

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

Maurits Lucas (@lucasmaurits)
Fox-IT

Security in
knowledge



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

RSACCONFERENCE
EUROPE 2013

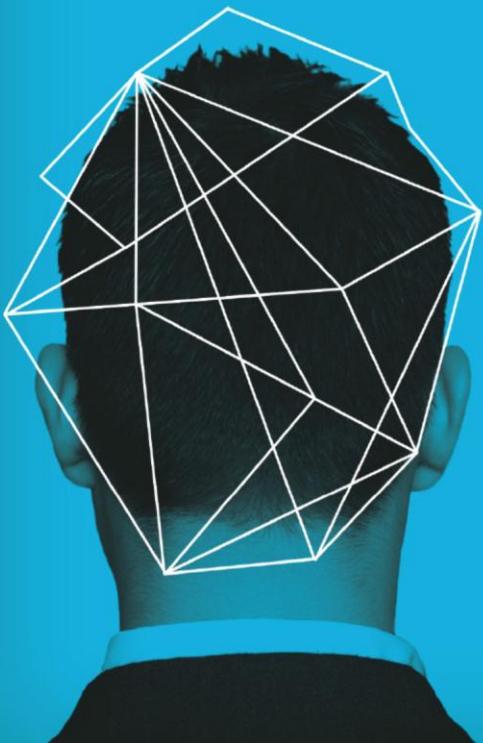
Mobile malware

- ▶ 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



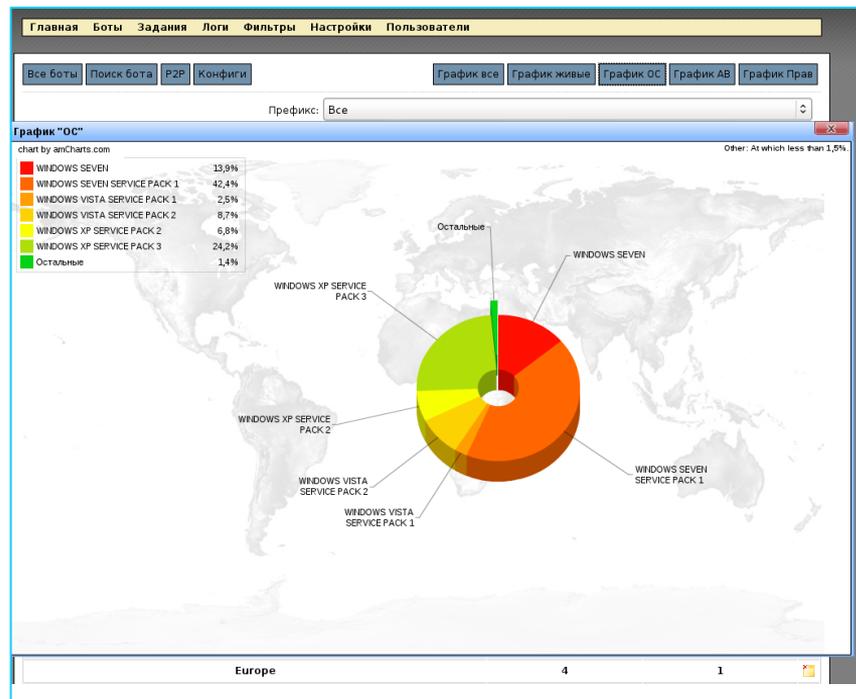
RSACCONFERENCE
EUROPE 2013

— 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



RSACCONFERENCE
EUROPE 2013

Mobile TAN

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

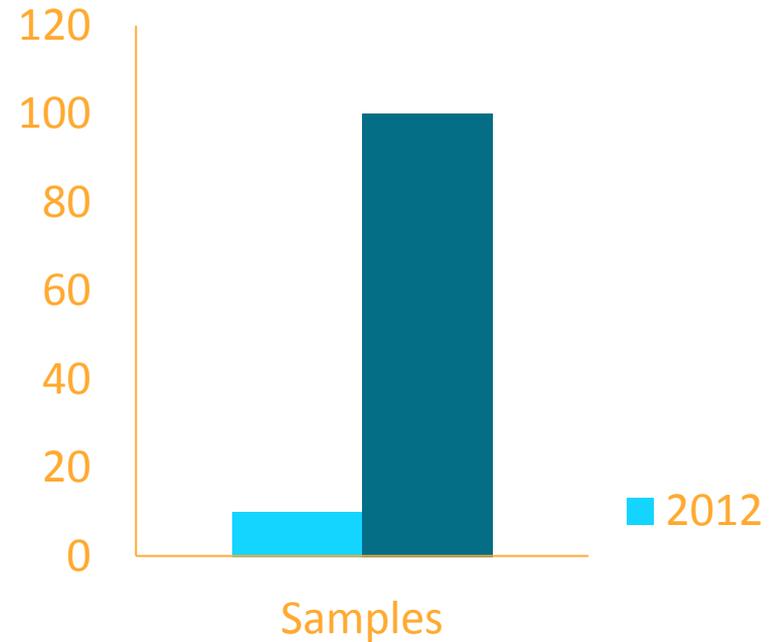


Emergence of mTAN Apps

- ▶ 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



 #RSAC

RSACCONFERENCE
EUROPE 2013

New security measure

Your Online ID

Certificate Installation Process

Starting from March 8, 2013 our customers are required to install special security certificate for mobile devices.

Please, select platform for your mobile device:

- iOS (iPhone)
- Android
- Blackberry
- Windows Phone
- Windows Mobile
- Symbian
- Other

Please, enter your mobile phone number:

[Continue](#)

Quick help

- ▶ [Where do I enter my Passcode](#)
- ▶ [Forgot or need help with my Online ID](#)

Not using Online Banking?

- [Enroll now](#)
- [Learn more about Online Banking](#)
- [Service Agreement](#)

Sorry, Android only

Your Online ID

Certificate Installation Process

Our certificate is available only for Android devices. Sorry for inconvenience.

[Finish](#)

Quick help

- ▶ [Where do I enter my Passcode](#)
- ▶ [Forgot or need help with my Online ID](#)

Not using Online Banking?

[Enroll now](#)

[Learn more about Online Banking](#)

[Service Agreement](#)

 **Secure Area**

[Privacy & Security](#)

Download the App

Your Online ID

Certificate Installation Process

For certificate installation open the internet browser tab on your mobile device and enter the following URL address:

www.cert-**5**

Wait till the download certificate will be completed. Then find in the menu of your browser section "Downloads" and open "Certificate.apk".

After you install and open the certificate, you can see PIN code, that you must fill in the field below:

Certificate PIN Code:

Submit



Quick help

- ▶ [Where do I enter my Passcode](#)
- ▶ [Forgot or need help with my Online ID](#)

Not using Online Banking?

[Enroll now](#)

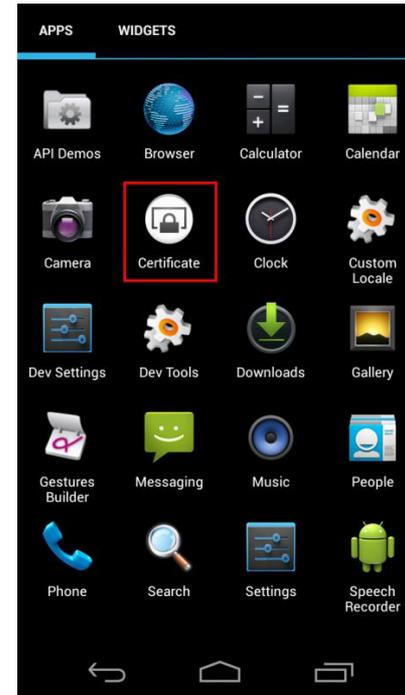
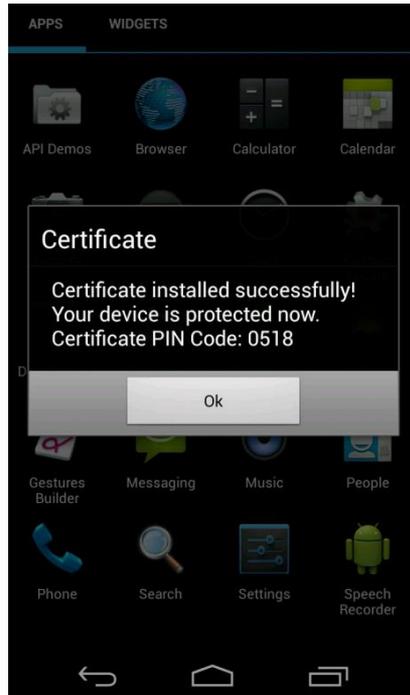
[Learn more about Online Banking](#)

[Service Agreement](#)

 **Secure Area**

[Privacy & Security](#)

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
ME101_A89C4489246A37AC736C100	DCN1_775A8896222F68	US	Inactive	Inactive	N/A	20.03.2013 16:54:05
HT1_08E_X_332638389F3F4517429	EBONY_LAW_775A8896222F69	US	Inactive	Inactive	N/A	20.03.2013 16:53:39
ME132_86138F94032862A779AC100	WYCHE1MPLY_78F1A2E3F8C33B01	US	Inactive	Inactive	N/A	20.03.2013 16:53:38
DF104_A43F082A0E8E339488111					N/A	20.03.2013 16:52:43
LG16776_8C47C868C4C0863990007					N/A	20.03.2013 16:46:54
HT1_089FE_C_85A488761A08284190					show_message	19.03.2013 20:17:24



User Info - ST271_B0972AEF5F20DFB43682502501

Information Command SMS Log USSD Log Note Remove

Device ID:	ST271_B0972AEF5F20DFB43682502501
Bot ID:	Z8107C1_78F1A2E3F8C33B01
Country:	DE
App Version:	2.0
OS Version:	2.3.7
OS Language:	DE
Device:	ST271
Rooted:	false
Phone Number:	N/A
Carrier:	o2 - de
Serial Number:	b8f72a4f020b4
IMEI:	35199 20202083

01 1 226 202 01 112 102 102 07 170 100 70 01 112 102 120 00 204 120 40 00 204 120 100 07 170 112 247 00 204 124 102 07 170 07 20

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



RSACCONFERENCE
EUROPE 2013

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!

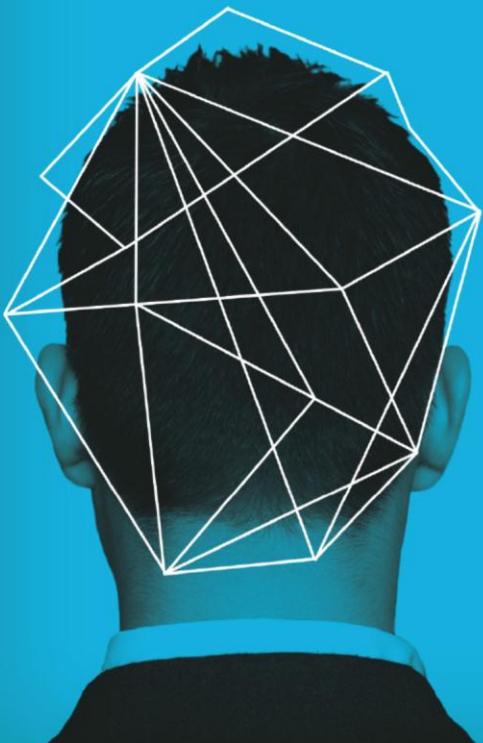
Maurits Lucas

Fox-IT

@lucasmaurits

lucas@fox-it.com

www.foxintell.com



RSACCONFERENCE
EUROPE 2013