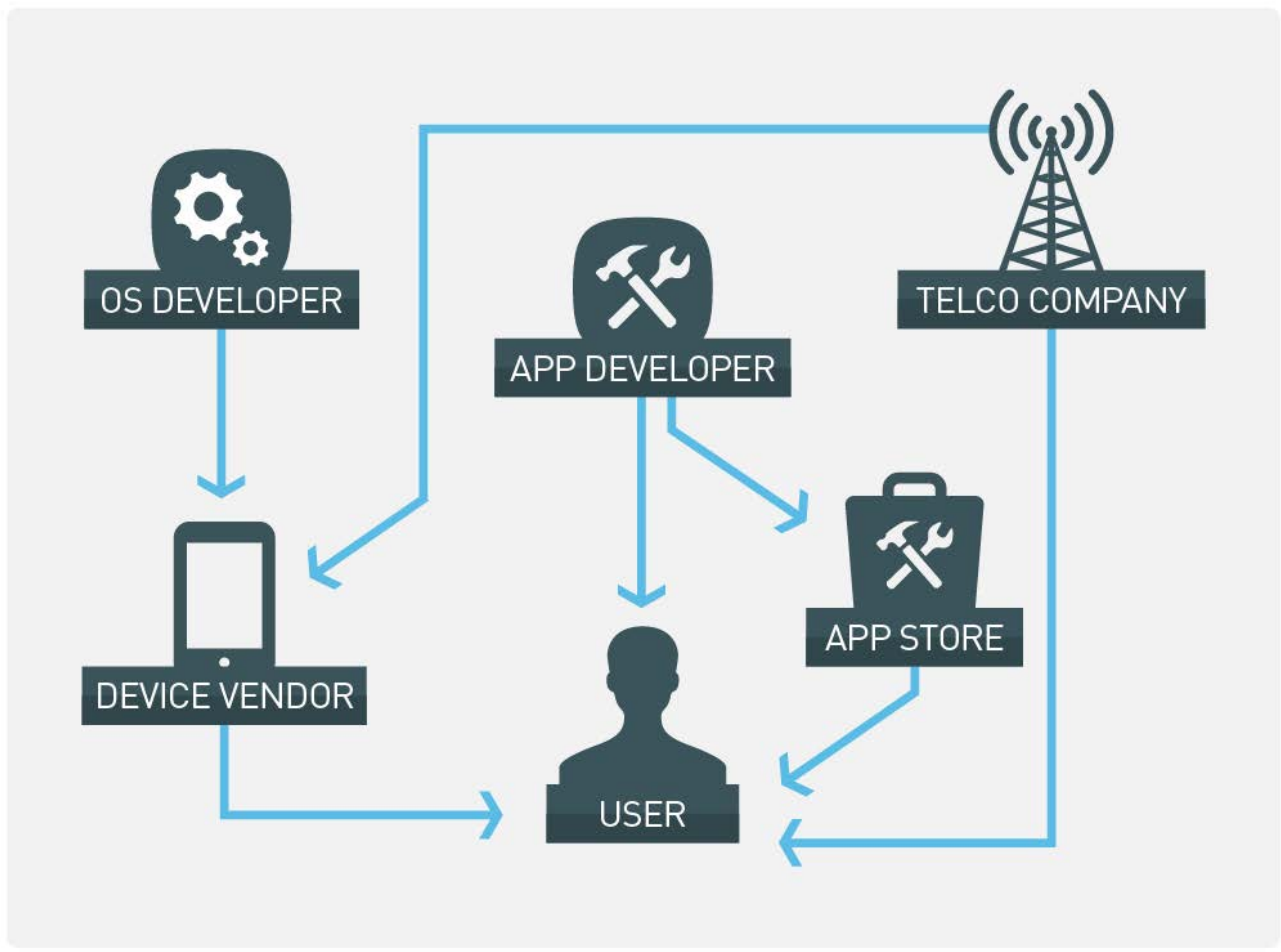
Eight of 10 iOS, Android mobile banking apps are improperly configured, new report says

Most mobile banking apps -- including those of major financial institutions -- contain configuration and design weaknesses that leave them with weakened security.

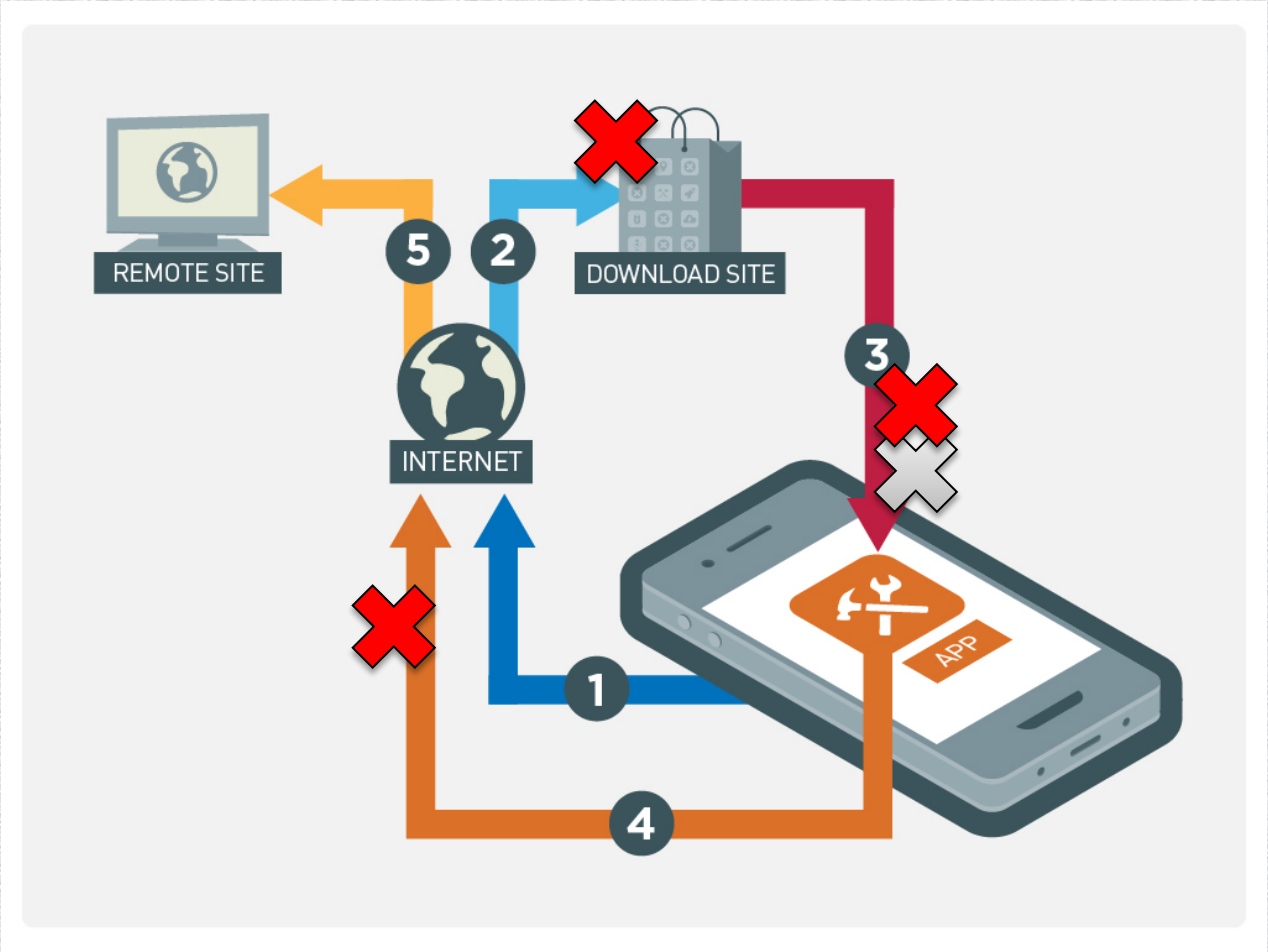
Security experts this month tested 275 Apple iOS- and Android-based mobile banking apps from 50 major financial institutions, 50 large regional banks, and 50 large U.S. credit unions. Overall, they found that eight out of 10 apps were improperly configured and not built using best practices software development. Among the big-name banks whose mobile apps were tested by security firm Praetorian include Bank of America, Citigroup, Wells Fargo, Goldman Sachs, Morgan Stanley, Capital One Financial, and Suntrust Banks. Praetorian did not disclose how each bank's apps fared in the tests.

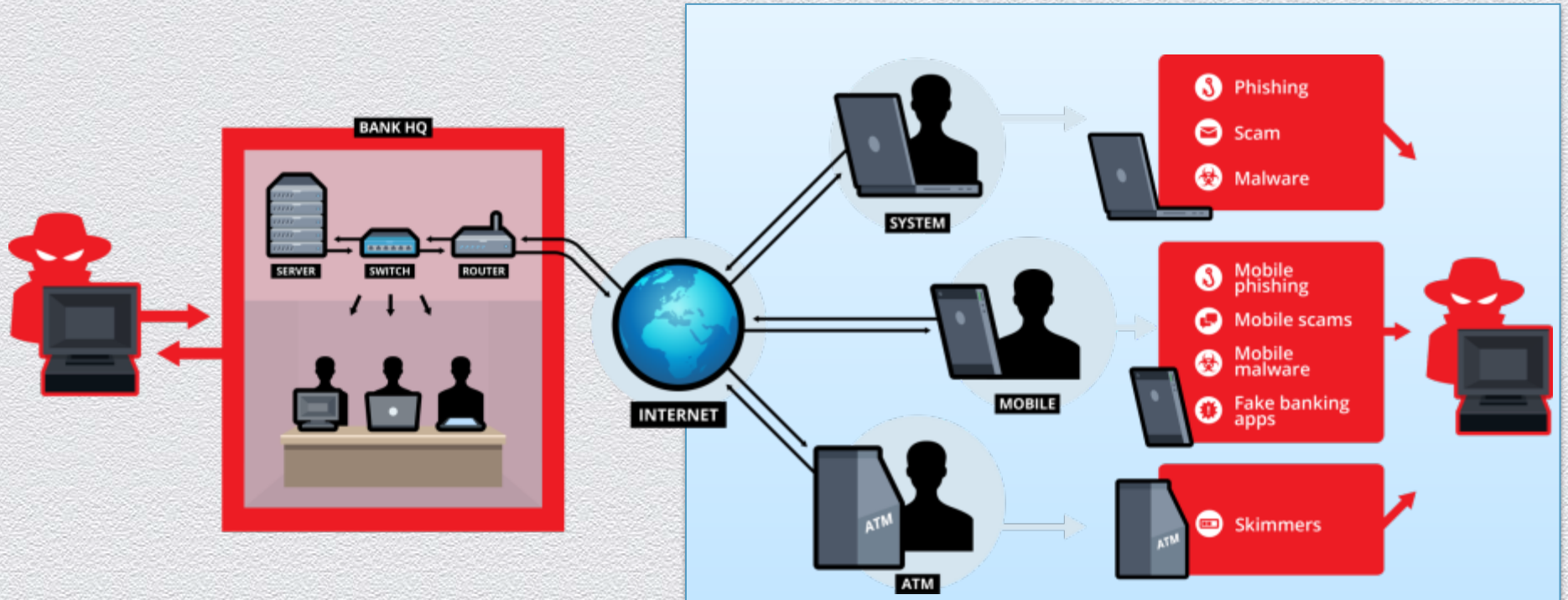
Best Practices and Recommendations

Securing the Mobile Ecosystem

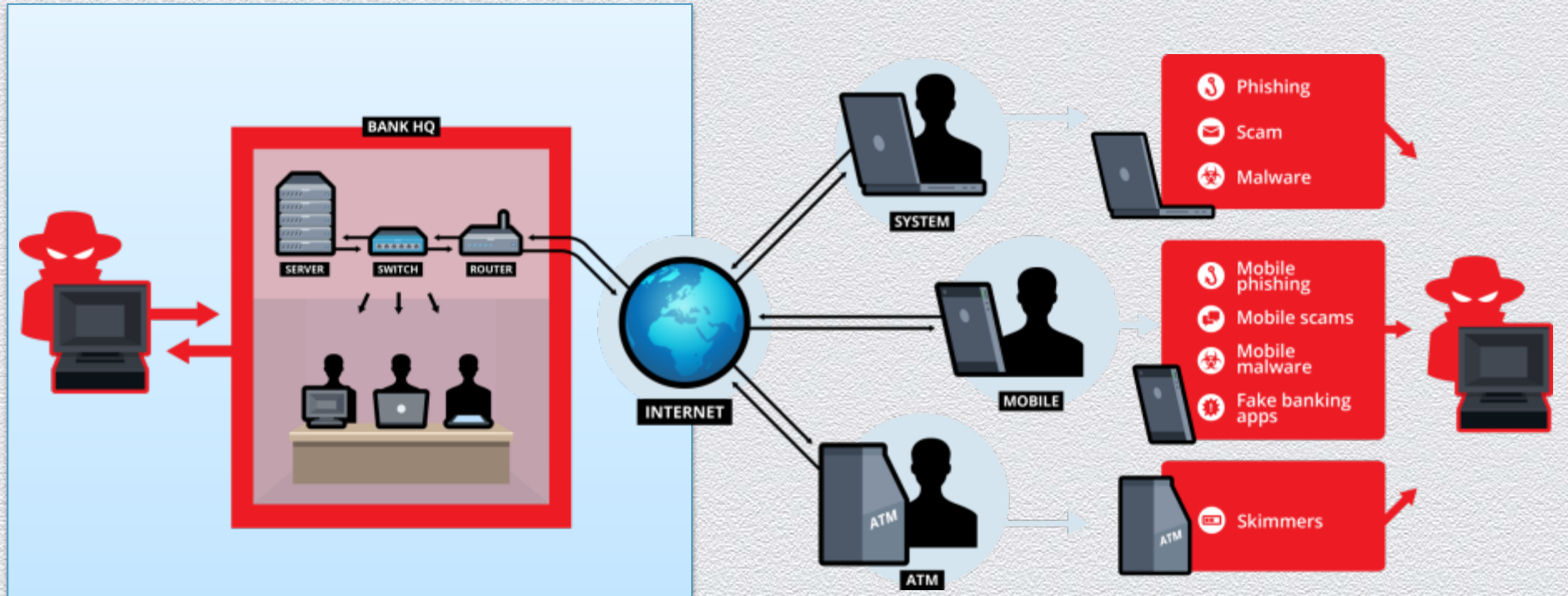


Addressing Threats at the Exposure Layer





1. Customer Advisory:
   - Use of security software
   - Update/Patch systems
   - Social engineering watch
2. Two-Factor Authentication



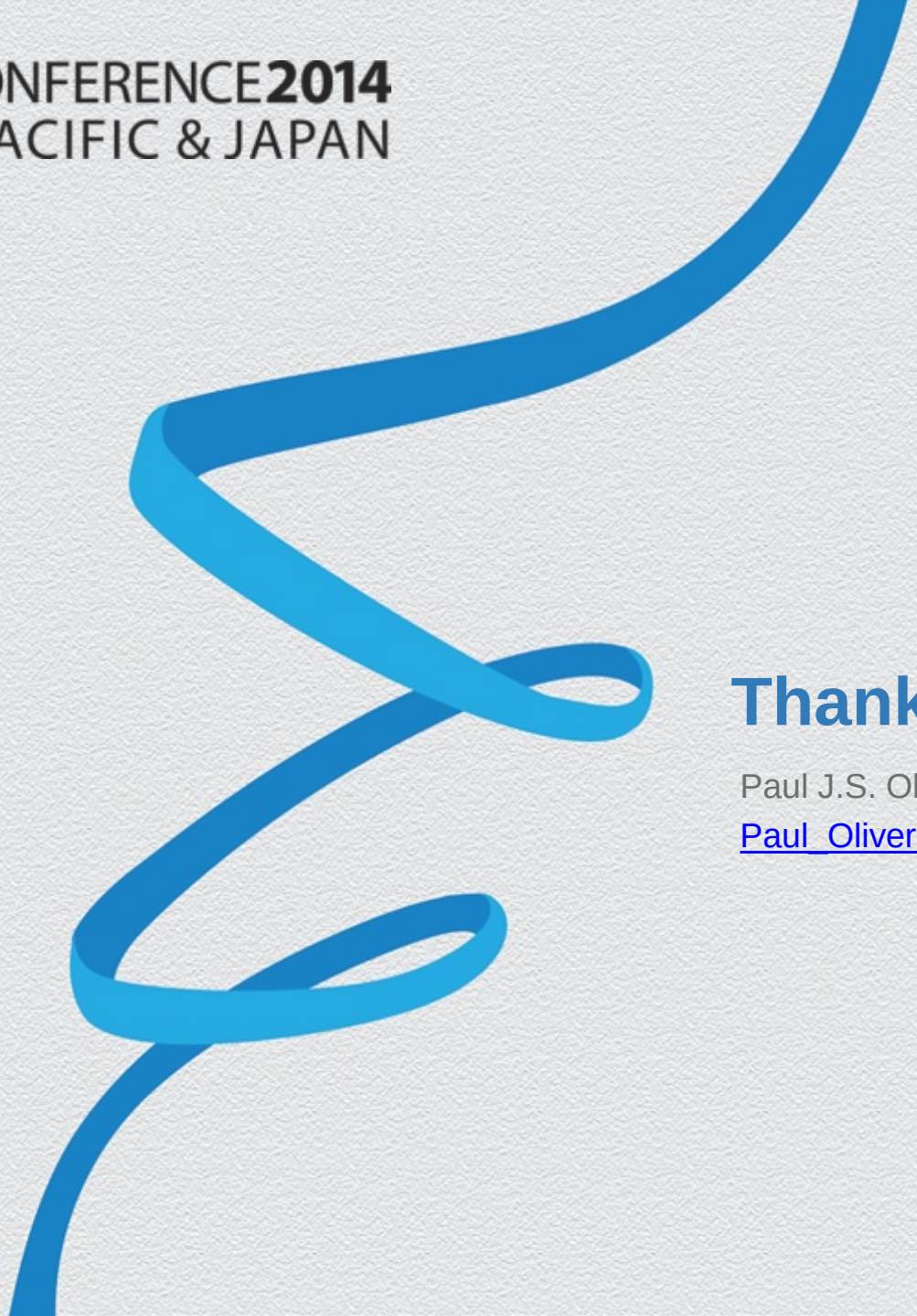
1. Virtual Patching
2. Custom Defense
3. Employee awareness and education

Summary

- Everything is going mobile, including online banking cybercrime
- Online banking threats continue to evolve, and may even render “traditional” security measures useless
- Securing the mobile ecosystem against online banking threats needs to be a collaborative effort


If history is repeating, it’s better to repeat the good side of it

RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN



Thank You!

Paul J.S. Oliveria
Paul_Oliveria@trendmicro.com