ONLINE- UND MOBILE
BEDROHUNGEN BEIM ONLINE-BANKING

ONLINE-ZAHLUNGEN SIND SEHR BELIEBT, ABER NICHT SICHER

98 % der Befragten nutzen regelmäßig Online-Banking und -Shopping oder elektronische Zahlungssysteme

59 % der Benutzer sind besorgt über Betrug beim Online-Banking

69 % sind um die Sicherheit ihrer persönlichen Daten (einschließlich Zugangsdaten für Online-Banking) besorgt

Kaspersky Lab and B2B International Study – 8.605 Teilnehmer aus 19 Ländern
http://media.kaspersky.com/pdf/Kaspersky_Lab_B2C_Summary_2013_final_EN.pdf

KASPERSKY lab

WELCHE ART VON DATENVERLUST BESORGT INTERNET-NUTZER AM MEISTEN?

Persönliche E-Mail-Nachrichten

37 % GESAMT

Kennwörter, Kontodaten

58 % GESAMT

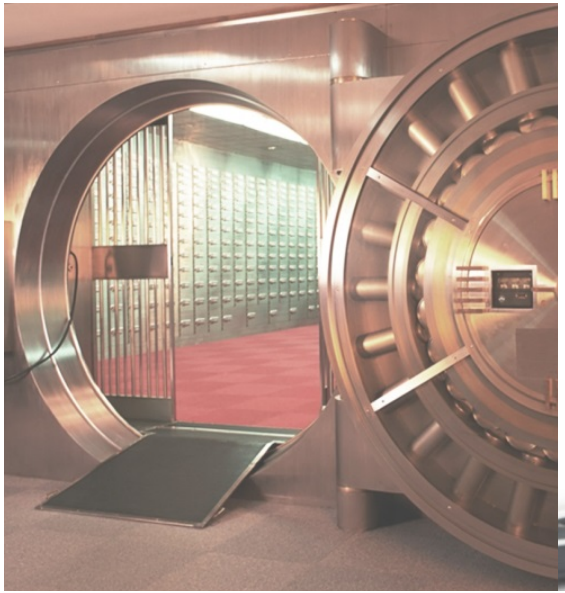
Bank-Informationen

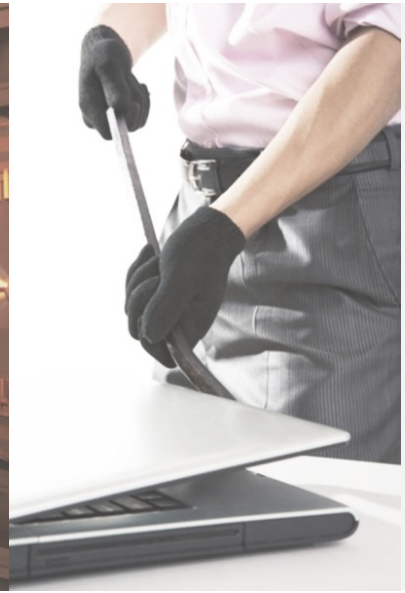
60 % GESAMT

Harris Interactive Kaspersky Digital Consumers Internet Security Needs – Topline Report, 2012

KASPERSKY lab

BANKÜBERFALL ODER ANGRIFF AUF DEN BENUTZER





- Früher überfielen Verbrecher Banken.
- Aber dies ist teuer, aufwändig und riskant.
- Jetzt betrügen sie Online-Benutzer um ihr Geld.
- Und leider sind sie dabei sehr erfolgreich.

HEUTZUTAGE VERKAUFEN CYBERKRIMINELLE BENUTZERAN-MELDEDATEN AUF EINFACHE WEISE WIE IN EINEM GESCHÄFT.

KASPERSKY lab

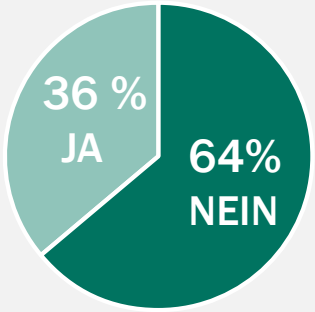
PROBLEME, AUF DIE BENUTZER IM INTERNET STOßEN

Probleme, auf die Benutzer im Internet stoßen

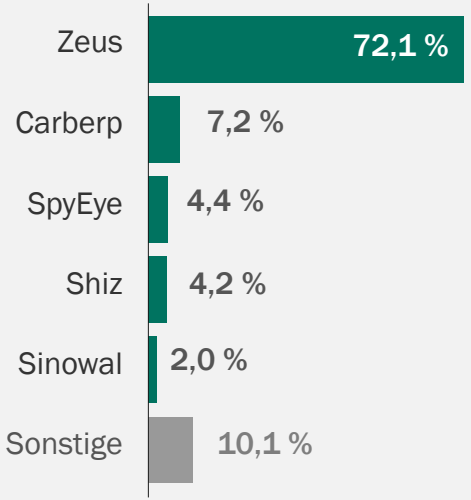
Bei mehr als 25 % der Verbraucher ist es in den letzten 12 Monaten zu einem Malware-Vorfall gekommen

36 % der Malware-Vorfälle führten zu finanziellen Verlusten

Hatten Sie finanzielle Verluste aufgrund eines Virus/einer Malware-Infektion?



Banking-Trojaner weltweit

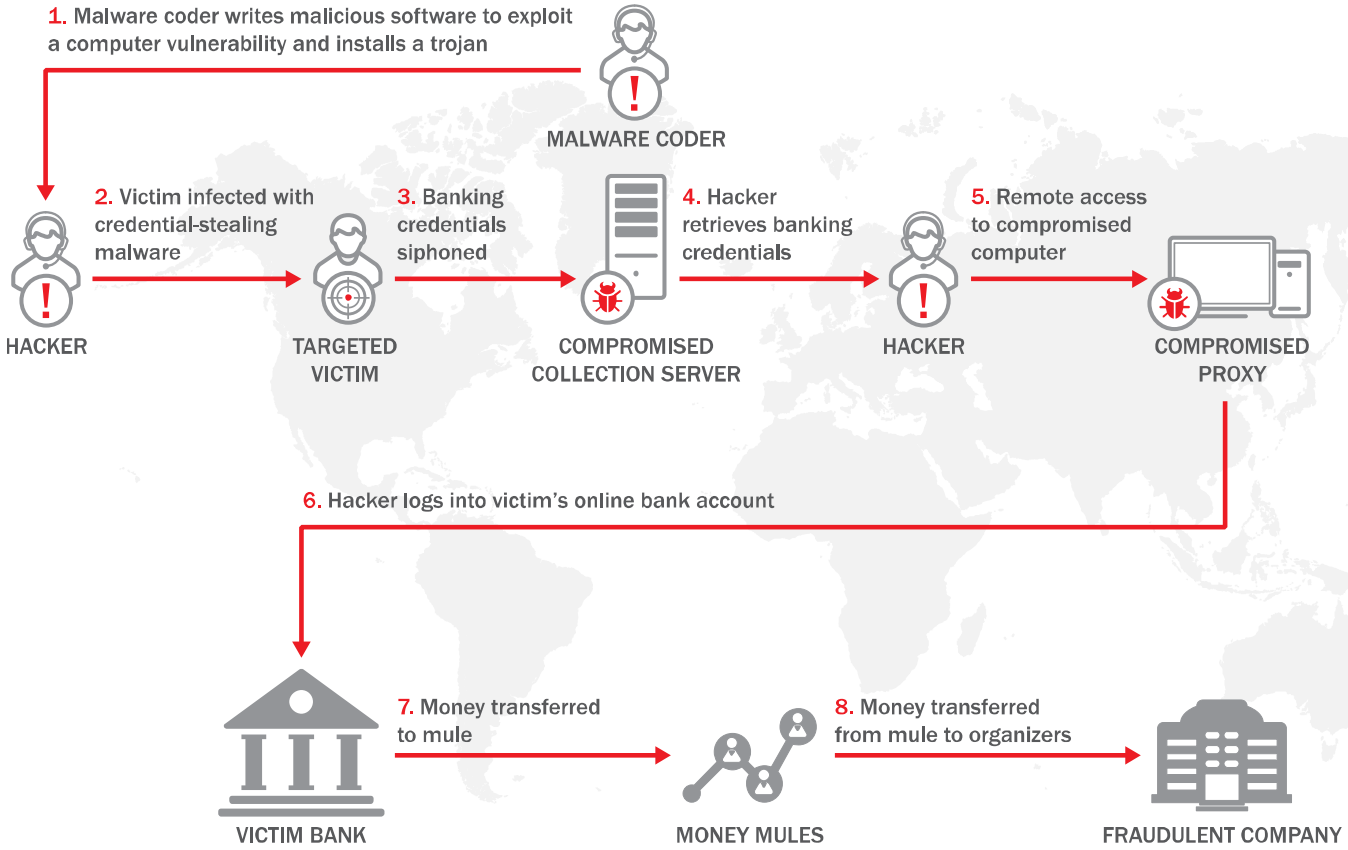


Quelle: Kaspersky Lab, September 2013

SIE DACHTEN, SIE KÖNNTEN IHRE BENUTZER SCHÜTZEN..... .....„UND SIE DACHTEN, SIE SEIEN AUF DER SICHEREN SEITE!“

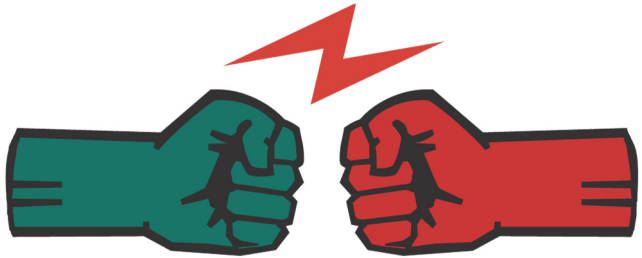
Weitere Informationen finden Sie in „**Staying safe from virtual robbers**“
http://www.securelist.com/en/analysis/204792304/Staying_safe_from_virtual_robbers

SO FUNKTIONIERT ONLINE-BANKING-BETRUG



MODERNE SCHUTZMECHANISMEN VON BANKEN VS. BANKING-TROJANER

Authentifizierung:
Anmeldename/Kennwort,
CVV2, SMS, gedruckte Belege



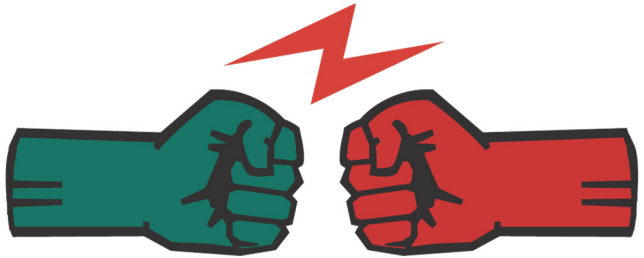
ZEUS

ZEUS – WICHTIGSTE MERKMALE

- Weit verbreitetster Banking-Trojaner
- ZeuS zeichnet die Tastaturanschläge von Benutzern auf, entweder virtuell oder physisch (Keylogging, Screenshots)
- ZeuS nutzt **Web-Injektionen** – Man-in-the-Browser-Attacken
- ZeuS ist in der Lage, die leistungsfähigsten Banksicherheitssysteme, darunter auch die 2-Faktoren-Authentifizierung, zu umgehen
- Wird über **Social Engineering** und **Drive-by-Downloads** verbreitet

MODERNE SCHUTZMECHANISMEN VON BANKEN VS. BANKING-TROJANER

Authentifizierung:
Anmeldename, Kennwort, SMS



Carberp

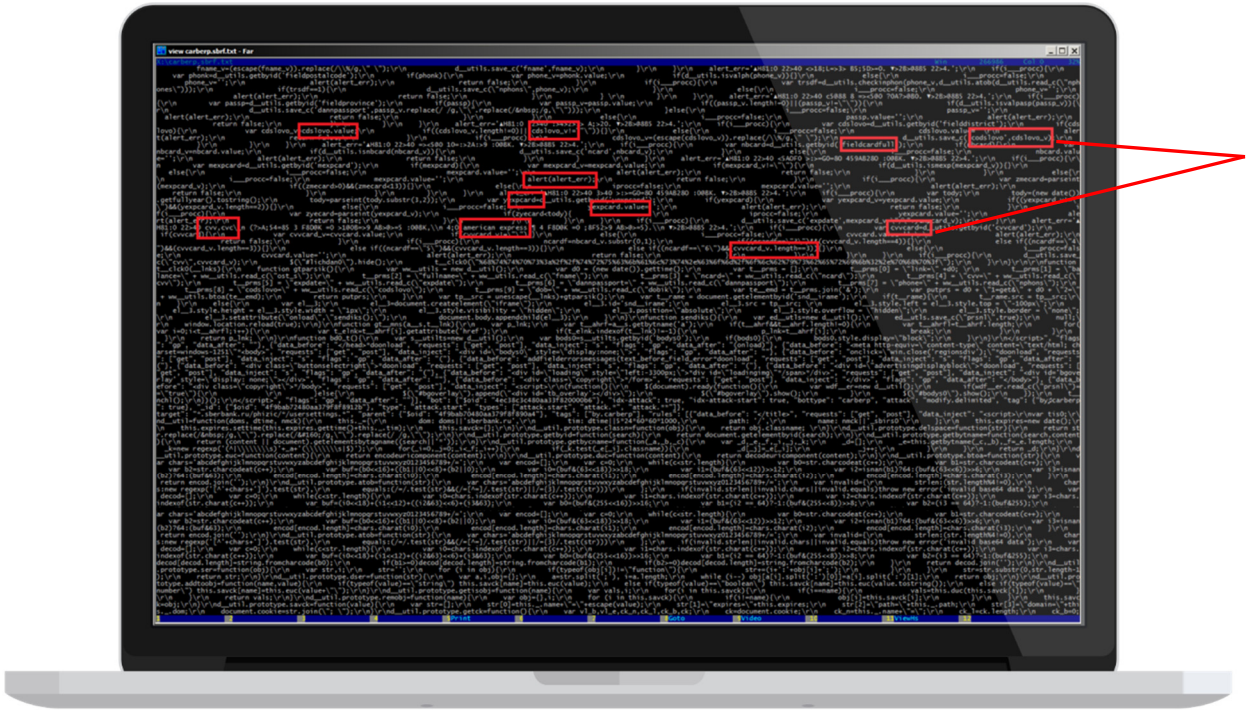
CARBERP: BANKKUNDENSOFTWARE + SCHLÜSSEL

Datendiebstahlmethoden:

- Injektion in den Webbrowser
- Abfangen von Zahlungsdaten
- Gefälschte Benachrichtigungen/ Popups

KASPERSKY lab

CARBERP: INTERZEPTOR FÜR BANKKUNDENSOFTWARE

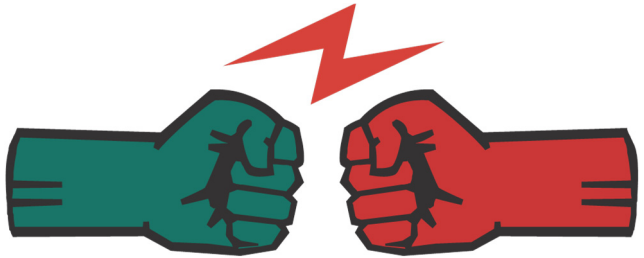


Abgefangene Daten
(CVV/CVC, PIN etc.)

KASPERSKY lab

MODERNE SCHUTZMECHANISMEN VON BANKEN VS. BANKING-TROJANER

Authentifizierung:
Anmeldename/Kennwort,
SMS, Token, TAN-Generatoren,
Webcam-Erfassung



SpyEye

SPYEYE: UMGEHUNG VON TAN-GENERATOREN

TAN-Vorteile:

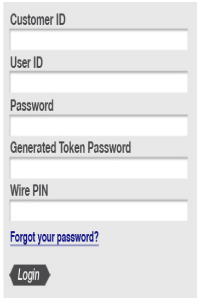
- Der Benutzer muss ein individualisiertes Gerät besitzen
- Der Besitzer muss die PIN kennen
- Eindeutiger Transaktionscode

KASPERSKY lab

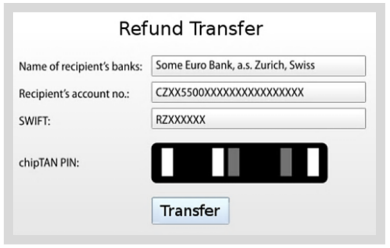
SPYEYE: CHIPTAN-UMGEHUNG DURCH SOCIAL ENGINEERING

Benutzer wird gefälschter Warnhinweis auf der Online-Banking-Seite angezeigt

Benutzer werden gefälschte Informationen zu Überweisungen auf sein Konto angezeigt



Benutzer wird zu Rückerstattung aufgefordert

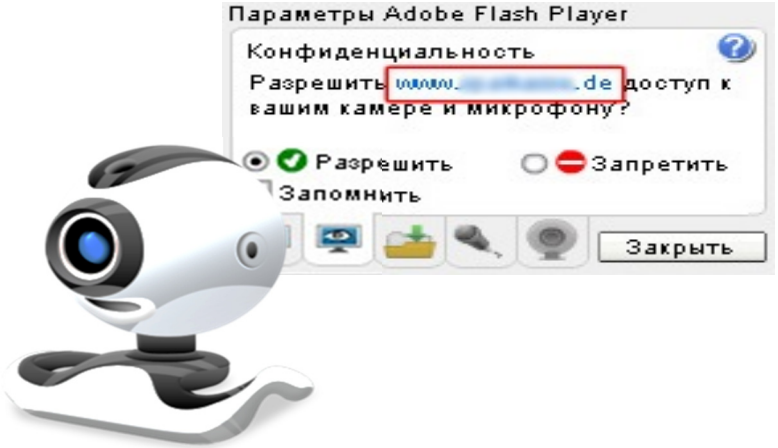


Benutzer gibt Einmalkennwort für Transaktionen ein ... und überweist sein eigenes Geld an Betrüger

„Eine Ihrer letzten Transaktionen beruht auf einem Fehler. Ihrem Konto wurden Beträge gutgeschrieben, die eigentlich für einen anderen Empfänger bestimmt waren. Erstatten Sie den Betrag so schnell wie möglich zurück. Vielen Dank!“

KASPERSKY lab

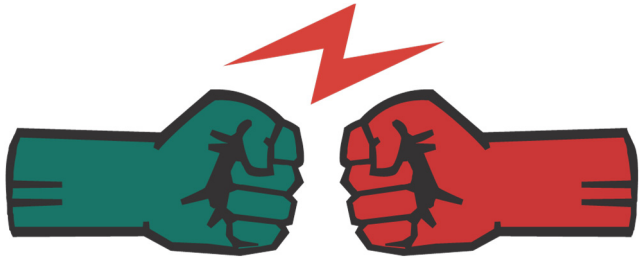
SPYEYE: AUSSPIONIEREN PER WEBCAM



Alles, was Sie am Telefon sagen, wird von Betrügern aufgezeichnet

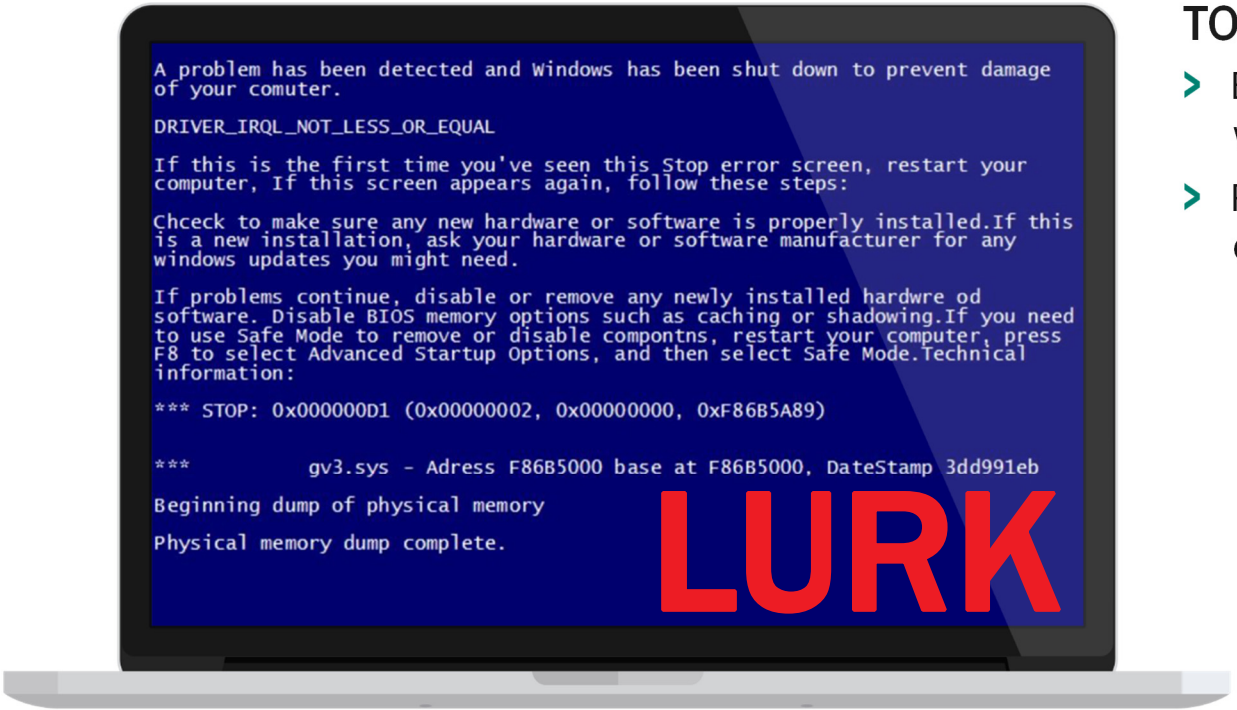
MODERNE SCHUTZMECHANISMEN VON BANKEN VS. BANKING-TROJANER

Authentifizierung:
Token



Lurk

LURK: DISTRIBUTION UND FUNKTIONSPRINZIP



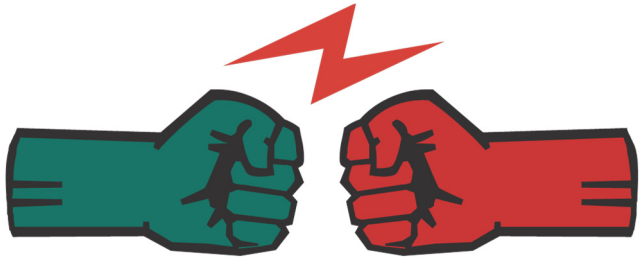
TOKEN-Umgehung:

- Blockiert den Computer, wenn das Token angeschlossen ist
- Remote-Zugriff auf den Computer durch Cyberkriminelle

KASPERSKY lab

BEDROHUNGEN FÜR MOBILE GERÄTE

Einmalkennwörter:
SMS



ZitMo
Zeus in the Mobile

SpitMo
SpyEye in the Mobile

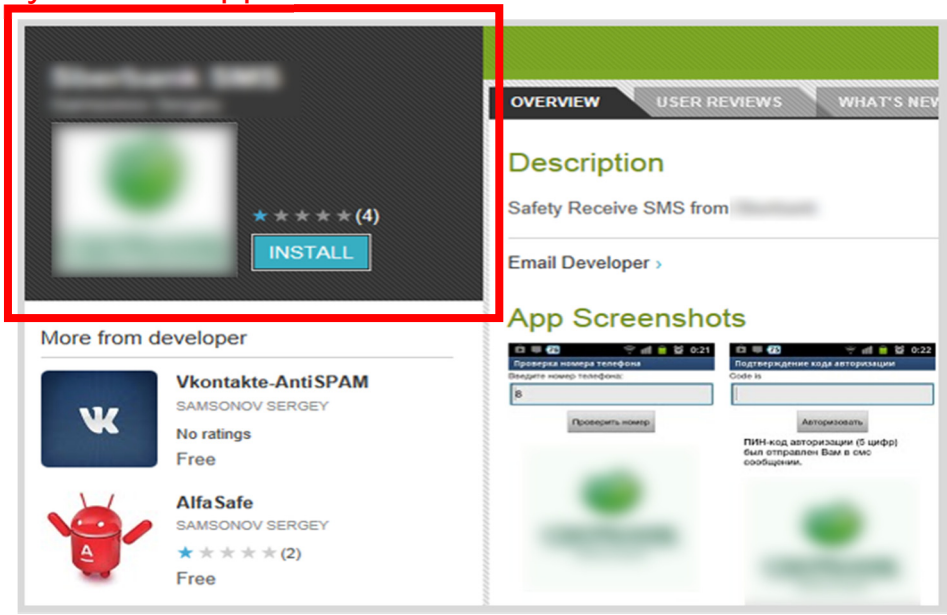
CitMo
Carberp in the Mobile

MOBILE BEDROHUNGEN: EINIGE BEISPIELE

Funktionsweise

- Dem Benutzer wird nahegelegt, sich das Programm aus einem Online-Store herunterzuladen
- Das Programm ist ein Schadprogramm, das nach der Installation SMS-Einmalkennwörter abfängt

CyberSafe App



Diebstahl von SMS-Autorisierungscodes

FAZIT

- Finanz-Malware agiert **immer spezifischer**
- Neue Schutzmaßnahmen von Banken werden **rasch durchbrochen/umgangen**
- Gezielte Angriffe sind immer verbreiteter und beinahe schon Routine
- Es gibt **sehr viele Gelegenheiten** zur Ausnutzung von Schwachstellen

Leistungsfähige
SICHERHEITS-SOFTWARE
ist unerlässlich

GESPRÄCHSBEDARF?

KFP_HQ@kaspersky.com

www.kaspersky.com/fraudprevention

KASPERSKY lab