

# Social Engineering (SE)

BeerTalk

Berlin, 17. Februar 2015

Walter Sprenger

## Introduction to Social Engineering

- ✦ Attack / Spoofing vectors
- ✦ Phishing Sites / Trojan Horses

## Live Demos

## Compass Experience

- ✦ Countermeasures
- ✦ Social Engineering Test Benefits

# What is Social Engineering?

Compass Security  
Deutschland GmbH  
Tauentzienstr. 18  
De-10789 Berlin

Tel. +49 30 21 00 253-0  
Fax +49 30 21 00 253-69  
team@csnc.de  
www.csnc.de

# What is social engineering?



A vertical decorative image on the left side of the slide shows a close-up of a computer keyboard with a yellow padlock resting on one of the keys. A solid dark blue vertical bar is positioned to the left of the keyboard image.

## Attack Vectors / Spoofing Methods

Compass Security  
Deutschland GmbH  
Tauentzienstr. 18  
De-10789 Berlin

Tel. +49 30 21 00 253-0  
Fax +49 30 21 00 253-69  
team@csnc.de  
www.csnc.de

# Attack & Spoofing Vectors



Social Networks



Impersonation



Drive-by-Infection



Baiting



Phishing



Fingerprinting



E-Mail Infection



Phone



Malicious Website



Dumpster Diving

## Why do you trust a message?

- ✦ I know the sender (phone number, mail-address)
- ✦ I know the structure of the message
- ✦ I expect the message

## Why do you trust a web site?

- ✦ I know the domain of the website
- ✦ I know how the web site looks like
- ✦ I trust the seal on the web site
- ✦ I trust the SSL/TLS certificate

Why make a lot of noise if one victim provides the information I want?

- ✦ Run attack to only a few individuals
- ✦ Take more time on one individual, better preparation of the attack

## Targeted Attacks

- ✦ Do not raise suspicion
- ✦ No AntiVirus patterns for used malware
- ✦ Hard to detect in log files / with intrusion prevention systems
- ✦ Longer infection possible, restart malware everytime the user logs in – long time compromise



A vertical decorative strip on the left side of the slide features a close-up photograph of a computer keyboard with a yellow padlock resting on one of the keys. A solid dark blue vertical bar is positioned to the left of the keyboard image.

## Phishing Sites

Compass Security  
Deutschland GmbH  
Tauentzienstr. 18  
De-10789 Berlin

Tel. +49 30 21 00 253-0  
Fax +49 30 21 00 253-69  
team@csnc.de  
www.csnc.de

# Simple Phishing Website



Microsoft Office Outlook Web Access

Security ( [show explanation](#) )

- This is a public or shared computer
- This is a private computer

Use Outlook Web Access Light

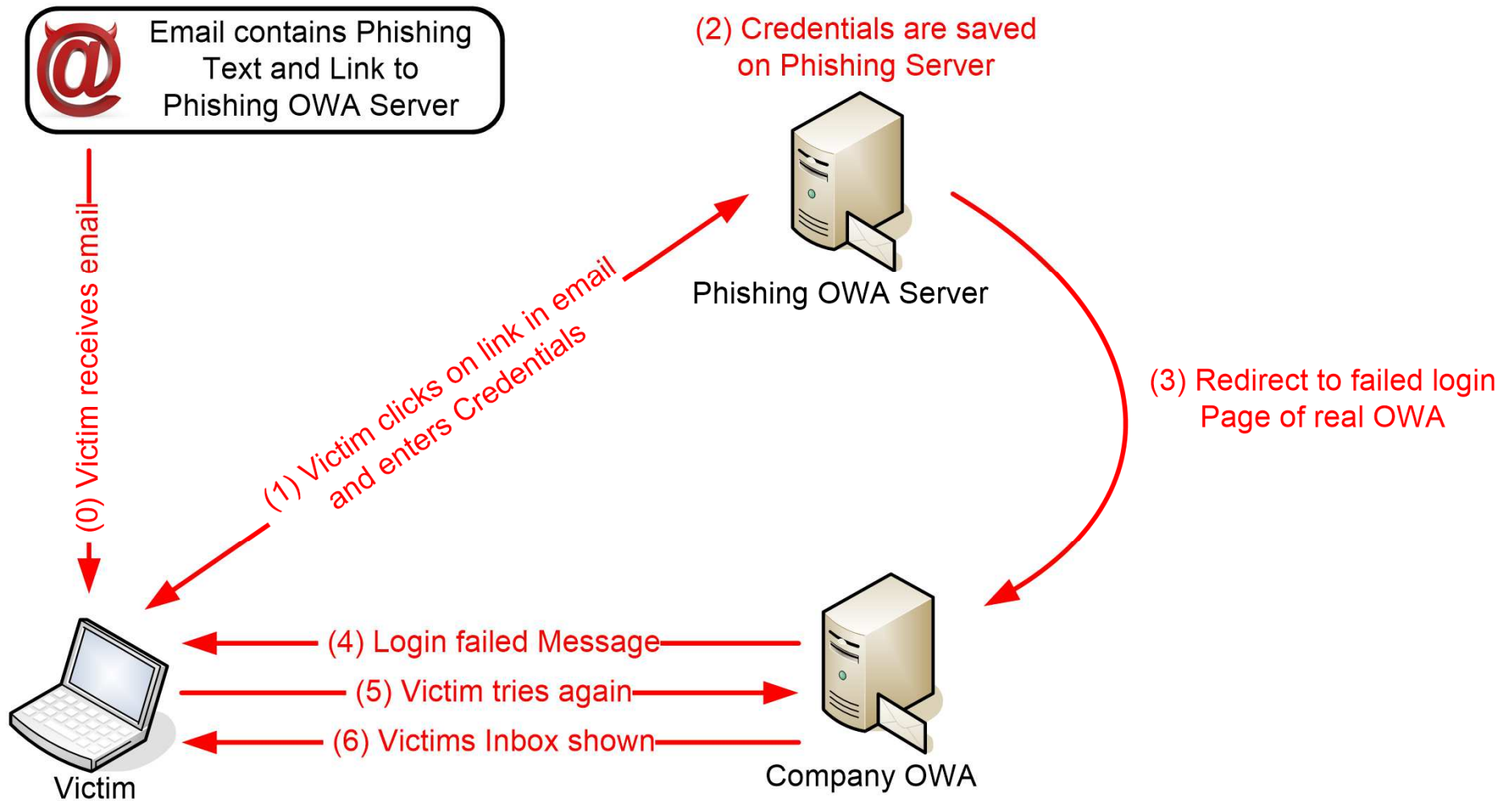
Domain\user name:

Password:

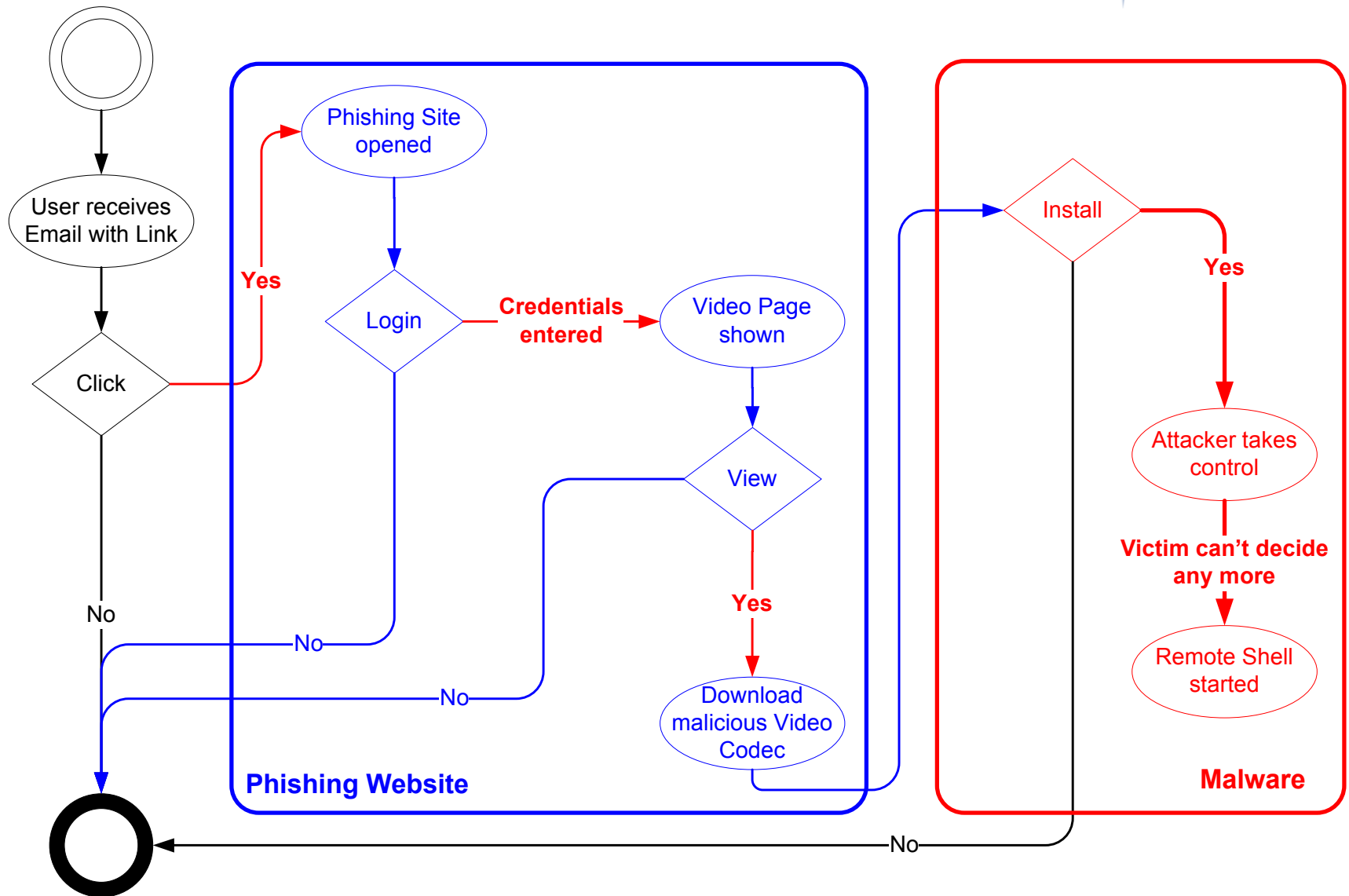
Connected to Microsoft Exchange  
© 2007 Microsoft Corporation. All rights reserved.

The image shows a screenshot of a phishing website designed to look like the Microsoft Office Outlook Web Access login page. It features a blue gradient background and the Microsoft logo. The page includes a security section with radio buttons for "public or shared computer" (which is selected) and "private computer", and a checkbox for "Use Outlook Web Access Light". Below this are two yellow input fields for "Domain\user name:" and "Password:", followed by a "Log On" button. At the bottom, there is a small icon and text indicating a connection to Microsoft Exchange and a copyright notice for 2007 Microsoft Corporation.

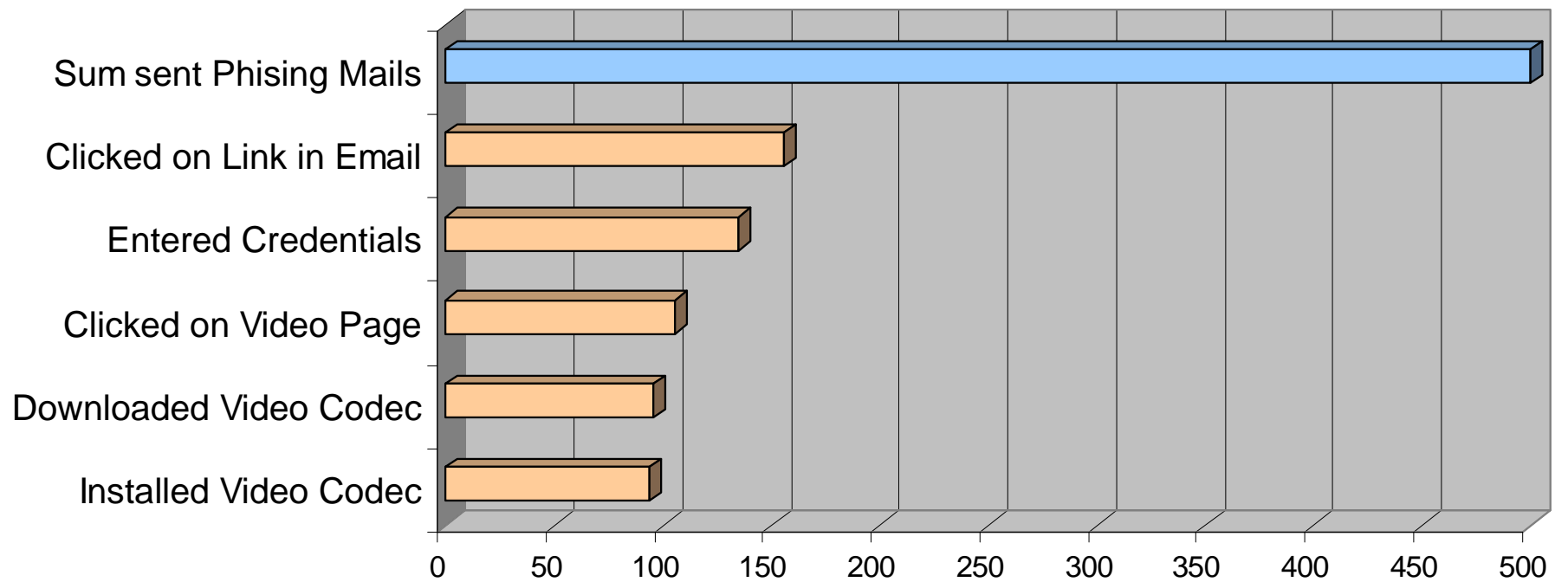
# Simple Phishing Website explained



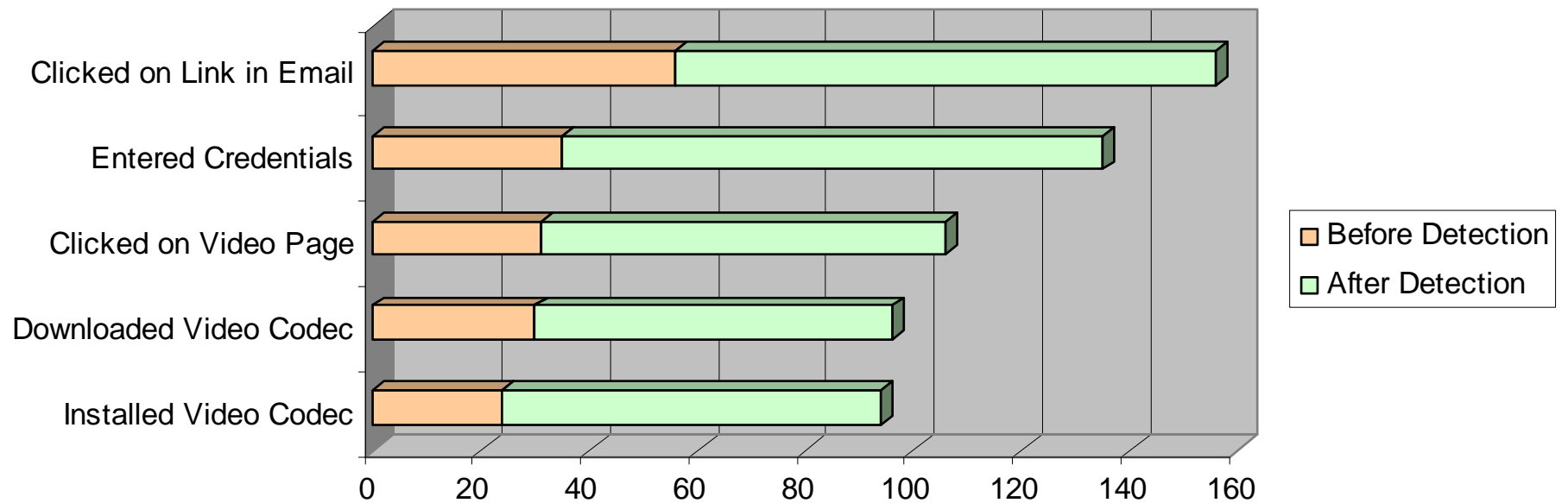
# Example of complex Phishing Site



# Analysis of complex Phishing Sites



## Analysis of complex Phishing Sites (2)



The title "Trojan Horses" is written in a blue, sans-serif font. To the left of the text is a vertical decorative bar with a blue-to-white gradient. The background of the slide is a light blue, slightly blurred image of a computer keyboard, with a yellow padlock resting on one of the keys.

# Trojan Horses

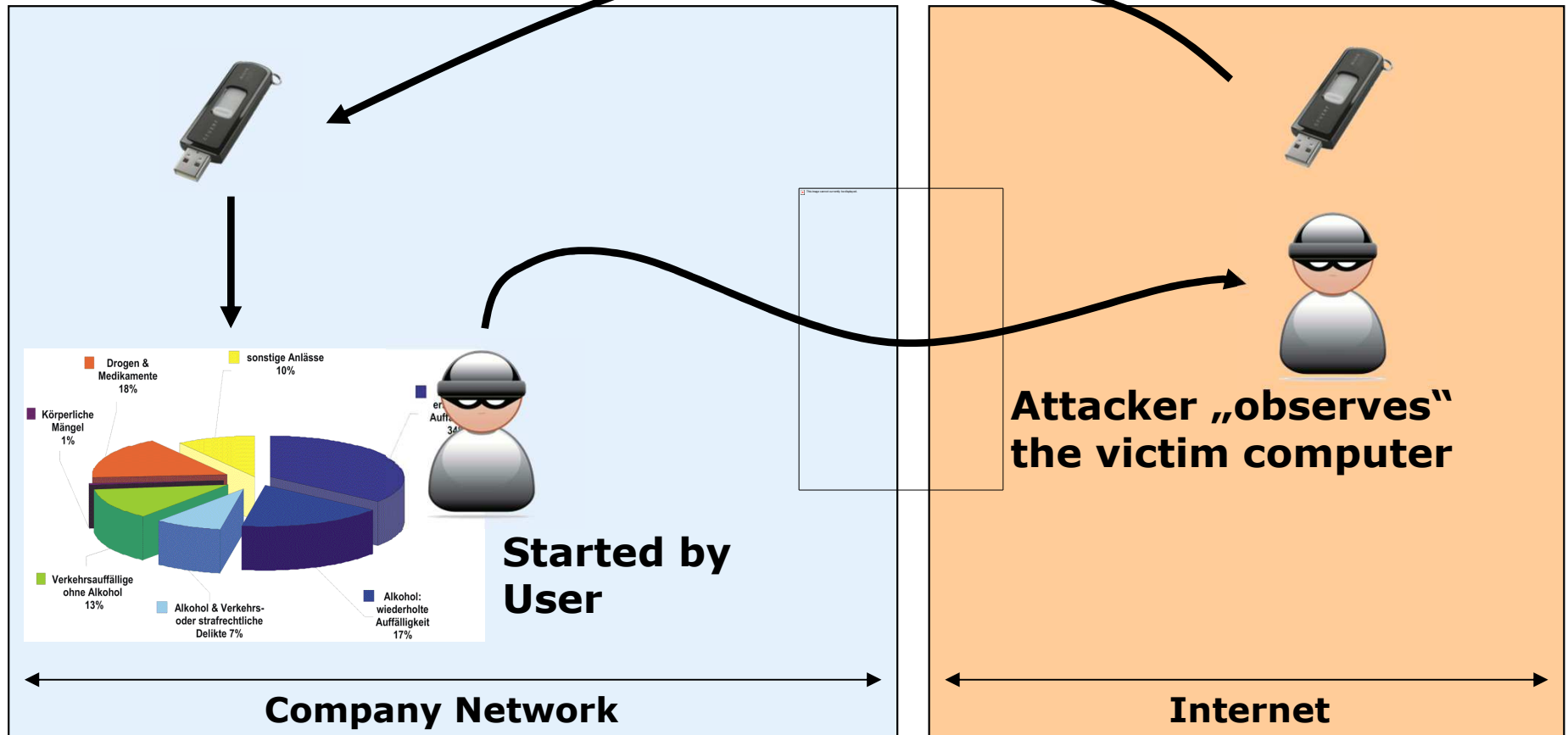
Compass Security  
Deutschland GmbH  
Tauentzienstr. 18  
De-10789 Berlin

Tel. +49 30 21 00 253-0  
Fax +49 30 21 00 253-69  
team@csnc.de  
www.csnc.de

# Trojan Horse

## Covert Channel

### Delivery via USB-Stick







## Live Demos

Compass Security  
Deutschland GmbH  
Tauentzienstr. 18  
De-10789 Berlin

Tel. +49 30 21 00 253-0  
Fax +49 30 21 00 253-69  
team@csnc.de  
www.csnc.de

## A1) Webmail Phishing

- ✦ Attack Vector:
  - ✦ eMail with URL
- ✦ Goal:
  - ✦ Get Webmail/Windows credentials

## A2) FaceBook Phishing (Invitation)

- ✦ Attack Vector:
  - ✦ eMail with Facebook invitation
- ✦ Goal:
  - ✦ Get Facebook credentials / Impersonation

## B1) SMS from your Bank

- ✦ Attack Vector:
  - ✦ SMS with call back number
- ✦ Goal:
  - ✦ Get personal information

## B2) GPS location

- ✦ Attack Vector:
  - ✦ SMS with URL to location web site
- ✦ Goal:
  - ✦ Get coordinates of victim

## B3) iCloud Phishing

- ✦ Attack Vector:
  - ✦ SMS with URL to phishing web site
- ✦ Goal:
  - ✦ Get iCloud credentials
  - ✦ Steal data stored in iCloud (contacts, files, backup, etc.)

## B4) Android NFC Business Card

- ✦ Attack Vector:
  - ✦ Business card with modified NFC, points to phishing web site
- ✦ Goal:
  - ✦ Get Google credentials
  - ✦ Steal data stored on Google (mails, contacts, files, etc.)
  - ✦ Install trojan app on mobile phone

## B5) CallID Spoofing

- ✦ Attack Vector:
  - ✦ Call with spoofed sender number
- ✦ Goal:
  - ✦ Get personal information

## C1) Exe in Word-Dokument

- ✦ Attack Vector:
  - ✦ Mail with Word-Document
- ✦ Goal:
  - ✦ Remote control the workstation of the user

## C2) Download EXE

- ✦ Attack Vector:
  - ✦ Facebook chat message – download URL
- ✦ Goal:
  - ✦ Remote control the workstation of the user

## C3) USB Trojan

- ✦ Attack Vector:
  - ✦ USB stick with interesting file (EXE)
- ✦ Goal:
  - ✦ Remote control the workstation of the user

## D1) Drive-By Java 0-Day

- ✦ Attack Vector:
  - ✦ Web site with URL
- ✦ Goal:
  - ✦ Remote control the workstation of the user

A vertical decorative strip on the left side of the slide features a close-up photograph of a computer keyboard with a yellow padlock resting on one of the keys. A solid dark blue vertical bar is positioned to the left of the keyboard image.

## Countermeasures

Compass Security  
Deutschland GmbH  
Tauentzienstr. 18  
De-10789 Berlin

Tel. +49 30 21 00 253-0  
Fax +49 30 21 00 253-69  
team@csnc.de  
www.csnc.de



# But, you can protect your Company



- ✦ Technical Countermeasures
  - ✦ Virus Scanner
  - ✦ Disable Autorun / USB / CD-ROM
  - ✦ Disable dangerous attachments in Emails
  - ✦ Firewalls / Content Filter / SSL-Split-Proxy
  - ✦ IDS
  - ✦ Protocol Sanitation (HTTP / DNS)
  - ✦ Limit user permissions
  - ✦ Secure WLAN
  
- ✦ Organizational Countermeasures
  - ✦ Access Control
  - ✦ Security Zones
  - ✦ Educate Employees – User Awareness
  - ✦ Security Policies
  - ✦ Awareness Demo
  - ✦ Social Engineering Test

# Social Engineering Test Benefits

Compass Security  
Deutschland GmbH  
Tauentzienstr. 18  
De-10789 Berlin

Tel. +49 30 21 00 253-0  
Fax +49 30 21 00 253-69  
team@csnc.de  
www.csnc.de

I know Social Engineering always works.

So why should I conduct a Social Engineering Test in my company?

# Social Engineering Test Benefits



Technical Infrastructure – Sufficient?

Incident Handling – Adequate?

Security Awareness Courses – Learning Success?

Security Processes – No Weak Points?

Access Control – Impenetrably?

Thank you!



Thank you very much  
for your attention!

# Contact



## Compass Security Deutschland GmbH

Taentzienstr. 18  
10789 Berlin

team@csnc.de | www.csnc.de | +49 30 21 00 253-0

 Secure File Exchange: [www.csnc.ch/filebox](http://www.csnc.ch/filebox)

