



The background of the slide is a close-up, shallow depth-of-field photograph. It shows a person's hand holding a blue credit card over a laptop keyboard. The keyboard keys are blurred, and the focus is on the edge of the credit card and the hand holding it. The overall color palette is soft and professional, with blues, greys, and skin tones.


ONLINE AND MOBILE BANKING THREATS

ONLINE PAYMENTS ARE VERY POPULAR BUT NOT SECURE



 **98%** of respondents regularly use online banking , online shopping or e-payment services

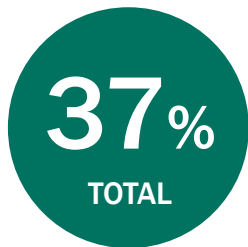
 **59%** of users have concerns about banking fraud online

 **69%** of people fear for the safety of their personal data (including banking credentials)

WHICH TYPE OF DATA LOSS IS MOST CRITICAL TO INTERNET USERS?



Personal
email messages



Passwords,
account details



Banking
details



ATTACKING THE BANK VS. ATTACKING THE USER



- Before criminals used to crack the banks
- But it's too expensive, complicated and risky
- Now they fraud users to steal money from them
- And unfortunately they are very successful in doing that

TODAY CYBERCRIMINALS SELL USER CREDENTIALS IN AN EASY WAY- LIKE IN A SHOP

| | | | |
|--|---|---|---|
| <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> |

PROBLEMS USERS ENCOUNTER WHILE ONLINE

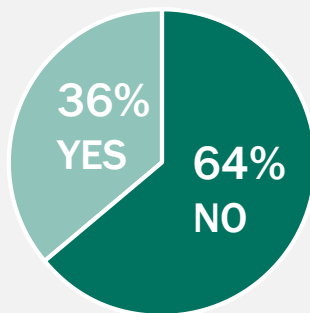
Problems users encounter while online



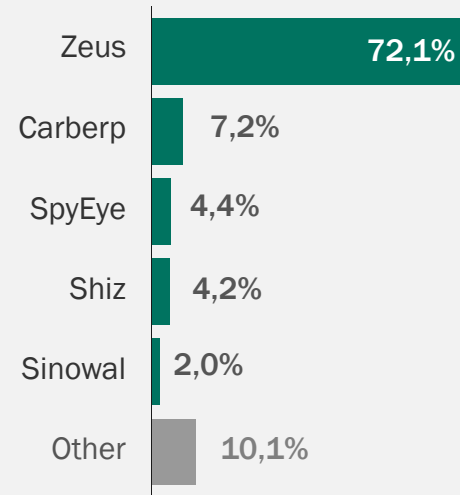
More than 25% of consumers have experienced a malware incident during last 12 months

36% of malware incidents resulted in financial loss

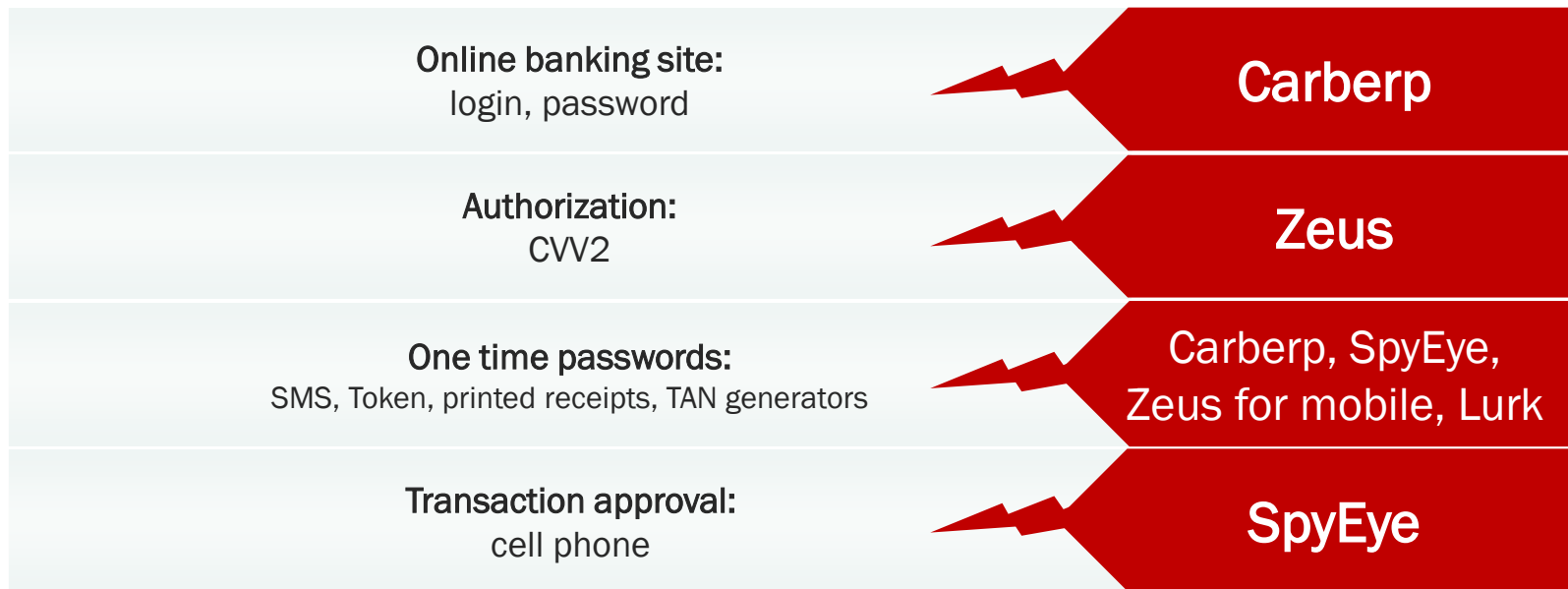
Did you incur any financial costs as a result of a virus / malware infection?



Banking trojans worldwide



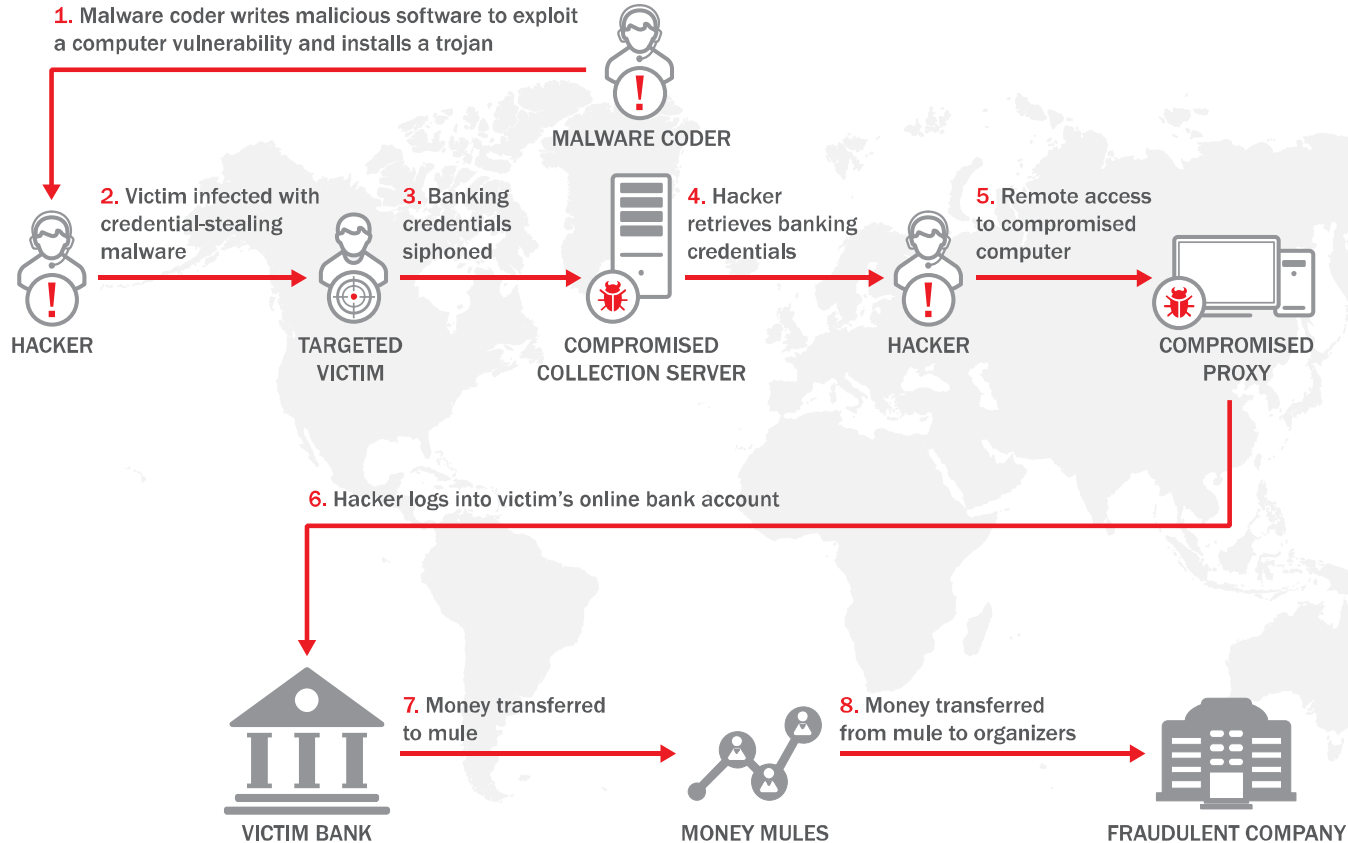
YOU THOUGHT YOU WERE PROTECTING YOUR USERS.....”AND YOU THOUGHT YOU WERE SAFE!”



Read more details in “**Staying safe from virtual robbers**”

http://www.securelist.com/en/analysis/204792304/Staying_safe_from_virtual_robbers

HOW THE FRAUD WORKS



MODERN PROTECTION MECHANISMS USED BY BANKS VS. BANKING TROJANS

Authentication:
login/password, CVV2,
SMS, printed receipts



ZEUS

ZEUS – MAIN FEATURES



> Most widespread online banking trojan out there



> ZeuS tracks which keys the user presses – virtual or physical (keylogging, screenshots)



> ZeuS uses **web injections** – Man in the Browser attacks



> ZeuS is capable of bypassing the most advanced bank security system, bypassing 2-factor authentication systems



> Spreads through **social engineering** and **drive-by downloads**

MODERN PROTECTION MECHANISMS USED BY BANKS VS. BANKING TROJANS

Authentication:
login, password, SMS



Carberp

CARBERP: BANK CLIENT SOFTWARE + KEYS



Data theft technologies:

- Injection in the web browser
- Interception of payment data
- Fake notice/ popups

MODERN PROTECTION MECHANISMS USED BY BANKS VS. BANKING TROJANS

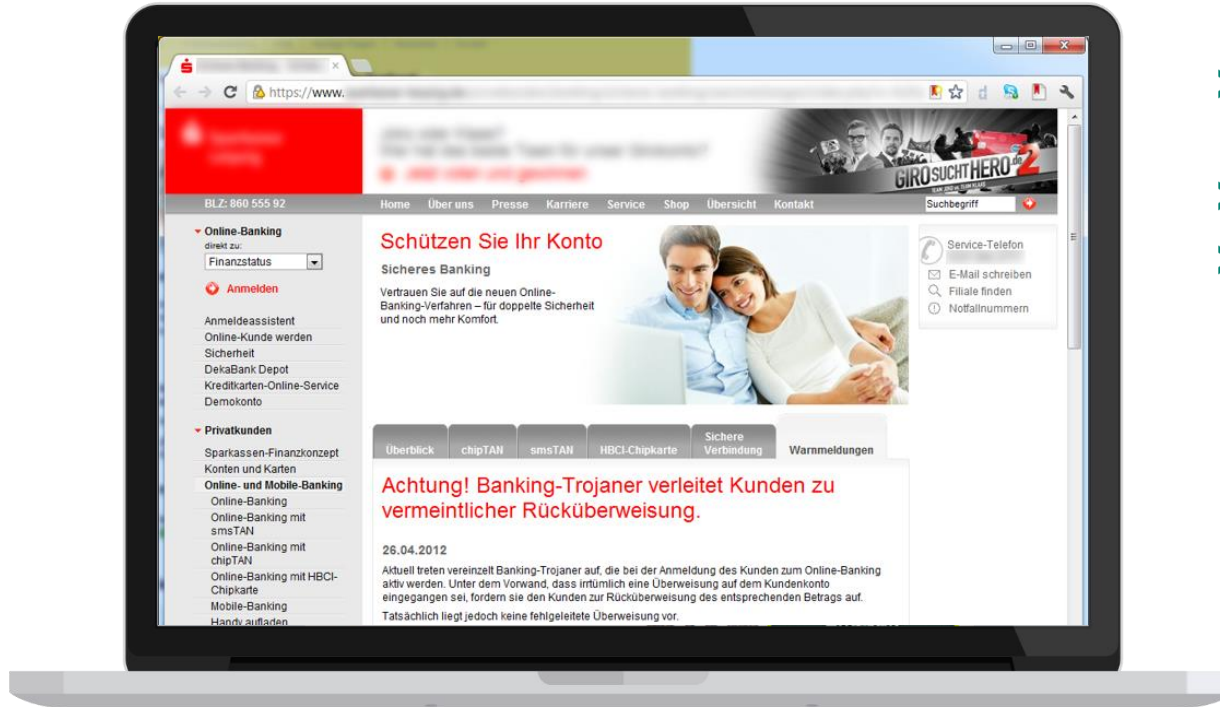
Authentication:

login/password, SMS, Token,
TAN generators, Cam capture



SpyEye

SPYEYE: TAN GENERATORS BYPASS



TAN benefits:

- The user must have the unique device
- The user must know the PIN
- Unique transaction code



SPYEYE: CHIPTAN BYPASS BY MEANS OF SOCIAL ENGINEERING

RECENT TRANSACTIONS

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

User sees fake Warning window on banking page

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 | € | |

User sees fake information about transaction to his account

| | |
|---------------------------------------|--------------------------|
| Customer ID | <input type="text"/> |
| User ID | <input type="text"/> |
| Password | <input type="password"/> |
| Generated Token Password | <input type="text"/> |
| Wire PIN | <input type="text"/> |
| Forgot your password? | |
| <input type="button" value="Login"/> | |

User is requested to refund money

| | |
|---|---|
| Refund Transfer | |
| Name of recipient's banks: | <input type="text" value="Some Euro Bank, a.s. Zurich, Swiss"/> |
| Recipient's account no.: | <input type="text" value="CZXX5500XXXXXXXXXXXXXXXXXX"/> |
| SWIFT: | <input type="text" value="RZXXXXXX"/> |
| chipTAN PIN: | <input type="text" value="██████"/> |
| <input type="button" value="Transfer"/> | |

User enters one time passwords for making transaction... and transfers his own money to cybercriminals

“One of your recent transactions was completed by mistake. You have received some funds that were designated to another recipient. Please refund the money back as soon as possible. Thank you!”

SPYEYE: SPYING VIA A WEBCAM



Everything you say on the phone are recorded by cybercriminals

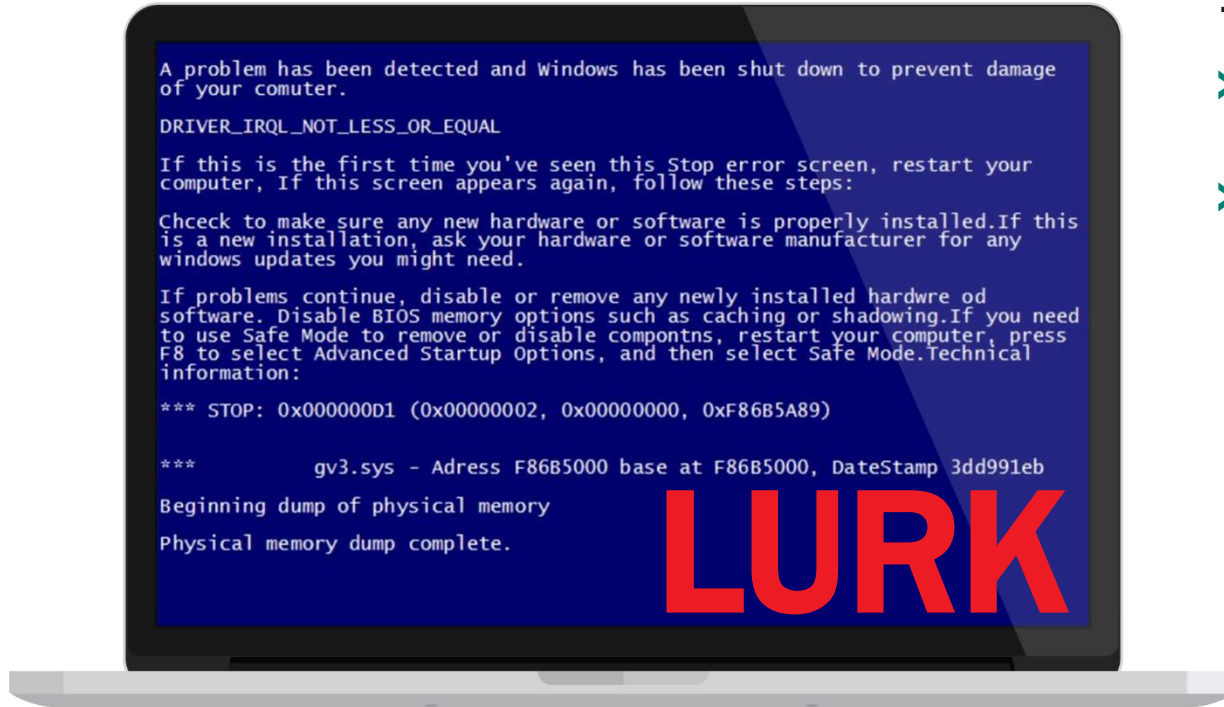
MODERN PROTECTION MECHANISMS USED BY BANKS VS. BANKING TROJANS

Authentication:
Token



Lurk

LURK: DISTRIBUTION AND PRINCIPLES OF WORK



TOKEN Bypass:

- Blocks the workstation when the token is inside
- Remote access to the workstation for cybercriminals

MOBILE THREATS

One time passwords:
SMS



ZitMo

Zeus in the Mobile

SpitMo

SpyEye in the Mobile

CitMo

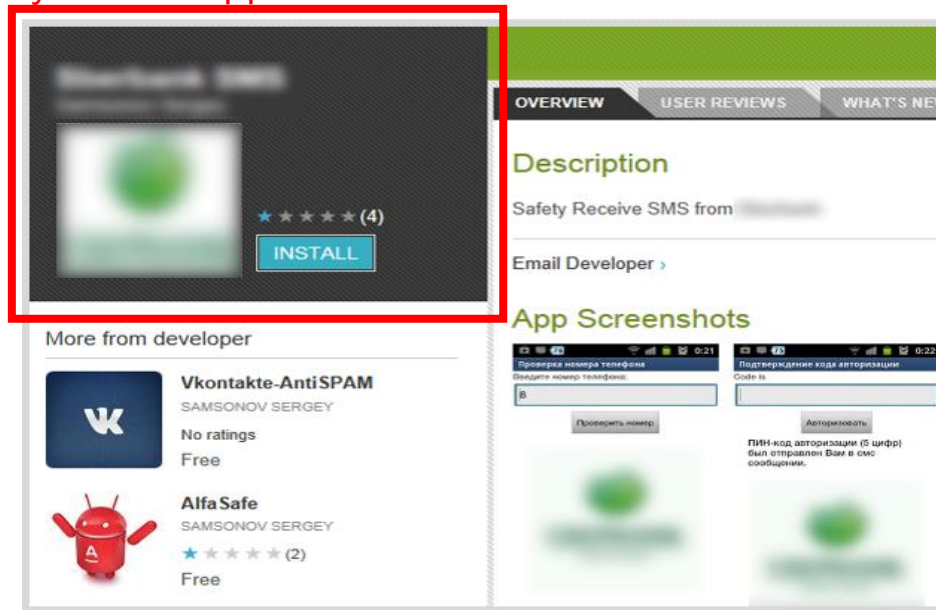
Carberp in the Mobile

MOBILE THREATS: FEW EXAMPLES

How it works

- By means of social engineering user is advised to download the app from an online store
- The app is malicious, once it's installed it steals one time SMS authentication passwords

CyberSafe App



SMS Authorization codes stealing

CONCLUSIONS

- Financial malware is getting **more targeted**
- New protection measures introduced by banks are **quickly cracked/bypassed**
- Targeted attacks are getting widespread and almost becoming a routine
- There is **a lot of space** for vulnerability exploitation

Effective
**SECURITY
SOFTWARE**
is a must

LET'S TALK?

KFP_HQ@kaspersky.com

www.kaspersky.com/fraudprevention

