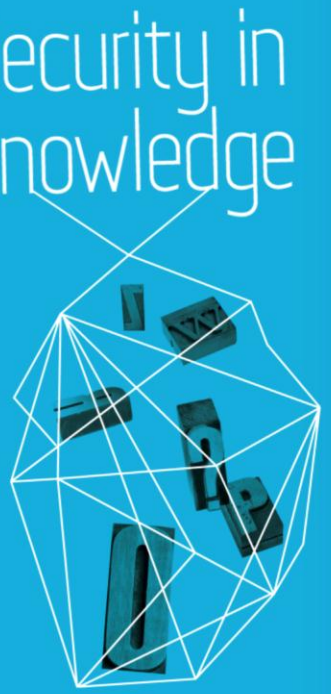
ROGUE APPS & DESKTOP MALWARE: A DANGEROUS COMBINATION FOR ONLINE SECURITY

Maurits Lucas (@lucasmaurits)
Fox-IT



Session ID: MBS-R08
Session Classification: Advanced

RSA CONFERENCE EUROPE 2013

Contents

- Rogue Mobile Apps versus Mobile Malware
- Introduction to Man-in-the-Browser
- Rogue Mobile apps and SMS – sample case
- Summary and conclusions

Rogue Apps vs Mobile Malware

#RSAC

RSA CONFERENCE EUROPE 2013

Mobile malware

- Misnomer when you compare with the desktop
- Better to speak of "*Rogue applications*"
  - You install them
  - You can remove them too
  - They are just apps, they don't touch the OS
- On the desktop, it's rather different ☺
- Thankfully – no real mobile AV either!

Rogue apps

- What is out there is almost exclusively Rogue Apps
- Don’t do what it says on the tin
- You install them but can uninstall them too
- Don’t attack the smartphone OS itself
- Won’t stay like this forever though!

Man-in-the-Browser Primer

#RSAC

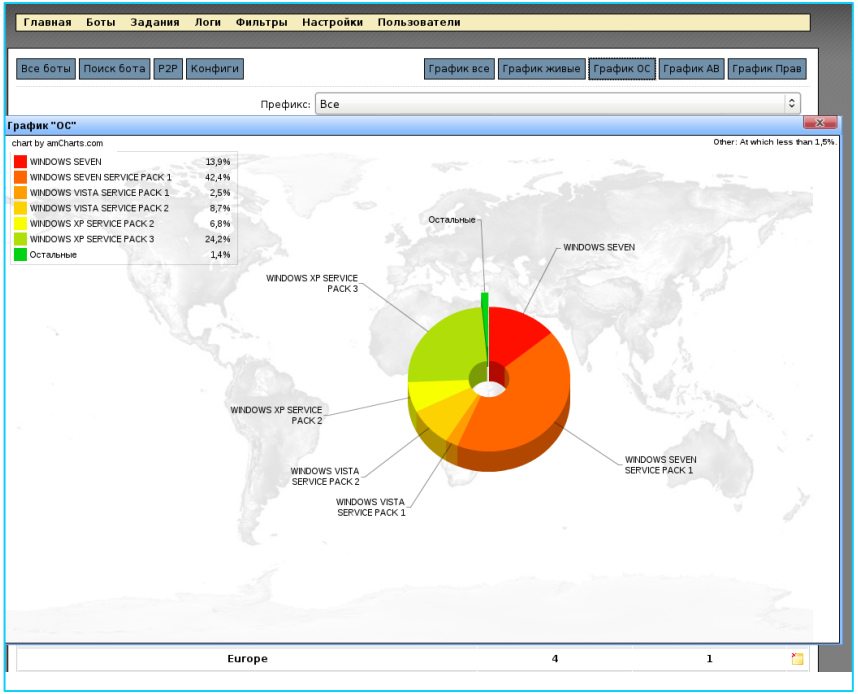
RSA CONFERENCE EUROPE 2013

Man in the Browser

- Type of attack where content is altered before rendering
- Performed by malware which forms botnets
- Used often in online banking fraud
- Significant losses

Man in the Browser malware

- Many families:
  - SpyEye
  - Zeus (and derivatives)
  - Sinowal / Torpig
  - Carberp
  - ... the list goes on and on



Malware functionality

- Main: Modify server content before it is rendered
- But also:
  - Config updates
  - Binary updates
  - Steal passwords, certificates, etc.
  - Screenshots (movies even)
  - And more!

Main steps in an attack

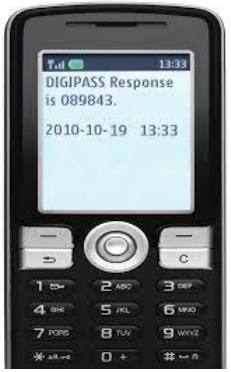
1. Lure user to infection point
2. Infect user with banking trojan
3. Insert additional transaction to mule
4. Get user to authorise transaction
5. Profit!

Authorise transaction?

- A lot of banks use Out-Of-Band mechanism to authorise transactions
- Beyond the reach of the trojan
- User must be social engineered into authorising the transaction without realising
- Hardest part of the attack!

OOB mechanisms

- Tokens
- Calculators
- Card readers
- TAN
- Mobile TAN



MitB attack takeaways

- Malware ≠ Attack
- There are many botnets
- Attack social engineers OOB authentication
- mTAN can be circumvented using Rogue App

Rogue mobile mTAN apps

Mobile TAN

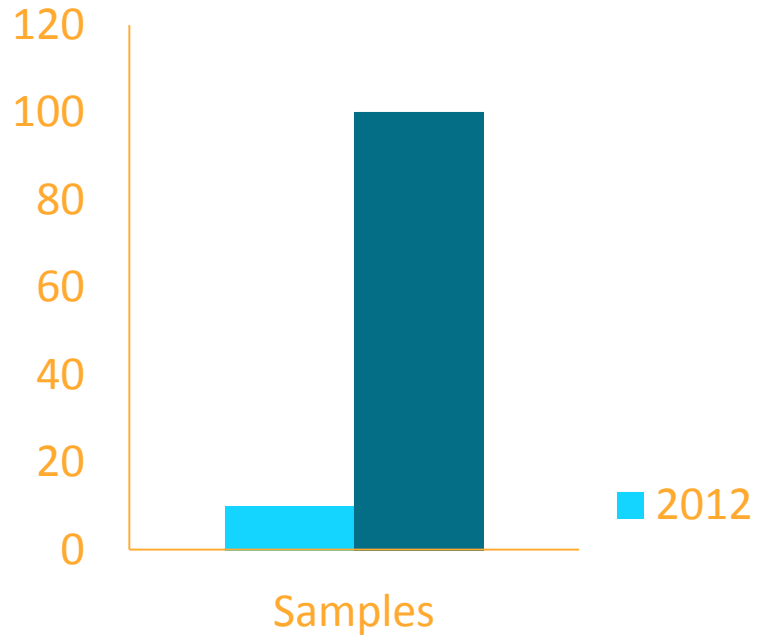
- Send SMS containing TAN to mobile
- OOB when introduced
- But then: smartphones!
- And smartphone apps!

Emergence of mTAN Apps

- Apps which silently forward mTAN
- First examples appeared years ago (ZitMo, SPitMO)
- Have suddenly taken off
- Now different strains

Taking off quantified

- 2012: dozen samples
- 2013: 1st 6 months > 100



One of the first - Symbian

- One of the first cases was in Germany
- Targeted Symbian (Nokia S60)
- Code signing certificates hard to come by
- Developer certificate for one phone was easier

Symbian attack

- User asked to look up and enter IMEI of phone
- Attacker requests developer cert for IMEI
- Several days later, user receives rogue app
- This did not scale well - obviously
- Never caught on

Then there were rumblings

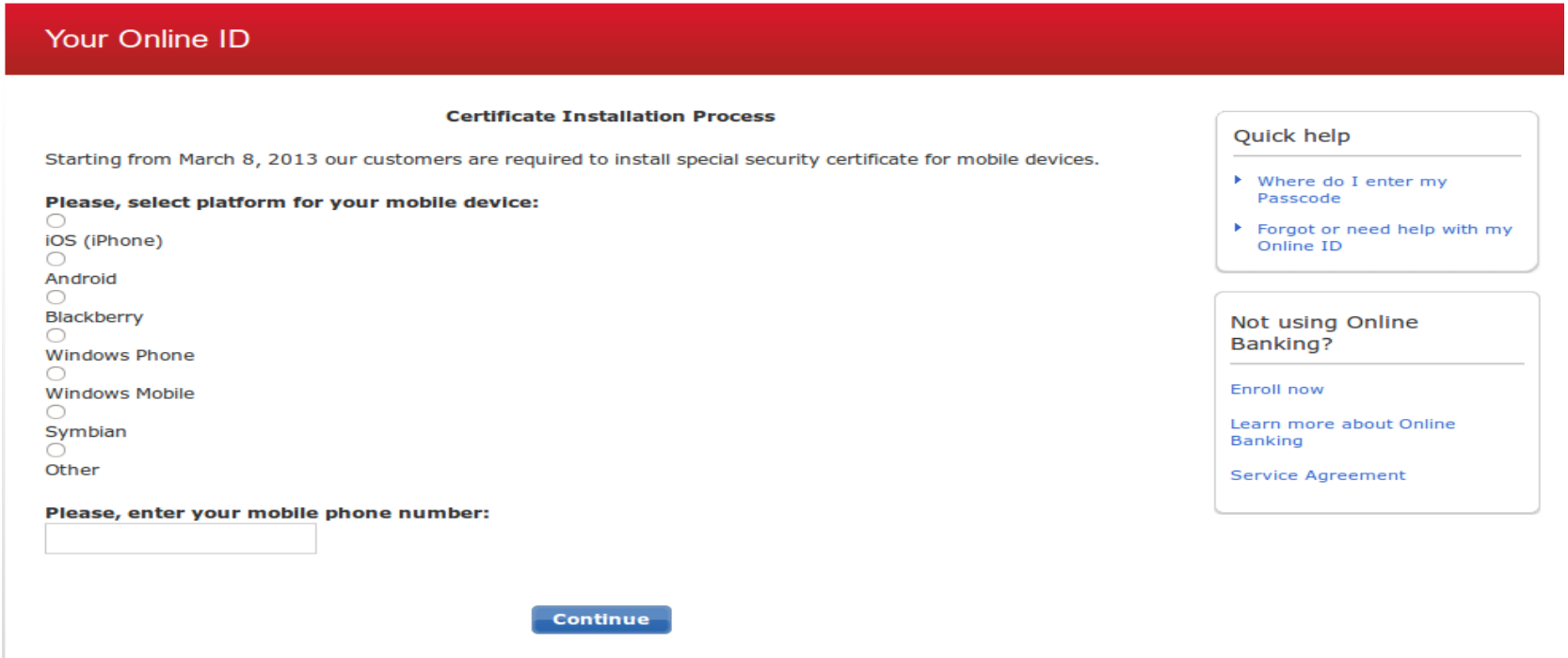
- ZitMo and SPitMO
- Targeting Android and Blackberry
- Would appear and disappear
- Always small scale – still figuring it out?

Then Perkele and friends

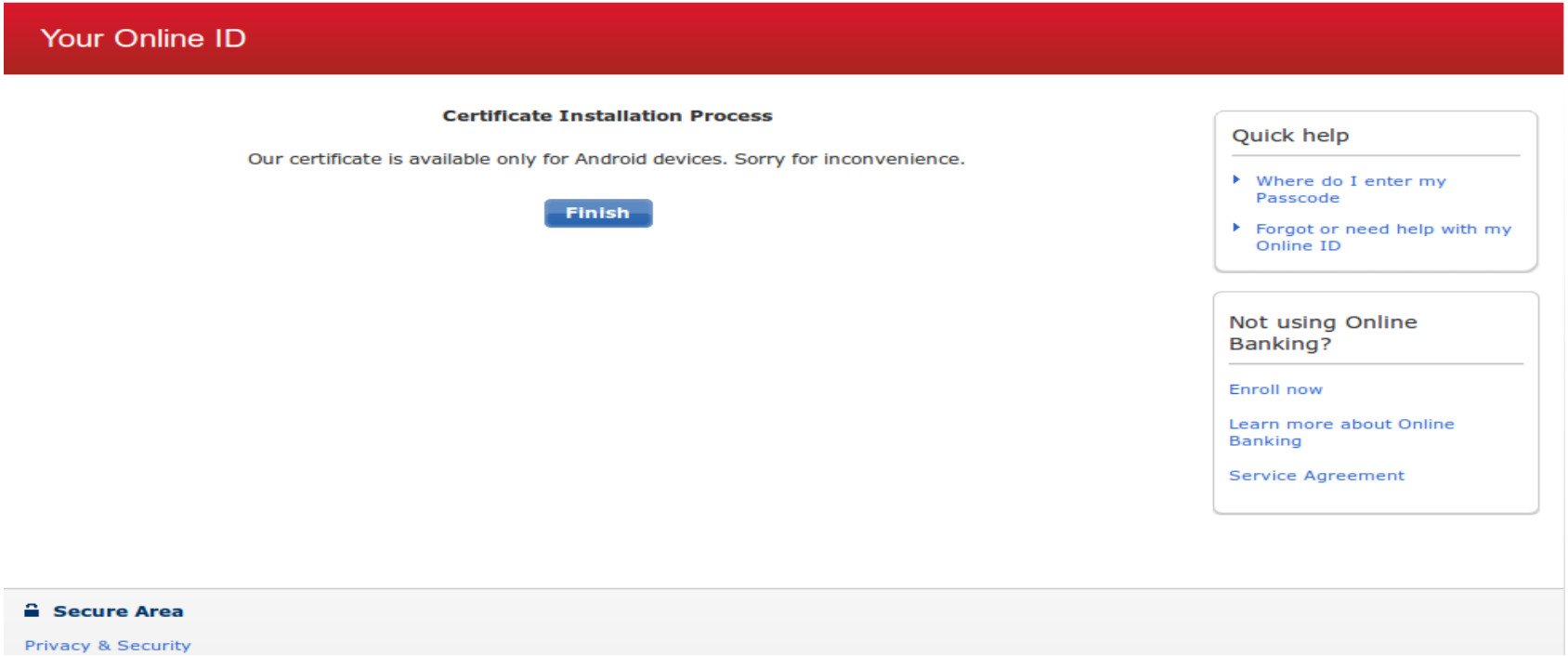
- Android mTAN stealing app with backend
- For sale in the underground
- Support – reskinning for chosen target
- Author got cold feet
- Several clones sprung up

Sample of Rogue App attack

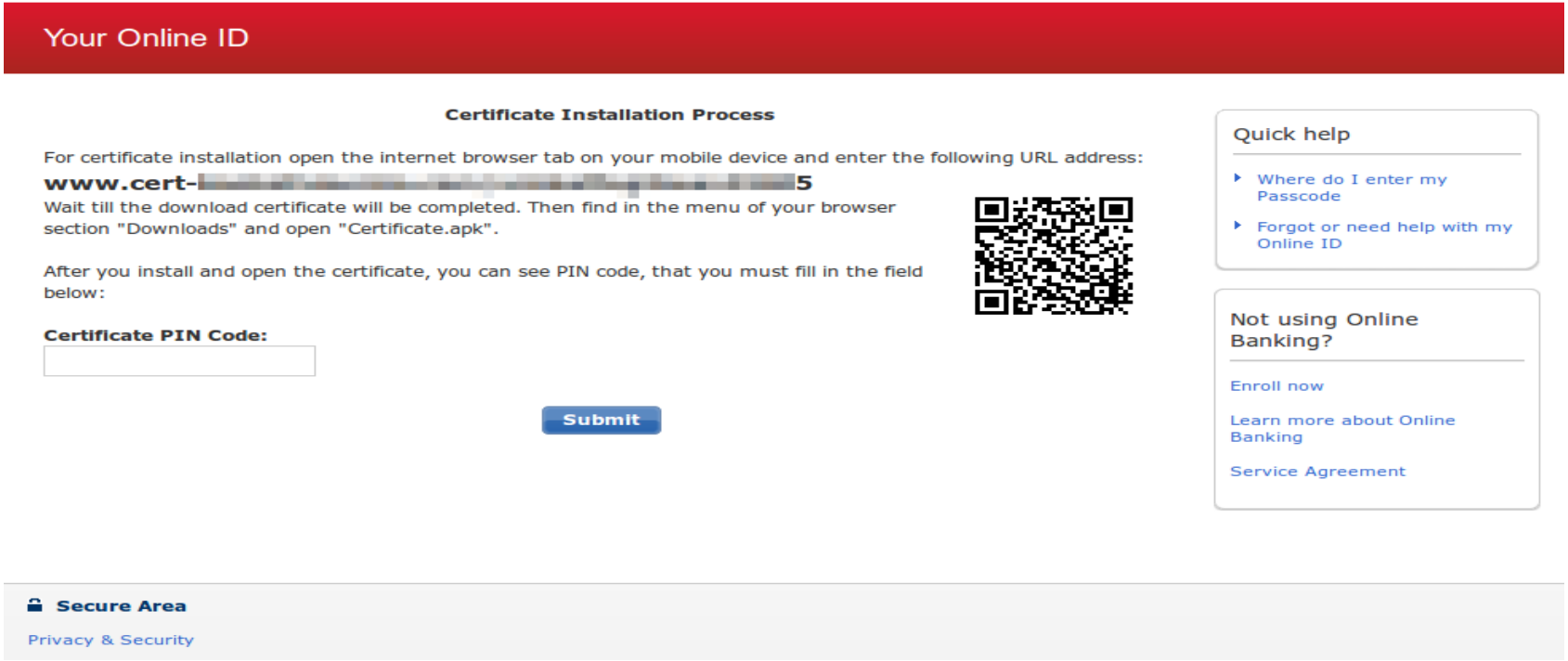
New security measure



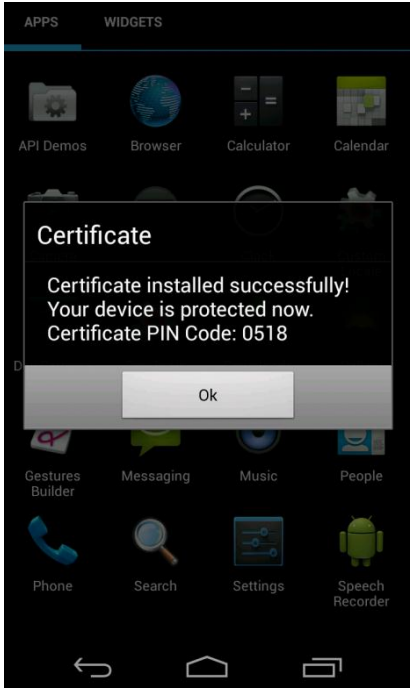
Sorry, Android only

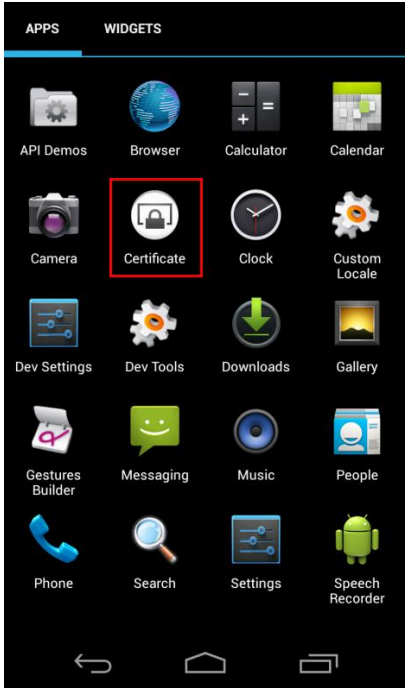


Download the App



To the mobile - Install App





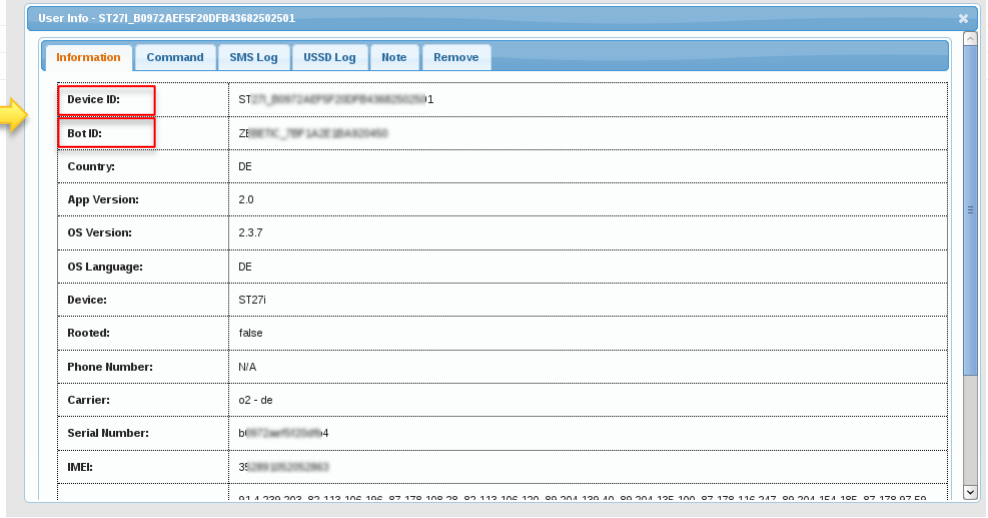
So what does the App do?

```
public void loadingSuccess(JSONObject paramJSONObject)
{
  String str;
  try
  {
    if (!paramJSONObject.getString("result").equals("true"))
      return;
    str = paramJSONObject.getString("command");
    if (str.equals("start_sms_forwarding"))
    {
      setNumbersForSmsDivert(preparePhoneNumbers(paramJSONObject.get("phone_number")));
      return;
    }
    if (str.equals("start_call_blocking"))
      setNumbersForCallBlock(preparePhoneNumbers(paramJSONObject.get("phone_number")));
  }
  catch (JSONException localJSONException)
  {
    Log.e("ReCheckCommandReceiver", localJSONException.toString());
  }
  if (str.equals("stop_sms_forwarding"))
    setNumbersForSmsDivert(null);
  else if (str.equals("stop_call_blocking"))
    setNumbersForCallBlock(null);
  else if (str.equals("send_sms"))
    sendSms(paramJSONObject.getString("phone_number"), paramJSONObject.getString("message_text"));
  else if (str.equals("execute_ussd"))
    executeUssd(paramJSONObject.getString("ussd_query"));
  else if (str.equals("stop_program"))
    stopProgram();
  else if (str.equals("show_message"))
    showMessage(paramJSONObject.getString("message_text"));
  else if (str.equals("delay_change"))
    changeCheckCommandDelay(paramJSONObject.getInt("delay"));
  else if (str.equals("ping"))
    ServerApi.smsPong(this.mContext);
 }
}
```

- *start_sms_forwarding*
- *start_call_blocking*
- *stop_sms_forwarding*
- *stop_call_blocking*
- *send_sms*
- *execute_ussd*
- *stop_program*
- *show_message*
- *delay_change*
- *ping*

Backend

Device ID	Bot ID	Country	SMS Hook	Call Block	Command	Last Activity
MB[redacted]	DC[redacted]	US	Inactive	Inactive	N/A	20.03.2013 16:54:05
HT[redacted]	EBON[redacted]F69	US	Inactive	Inactive	N/A	20.03.2013 16:53:39
MB[redacted]	WYCHE[redacted]3B01	US	Inactive	Inactive	N/A	20.03.2013 16:53:38
DF[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	N/A	20.03.2013 16:52:43
LG[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	N/A	20.03.2013 16:46:54
HT[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	show_message	19.03.2013 20:17:24



Implications

- Whole new can of worms
- Teach customers about mobile security
- Be able to detect attacks like these
- Have measures to clean up smartphones too

Countermeasures

- Good overview of threat landscape
- Including app stores
- Foster relations with platform owners, AV, etc.
- Have banking app check for unusual apps
- Move away from SMS as carrier

What next on mobile

- Mobile being used in cashout schemes
- Attempt to evade detection by switching channel
- Make sure you detect across channels

- Real mobile malware? MitM?

Summary and Conclusions

Summary

- MitB used for online banking attacks
- OOB needs social engineering
- mTAN stealing rogue apps have ballooned this year
- “Only” attack mTAN SMS messages
- Significant losses
- Consumer awareness low

Conclusions

- If you use mTAN, prepare for Perkele c.s.
- Rogue apps are troublesome at the least
- Overview of threat landscape essential
- Have measures to detect and cleanup
- Consider user education
- Start considering other channels on mobile

Thank you!

Maurits Lucas
Fox-IT
@lucasmaurits
lucas@fox-it.com
www.foxintell.com

#RSAC

RSA CONFERENCE EUROPE 2013