Minimizing the Threat of Mobile Banking Cybercrime

SESSION ID: MBS-T10

Paul J.S. Oliveria
Technical Communications Manager
Trend Micro Incorporated
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.
Double Cashing With Mobile Banking

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

ANDROID VOLUME THREAT GROWTH, 1Q 2013 TO 1Q 2014

- **1Q 2013**: 0.5M
- **2Q 2013**: 0.72M
- **3Q 2013**: 1M
- **4Q 2013**: 1.39M
- **1Q 2014**: 2.1M
Mobile Cybercriminal Underground

The Mobile Cybercriminal Underground Market in China

Lion Gu
Forward-Looking Threat Research Team

Cybercriminal Underground Wares Sold in China

<table>
<thead>
<tr>
<th>Internet short message gateway spamming service</th>
<th>5,000 text messages</th>
<th>RMB 300 (~US$50)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>10,000 text messages</td>
<td>RMB 400 (~US$65)</td>
</tr>
<tr>
<td></td>
<td>20,000 text messages</td>
<td>RMB 700 (~US$115)</td>
</tr>
<tr>
<td></td>
<td>50,000 text messages</td>
<td>RMB 1,500 (~US$250)</td>
</tr>
<tr>
<td></td>
<td>100,000 text messages</td>
<td>RMB 2,600 (~US$460)</td>
</tr>
</tbody>
</table>

Your password in ICBC Bank will expire tomorrow. Please change password in website: wap.icbcyyt.com as soon as possible. Sorry for any inconvenience. ICBC (95588)
Online banking malware are sporting new routines
Online Banking Malware 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

WITHIN YOUR CONTROL

OUTSIDE YOUR CONTROL

BANK HQ

SERVER

SWITCH

ROUTER

INTERNET

SYSTEM

MOBILE

ATM

ATM
Entry Points for Security Threats

- Fake apps
- Web threats
Where Users Stumble Upon Malicious Apps

- **APP STORES**: 27%
- **SITES**: 80%
- **OTHERS**: 1%
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

- 새마을금고 472KB
- 스마트뱅킹 2.51MB
- 스탠다드차타드은행 1.91MB
- 신한S뱅크 2.53MB
- 원터치개인 1.83MB
- 하나N Bank 1.78MB
“Trojanized” Banking Apps

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.
Mobile Phishing
Distribution of Mobile Phishing URLs

More than 40% of mobile phishing sites target financial services
Mobile Phishing

Welcome to Chase.com

Confirm Contact Information

Important: In order to continue to receive important account alerts such as low balance notifications or transaction confirmations, we need to confirm or update your email address. Please enter the information below to continue.

Your e-mail address (user@domain.com)
Your email password

Continue

Welcome to Chase.com

Error: No file uploaded! Please upload your valid photo of your government issued ID (such as Passport or Driver Licence) using the button below:

Photo ID
Choose file
No file chosen
Continue
Entry Points for Security Threats

- Cross-platform threats
- Man-in-the-middle attacks
Cross-Platform Threats
Cross-Platform Threats
Man-in-the-Middle Attacks

ZITMO and PERKEL
Operation Emmental

Translation:
Subject: Your order 9178158 from 04/02/14
Body/Email text: (The) payment. Your (Company) Switzerland Team.
Attachment: Receipt 2014.03.02.rtf

Translation:
To view the receipt, please double-click the icon.
Operation Emmental
Operation Emmental

Installation process of the mobile app. Step 2.
1. Install the mobile app from the SMS on your phone and start it.
2. Then you will have the possibility to generate the one-time password for accessing your bank account. Click “Generate password” to generate a password.
3. Enter the displayed password on this page and click “Next.”
   I didn’t receive an SMS with the link to the mobile app.
   One-time password, generated by the mobile app:
Operation Emmental

---

**TRANSLATION**

If you didn't receive the link to your mobile phone for whatever reason, please use alternative download methods:

Enter into your mobile browser the following address:

hxpx://bit.do/kFCN

or scan the QR code.

**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

- Targeted attacks
- Data breach
- Data loss/leak
Security Threats to Enterprises: Targeted Attacks
Security Threats to Enterprises: Data Breach
Security Threats to Enterprises: Data Leak/Loss
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.
Thank You!

Paul J.S. Oliveria

Paul_Oliveria@trendmicro.com