Social Engineering (SE)

BeerTalk

Berlin, 17. Februar 2015

Walter Sprenger

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

Agenda

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?

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

Misuse of Trust

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

Targeted Attacks

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

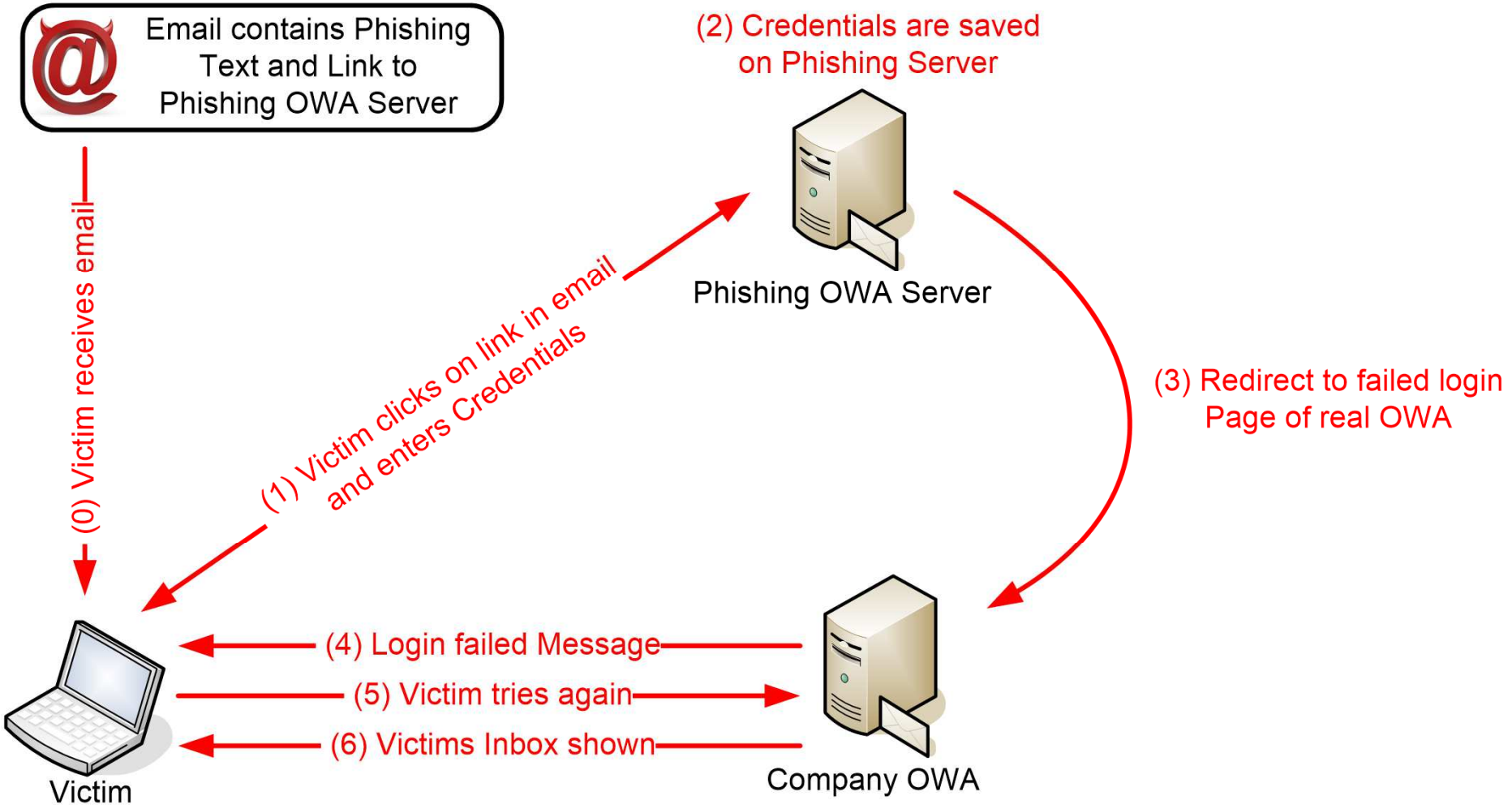
Phishing Sites

Compass Security
Deutschland GmbH
Tauentzienstr. 18
De-10789 Berlin

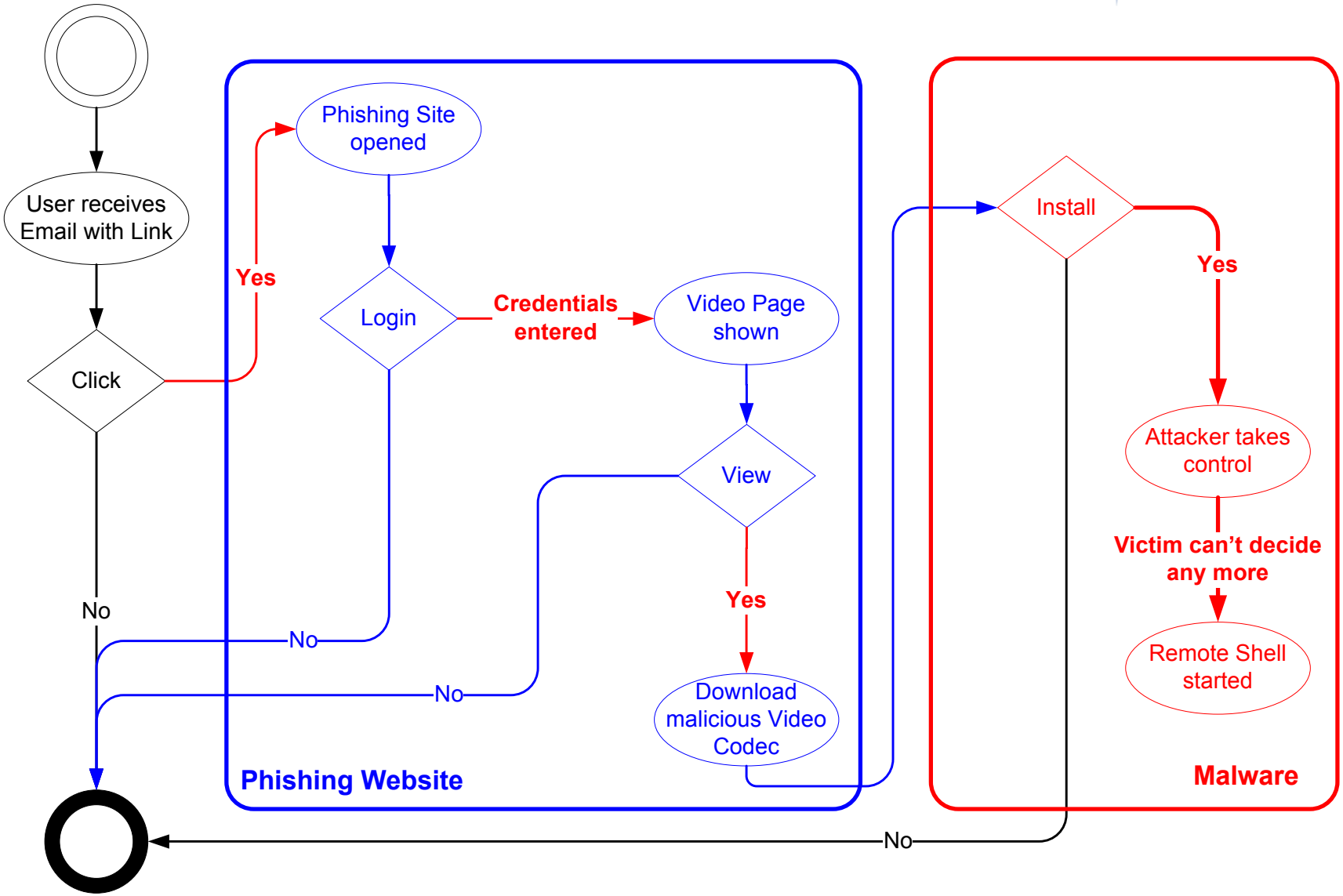
Tel. +49 30 21 00 253-0
Fax +49 30 21 00 253-69
team@csnc.de
www.csnc.de

Simple Phishing Website

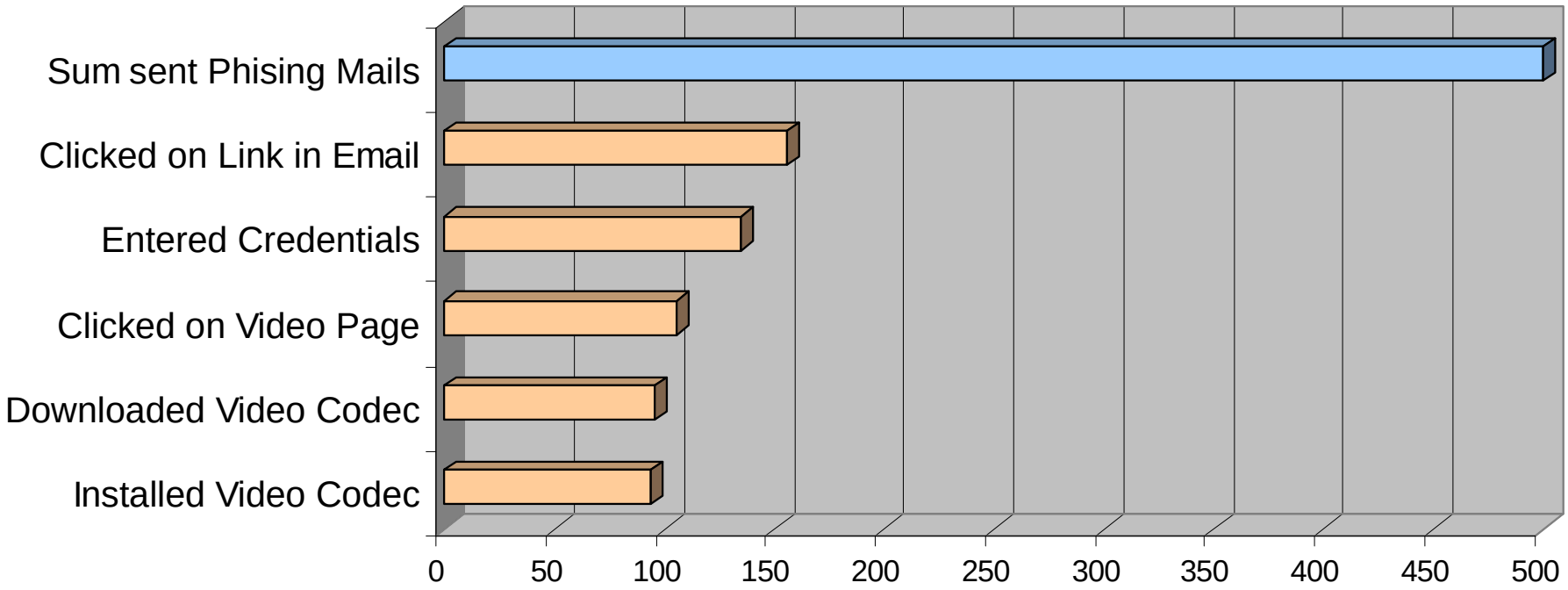
Simple Phishing Website explained



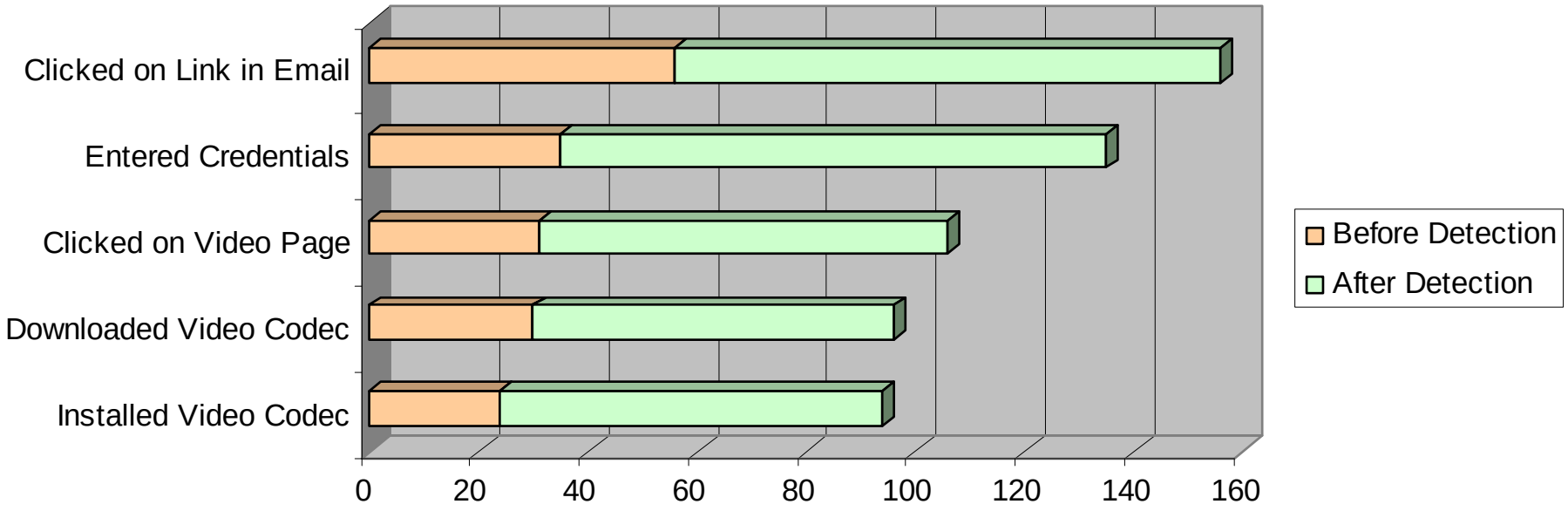
Example of complex Phishing Site



Analysis of complex Phishing Sites



Analysis of complex Phishing Sites (2)



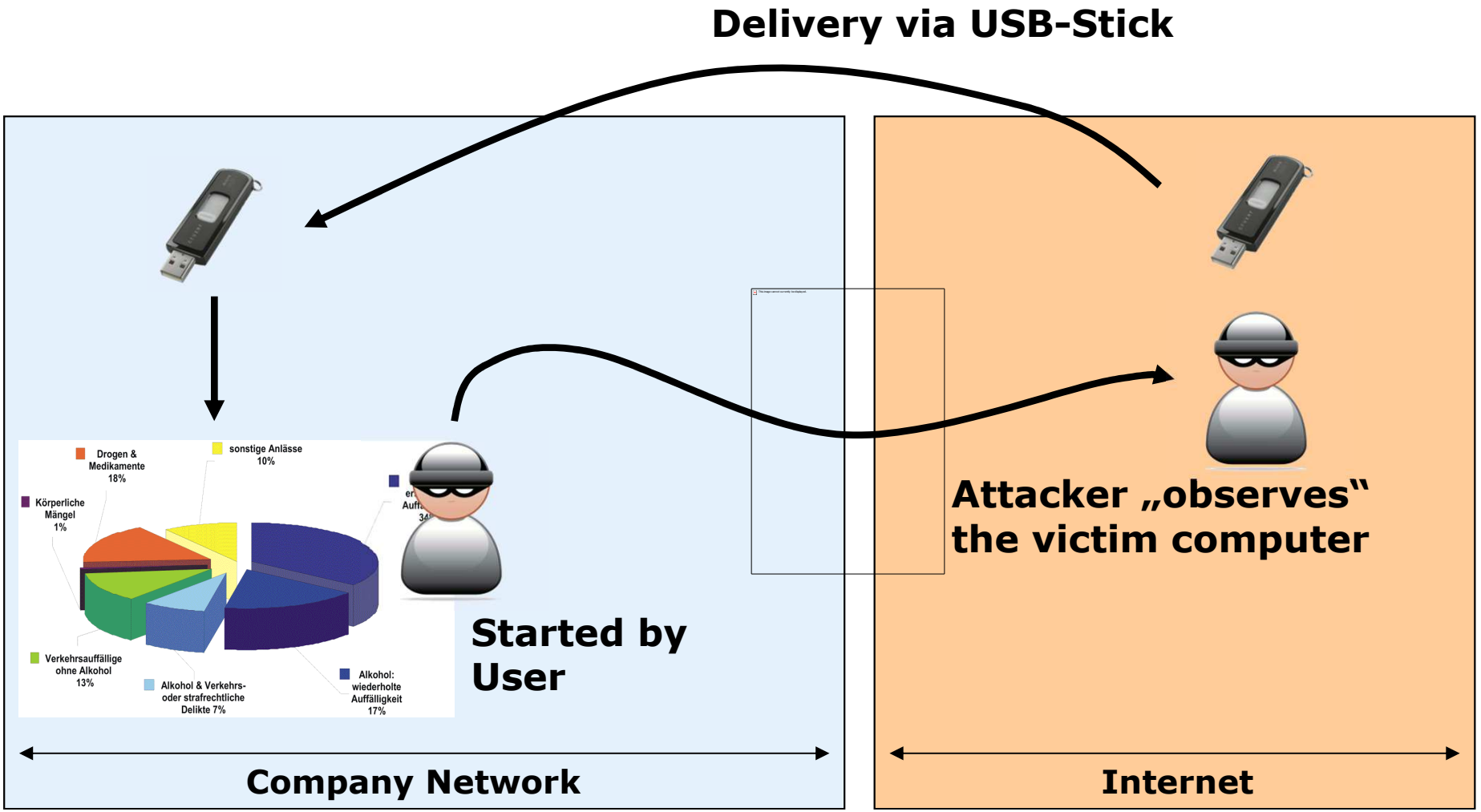
Trojan Horses

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



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

Live Demo – Computer Phishing

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

Live Demo – SmartPhone Information

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

Live Demo – SmartPhone Phishing

B3) iCloud Phishing

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

B4) Android NFC Business Card

- Attack Vector:
  - Business card with modifed 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

Live Demo – CallID Spoofing

B5) CallID Spoofing

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

Live Demo – Trojan User Interaction

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

Live Demo – Trojan DriveBy

D1) Drive-By Java 0-Day

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

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 attachements 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

Social Engineering Test Benefits

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 very much for your attention!

Contact

Compass Security Deutschland GmbH

Tauentzienstr. 18
10789 Berlin

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

Secure File Exchange: www.csnc.ch/filebox