



## Internet-Kriminalität

Romano Ramanti  
Zürcher Kantonalbank  
Fachstelle eFraud



---

## Was ist ein Hacker?

Ein Hacker ist jemand, der versucht einen Weg zu finden, wie man mit einer Kaffeemaschine Toast zubereiten kann

Zitat von Wau Holland

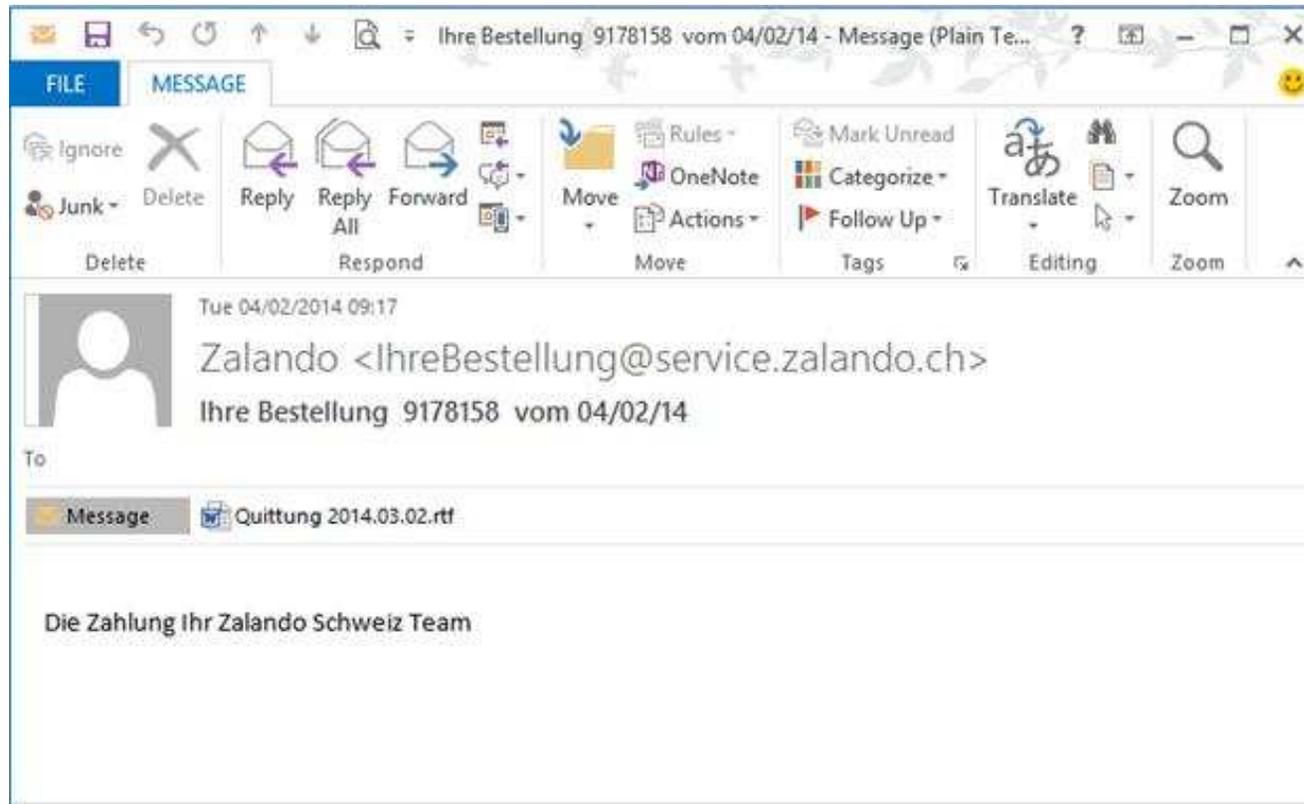
Gründer Chaos Computer Club (CCC)

# Hacker sind keine Cyberkriminelle

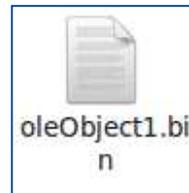
---

# Retefe Bankentrojaner

# Banking-Trojaner Retefe



# Ablauf Infektion Retefe

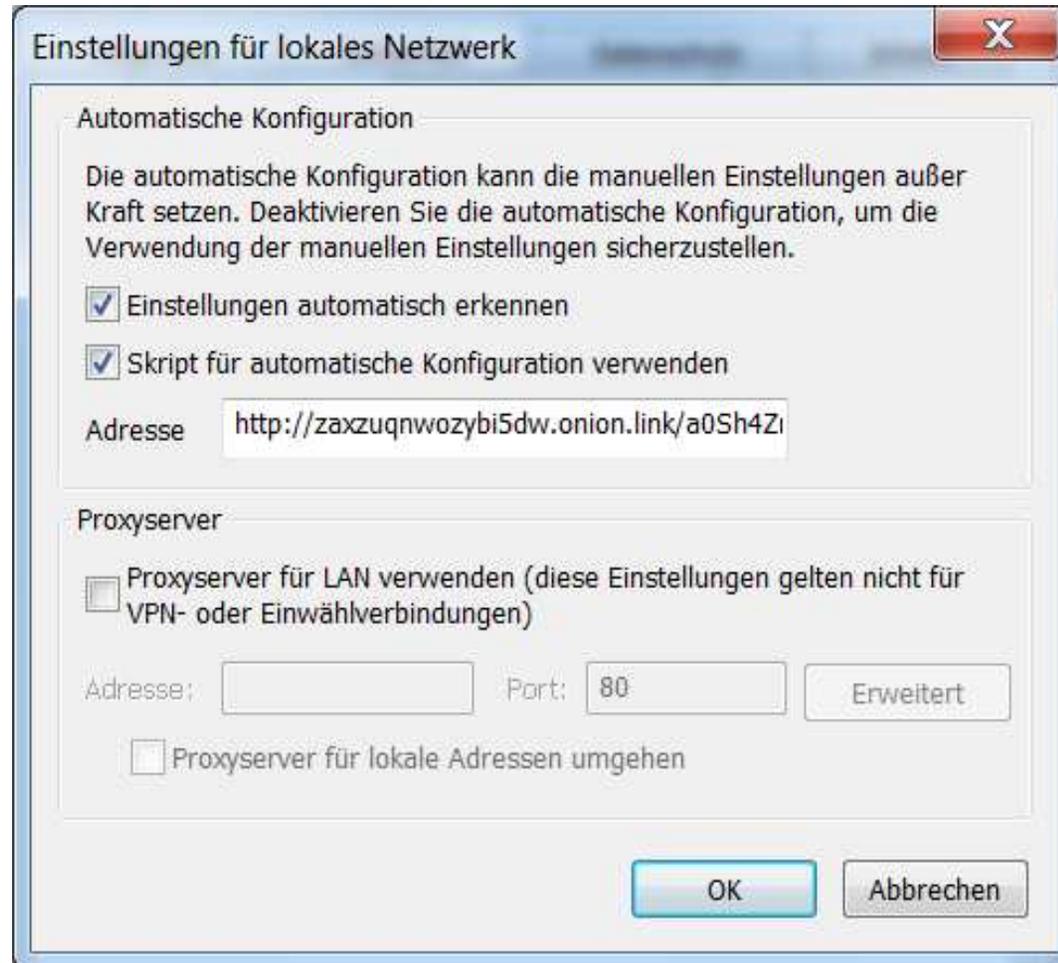


```
=wscript Zahlung_14_04_16_72055.js
```

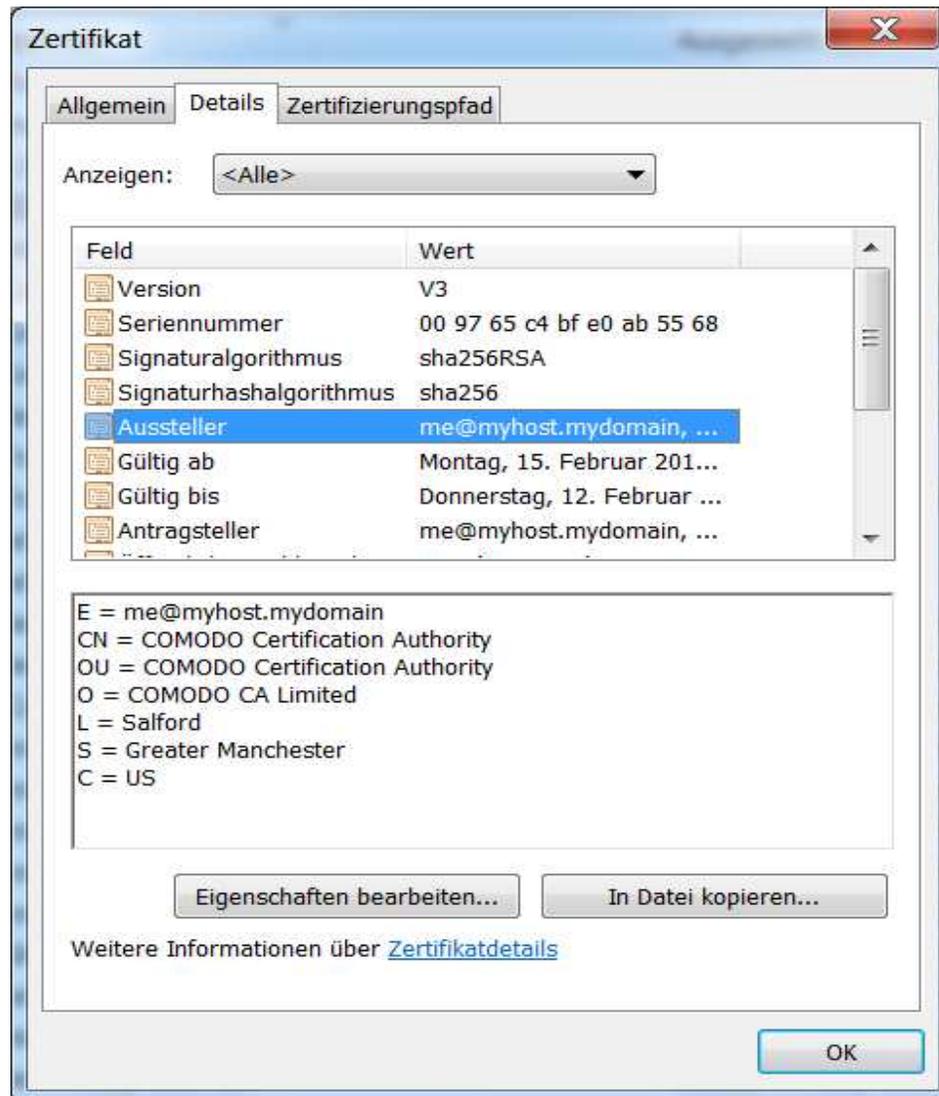


```
var Config = {  
  dl: ["ziplamtg2fn3q733.onion", "zaxzuguwozybi5dw.onion", "kxq2e7bwokxzp5ws.onion", "au63cg6xprf5qq5t.onion"],  
  zl: ["to", "link"],
```

# Veränderte Proxy-Einstellungen



# Gefälschtes X.509 Zertifikat



```
this.InstallCert = function() {  
    if (!this.IsCertUtilInstalled()) {}  
    this.ConfirmCert();  
    wss.Run("certutil -addstore -f -user \\"  
        ROOT\\ " \\"  
        "+Cert.FileName+"\\  
        "", 0, true)  
};
```

# https-Fake



# Meldung nach der Installation des Banking-Trojaner

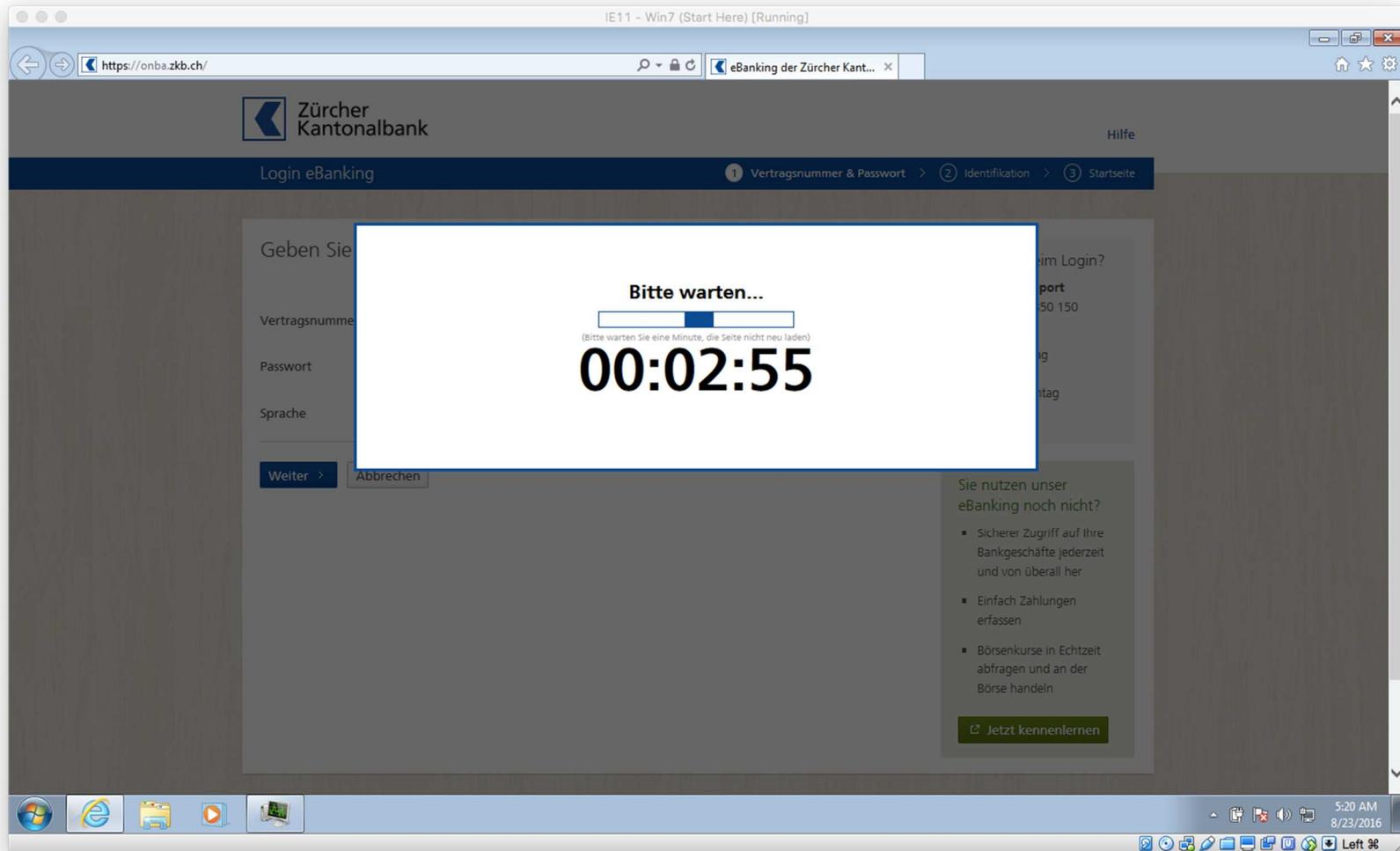


In Zusammenhang mit der Modernisierung des Sicherheitssystems kann von Ihnen eine zusätzliche Identifizierung beim Einloggen ins Benutzerkonto gefordert werden. Dementsprechend können wir Sie einmalig bitten, unsere Applikation für Smartphones auf Ihr Handy zu installieren, das zu Ihrem Konto hinzugefügt ist. Sie müssen die gegebene Applikation auf Ihr Handy installieren, um Ihr Konto weiter zu benutzen können\*. Ohne Installation der mobilen Applikation wird der Zugang auf das Konto gesperrt. Danke für das Verständnis.

\* Nach der Installation der mobilen Applikation kann die Periode der Synchronisation und anderer Maßnahmen für die maximale Sicherheitssicherung bis zu 3 Arbeitstagen dauern. In dieser Zeit können Sie Ihr Konto nicht benutzen.

OK

# Banking Trojaner Retefe



# Installation der App



## Installation der Mobil-Applikation. Schritte 2:

1. Installieren Sie die mobile Applikation auf Ihrem Telefon und starten Sie diese.
2. Daraufhin erhalten Sie die Möglichkeit das Einmalpasswort für den Zugang zu Ihrem Konto zu generieren. Klicken Sie auf „Passwort generieren“ für die Generierung des Passwortes.
3. Geben Sie das generierte Passwort auf dieser Seite ein und klicken Sie auf 'Weiter'.

[Ich habe keine SMS mit dem Link erhalten.](#)

Wenn Sie aus irgendwelchem Grund die SMS mit dem Link nicht erhalten können, nutzen Sie bitte unsere alternativen Download-Varianten.

Geben Sie in Ihrem **Mobilbrowser** die folgende Adresse ein:

<http://n2rzn.tk>

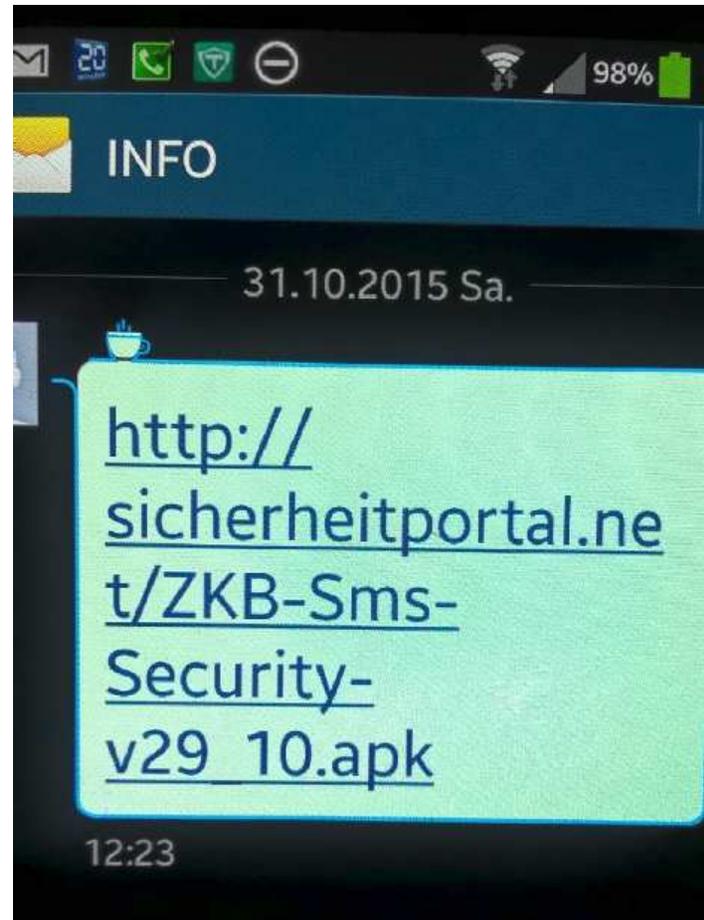
oder

scannen Sie den QR-Code.

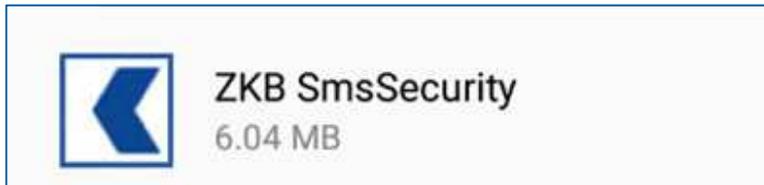


Einmaliges Passwort, das von der mobilen   
Applikation generiert worden ist::

Kunde erhält anschliessend eine SMS mit dem Download-Link



# Banking Trojaner wird anschliessend auf dem Handy installiert



## Request permission:

Source: submitted apk	Request permission: android.permission.INTERNET
Source: submitted apk	Request permission: android.permission.READ_PHONE_STATE
Source: submitted apk	Request permission: android.permission.READ_SMS
Source: submitted apk	Request permission: android.permission.RECEIVE_SMS

# Fernsteuerung der App

535106 STARTB

+ [REDACTED]

I=357736050975539;  
DA=Yes;  
Service Started

---

## Social Engineering (Phishing)

# Zürcher Kantonalbank Phishing

The image shows a browser window displaying a phishing website for the Zürcher Kantonalbank. The browser's address bar is redacted with a black box. The website header includes the bank's logo and the text 'Zürcher Kantonalbank' and 'Hilfe'. Below the header is a blue navigation bar with the text 'Login eBanking' and four menu items: 'Information', 'Vertragsnummer & Passwort', 'Identifikation', and 'Startseite'. The main content area is titled 'Geben Sie Ihre Vertragsnummer und Passwort ein'. It contains a form with the following fields: 'Vertragsnummer' (with the value '700'), 'Passwort', 'Vorname', 'Name', 'Geburtsdatum', 'Wohnort', 'Straße, Haus-Nr', 'Postleitzahl', 'Telefon', and 'Mobiltelefon'. To the right of the form is a sidebar with two sections. The first section is titled 'Probleme beim Login?' and contains the text 'eBanking Support', 'Telefon 0844 840 140', 'Servicezeiten', and 'Montag - Sonntag 08.00 - 22.00'. The second section is titled 'Sie nutzen unser eBanking noch nicht?' and contains a list of bullet points: '• Sicherer Zugriff auf Ihre Bankgeschäfte jederzeit und von überall her', '• Einfach Zahlungen erfassen', and '• Börsenkurse in Echtzeit abfragen und an der Börse handeln'. Below the list is a green button with the text 'Jetzt kennenlernen'.

# Tracking-Mails

**Betreff:** Fragen zu Ihrem Konto

**Datum:** Fri, 7 Apr 2017 10:18:17 +0200

**Von:** Zürcher Kantonalbank <[christian.weininger@zkb-ch.ga](mailto:christian.weininger@zkb-ch.ga)>

**An:**



Guten Tag,

ich heisse Christian Weininger, ich bin Inspektor des Sicherheitsdienstes in der Zentralfiliale der Züricher Kantonalbank.

Es gibt einige Fragen zu Ihnen, an welche E-Mail-Adresse kann ich das Dokument mit der Liste der Fragen zuschicken?

Mit freundlichen GRÜSSEN,  
Christian Weininger



# Was können Sie für sicheres eBanking beitragen? 3/4

## 5 Schritte für mehr Computer-Sicherheit

### (1) Daten regelmässig sichern

- Sicherung auf externen Medien
- Kontrollieren Sie, dass die Daten auch wirklich gespeichert wurden
- Einsatz von Backup-Programmen

### (2) Schützen – Einsatz einer Antiviren-Software

- Installation eines Virenschutz-Programmes
- So einstellen, dass die Virensignaturen automatisch aktualisiert werden

[www.ebankingabersicher.ch](http://www.ebankingabersicher.ch)

## 5 Schritte für mehr Computer-Sicherheit

### (3) Überwachen – Einsatz einer Firewall

- Datenverkehr zwischen Ihrem Computer und dem Internet wird kontrolliert
- «offene Türen» werden geschlossen
- Alarmierung bei Gefahren oder verdächtigen Aktivitäten

### (4) Vorbeugen

- Installieren Sie die Updates der Softwarehersteller regelmässig
- Automatisches Herunterladen und installieren der Updates aktivieren

### (5) Aufpassen

- Achten Sie darauf, wo und wann Sie persönliche Informationen im Internet bekannt geben
- Verwenden Sie eines sicheres Passwort  
([www.datenschutz.ch](http://www.datenschutz.ch) – [passwortcheck](#))
- Keine Daten per E-Mail bekannt geben

---

## Fazit

Es gibt keinen 100% Schutz  
Sie sind die beste Firewall