



RISIKEN BEIM
ONLINE- UND MOBILE-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

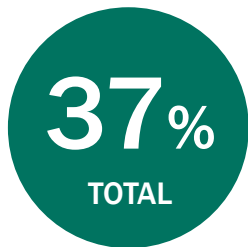
 69%

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

WELCHE ART VON DATENVERLUST FÜRCHTEN NUTZER AM MEISTEN?



Persönliche
E-Mail-Nachrichten



Kennwörter,
Kontodaten



Bank-
daten






BANKÜBERFALL ODER ANGRIFF AUF DEN BENUTZER



- Früher überfielen Kriminelle Banken
- Aber dies ist teuer, aufwendig und riskant
- Heute betrügen sie Online-Benutzer um ihr Geld
- Und leider sind sie dabei sehr erfolgreich

ZUGANGSDATEN WERDEN HEUTE AUF ONLINE-PLATTFORMEN VERKAUFT

<p>Visa Cw 2 \$ per 1</p>  <p>Warranty : 3 day Max buy : 30</p> <p>Min buy : 5 In Stock : 42</p> <p>Buy now quantity</p> <p>5 10 15 20 30</p>	<p>Master Cw 2.5 \$ per 1</p>  <p>Warranty : 3 day Max buy : 30</p> <p>Min buy : 5 In Stock : 42</p> <p>Buy now quantity</p> <p>5 10 15 20 30</p>	<p>Discover Cw 3.5 \$ per 1</p>  <p>Warranty : 3 day Max buy : 30</p> <p>Min buy : 5 In Stock : 42</p> <p>Buy now quantity</p> <p>5 10 15 20 30</p>	<p>Amex Cw 3.5 \$ per 1</p>  <p>Warranty : 3 day Max buy : 30</p> <p>Min buy : 5 In Stock : 42</p> <p>Buy now quantity</p> <p>5 10 15 20 30</p>
<p>50\$ For 500\$ Balance</p>  <p>50\$ For 500\$ Balance</p> <p>Warranty : 3 day Max buy : 3</p> <p>Min buy : 1 In Stock : 13</p> <p>Buy now Buy With Balance</p> <p>500\$ 1000\$ 1500\$ 2000\$ 3000\$ Balance</p>	<p>50\$ For 500\$ Balance</p>  <p>50\$ For 500\$ Balance</p> <p>Warranty : 3 day Max buy : 30</p> <p>Min buy : 5 In Stock : 42</p> <p>Buy now Buy With Balance</p> <p>500\$ 1000\$ 1500\$ 2000\$ 3000\$ Balance</p>	<p>50\$ For 500\$ Balance</p>  <p>50\$ For 500\$ Balance</p> <p>Warranty : 3 day Max buy : 30</p> <p>Min buy : 5 In Stock : 42</p> <p>Buy now Buy With Balance</p> <p>500\$ 1000\$ 1500\$ 2000\$ 3000\$ Balance</p>	<p>50\$ For 500\$ Balance</p>  <p>50\$ For 500\$ Balance</p> <p>Warranty : 3 day Max buy : 30</p> <p>Min buy : 5 In Stock : 42</p> <p>Buy now Buy With Balance</p> <p>500\$ 1000\$ 1500\$ 2000\$ 3000\$ Balance</p>

PROBLEME, AUF DIE BENUTZER IM INTERNET STOSSEN

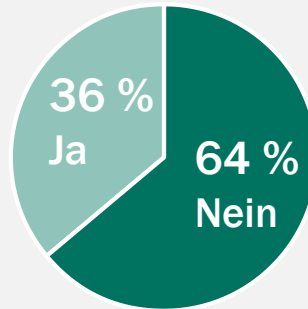
Probleme, auf die
Benutzer im Internet stoßen



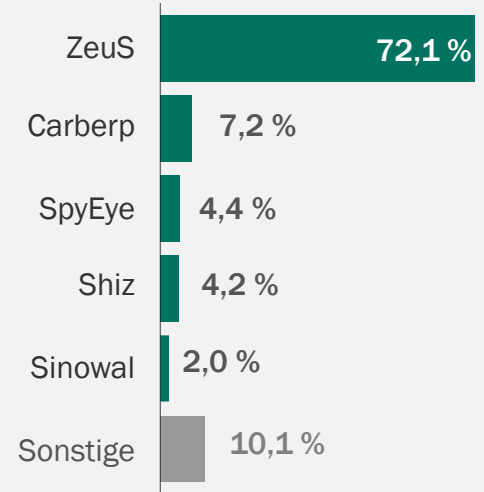
Bei mehr als 25 % der
Verbraucher ist es in den letzten
12 Monaten zu einem Malware-
Vorfall gekommen

36 % der Malware-Vorfälle
führten zu finanziellen Verlusten

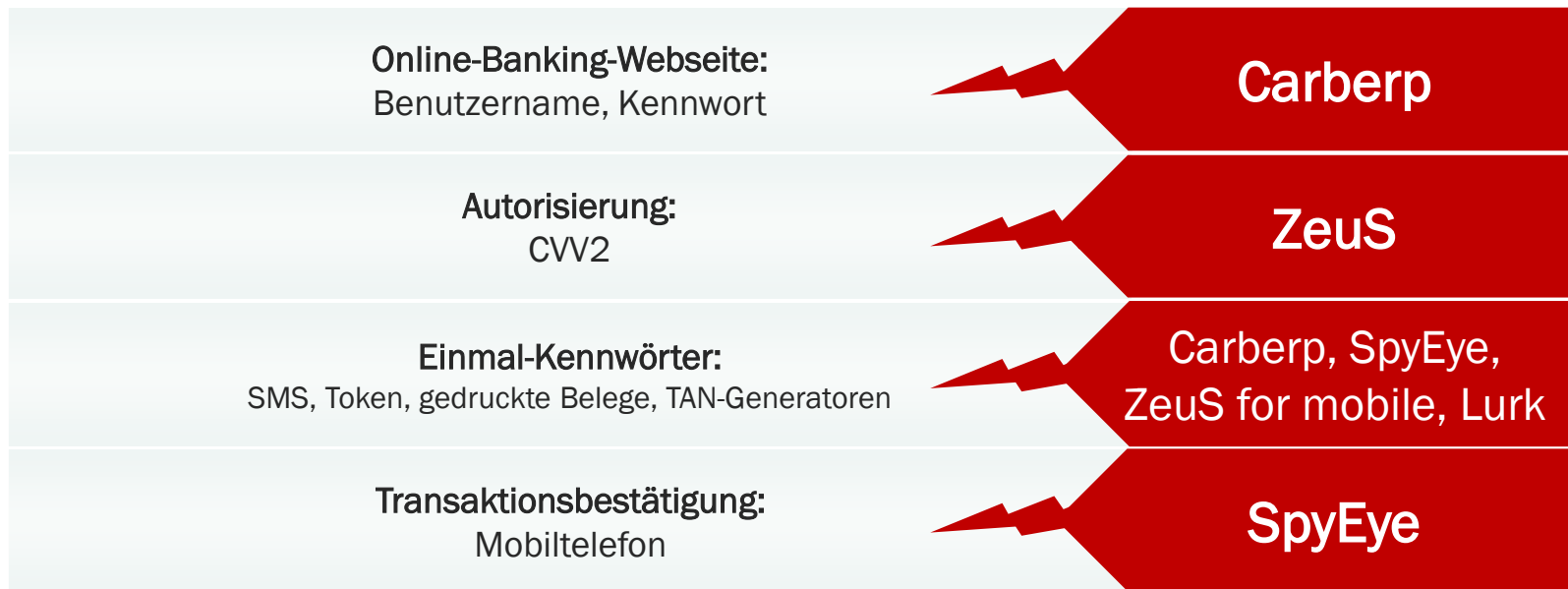
Hatten Sie finanzielle Verluste aufgrund
einer Virus- oder Malware-Infektion?



Banking-Trojaner weltweit

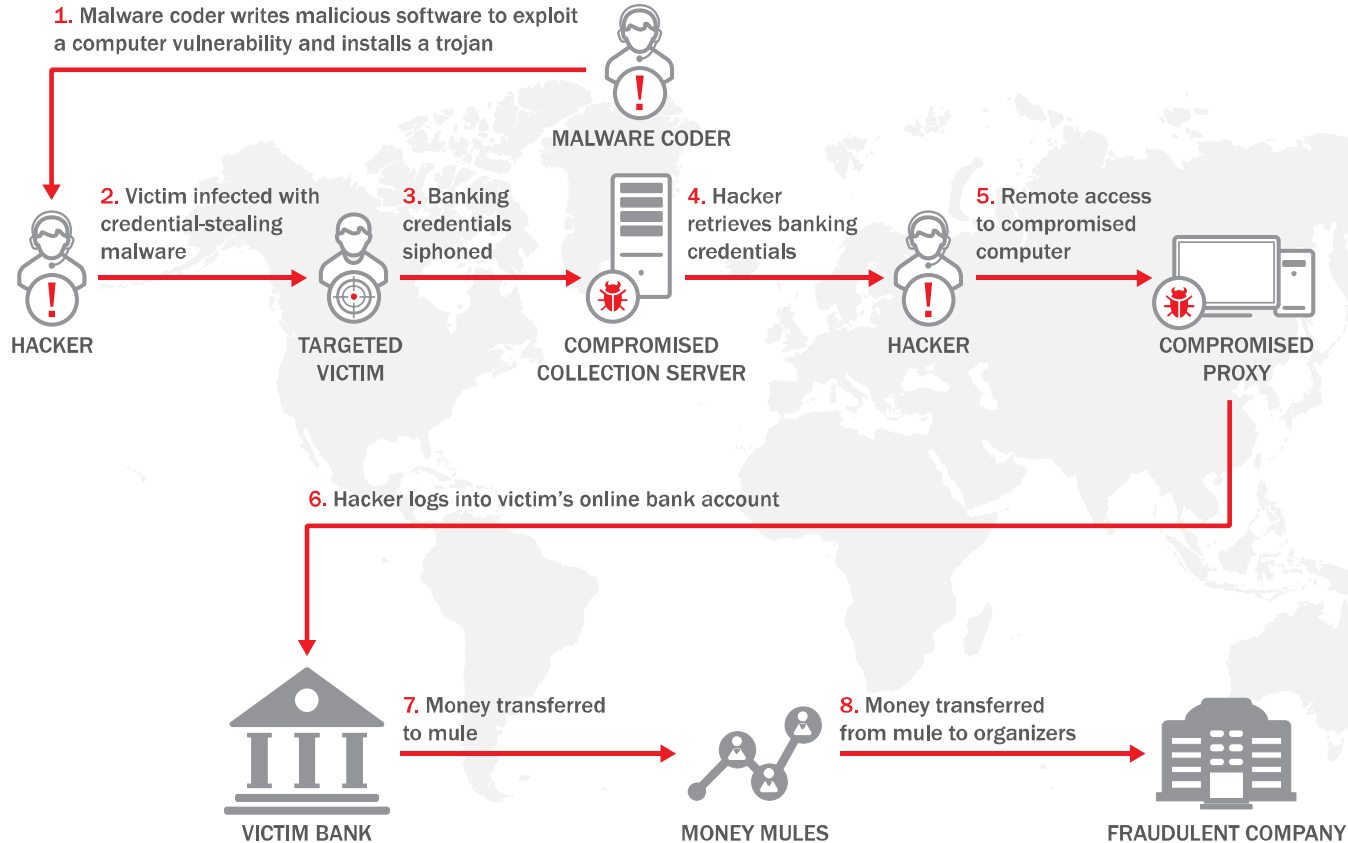


BEKANNTE BANKING-TROJANER UND IHRE ZIELE„UND SIE DACHTEN, SIE SEIEN AUF DER SICHEREN SEITE!“



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



> der am weitesten verbreitete 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: BANKKUNDEN-SOFTWARE + SCHLÜSSEL



Methoden des Datendiebstahls:

- Инъекция в den Webbrowser
- Abfangen von Zahlungsdaten
- Gefälschte Benachrichtigungen/ Popups

MODERNE SCHUTZMECHANISMEN VON BANKEN VS. BANKING-TROJANER

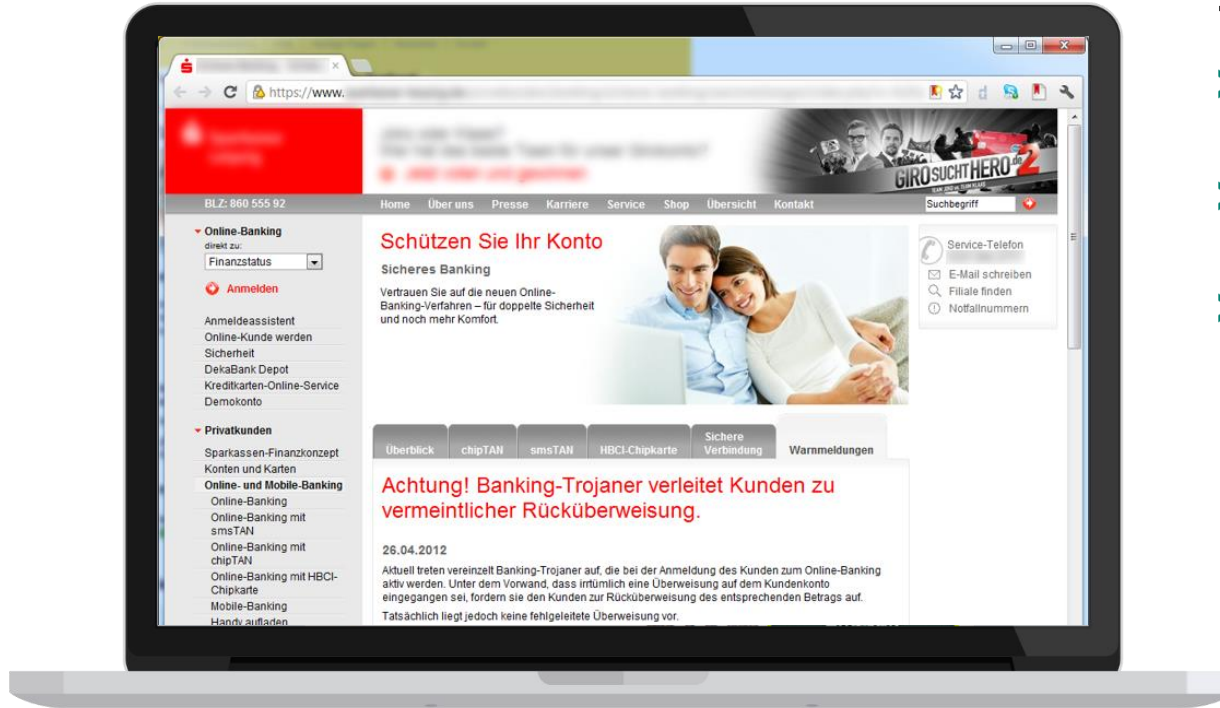
Authentifizierung:

Anmeldenname/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



SPYEYE: CHIPTAN-UMGEHUNG DURCH SOCIAL ENGINEERING

RECENT TRANSACTIONS

03.04.2012	8000	€	Warning 
01.03.2012	75	€	OK
18.01.2012	50	€	OK
<hr/>			
TOTAL	16125	€	

Dem Benutzer wird ein gefälschter Warnhinweis auf der Online-Banking-Seite angezeigt.

RECENT TRANSACTIONS

04.04.2012	-8000	€	OK
03.04.2012	8000	€	OK
01.03.2012	75	€	OK
18.01.2012	50	€	OK
<hr/>			
TOTAL	8125	€	

Dem Benutzer werden gefälschte Informationen zu Überweisungen auf sein Konto angezeigt.



Customer ID

User ID

Password

Generated Token Password

Wire PIN

[Forgot your password?](#)

Der Benutzer wird zur Rückerstattung aufgefordert.



Refund Transfer

Name of recipient's banks:

Recipient's account no.:

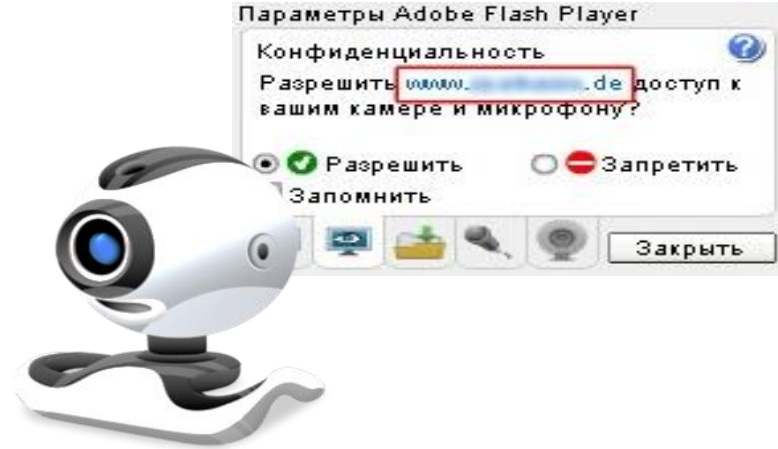
SWIFT:

chipTAN PIN:

Der Benutzer gibt Einmal-Kennwörter 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. Erstaten Sie den Betrag so schnell wie möglich zurück. Vielen Dank!“

SPYEYE: AUSSPIONIEREN PER WEBCAM



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

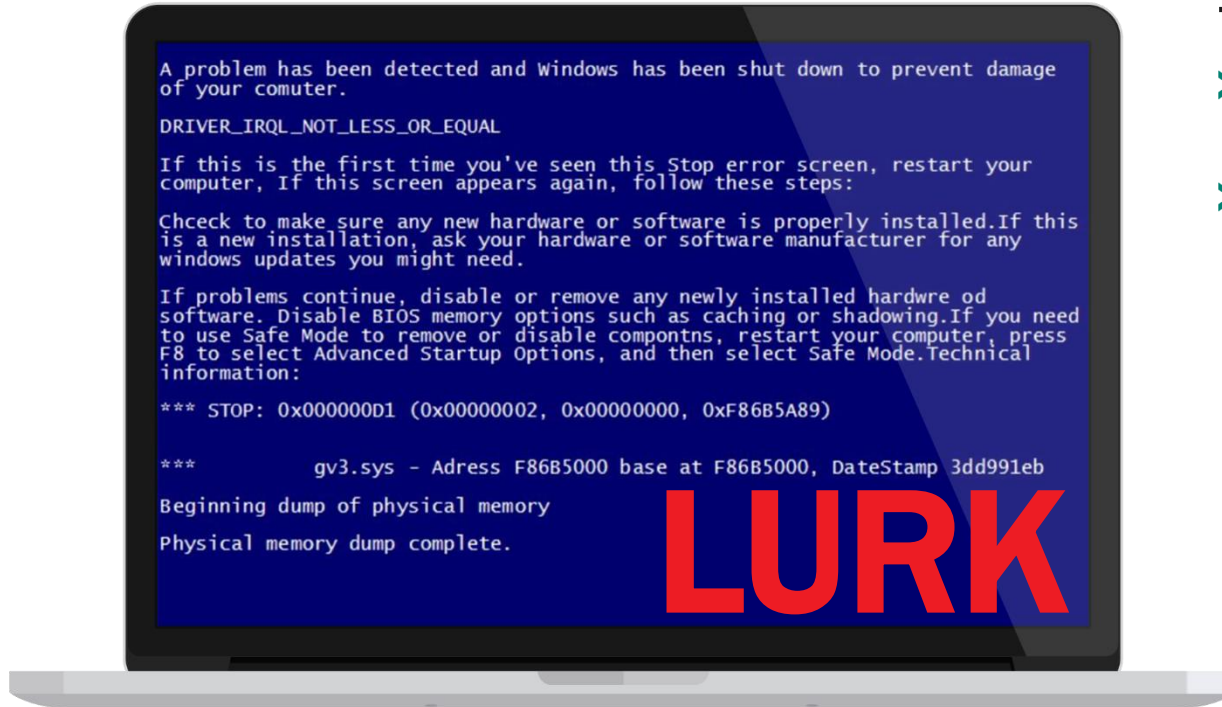
MODERNE SCHUTZMECHANISMEN VON BANKEN VS. BANKING-TROJANER

Authentifizierung:
Token



Lurk

LURK: DISTRIBUTION UND FUNKTIONSPRINZIP



TOKEN-Umgehung:

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

BEDROHUNGEN FÜR MOBILE GERÄTE

Einmalkeennwörter:
SMS



ZitMo

Zeus in the Mobile

SpitMo

SpyEye in the Mobile

CitMo

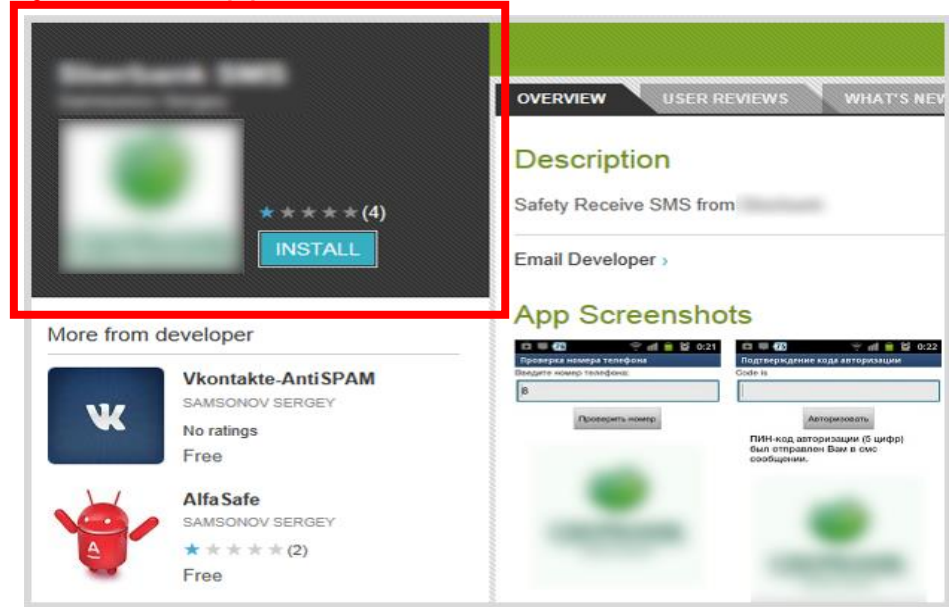
Carberp in the Mobile

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-Einmal-Kennwörter 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 weiter verbreitet und beinahe schon Routine
- Noch immer gibt es **viele Schwachstellen**, die von Cyber-Kriminellen erkannt und genutzt werden

Leistungsfähige
**SICHERHEITS-
SOFTWARE**
ist unerlässlich

GESPRÄCHSBEDARF?

KFP_HQ@kaspersky.com

www.kaspersky.com/fraudprevention