Social Engineering / SmartPhone and DriveBy

Beer-Talk Compass Security AG, October 25, 2012

Walter Sprenger

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Agenda

Introduction to Social Engineering

- Attack/spoofing vectors
- Phishing Sites / Trojan Horses

Live Demos

Compass Experience

- Numbers and Facts
- Social Engineering Pitfalls
- Countermeasures

Social Engineering Test Benefits

What is Social Engineering?

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

What is social engineering?

Attack Vectors / Spoofing Methods

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Attack vectors

Social Networks

Impersonation

Drive-by-Infection

Baiting

Phishing

Fingerprinting

E-Mail Infection

Phone

Malicious Website

Dumpster Diving

Spoofing Methods

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 only provide data on secured web sites

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 AntiVir 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

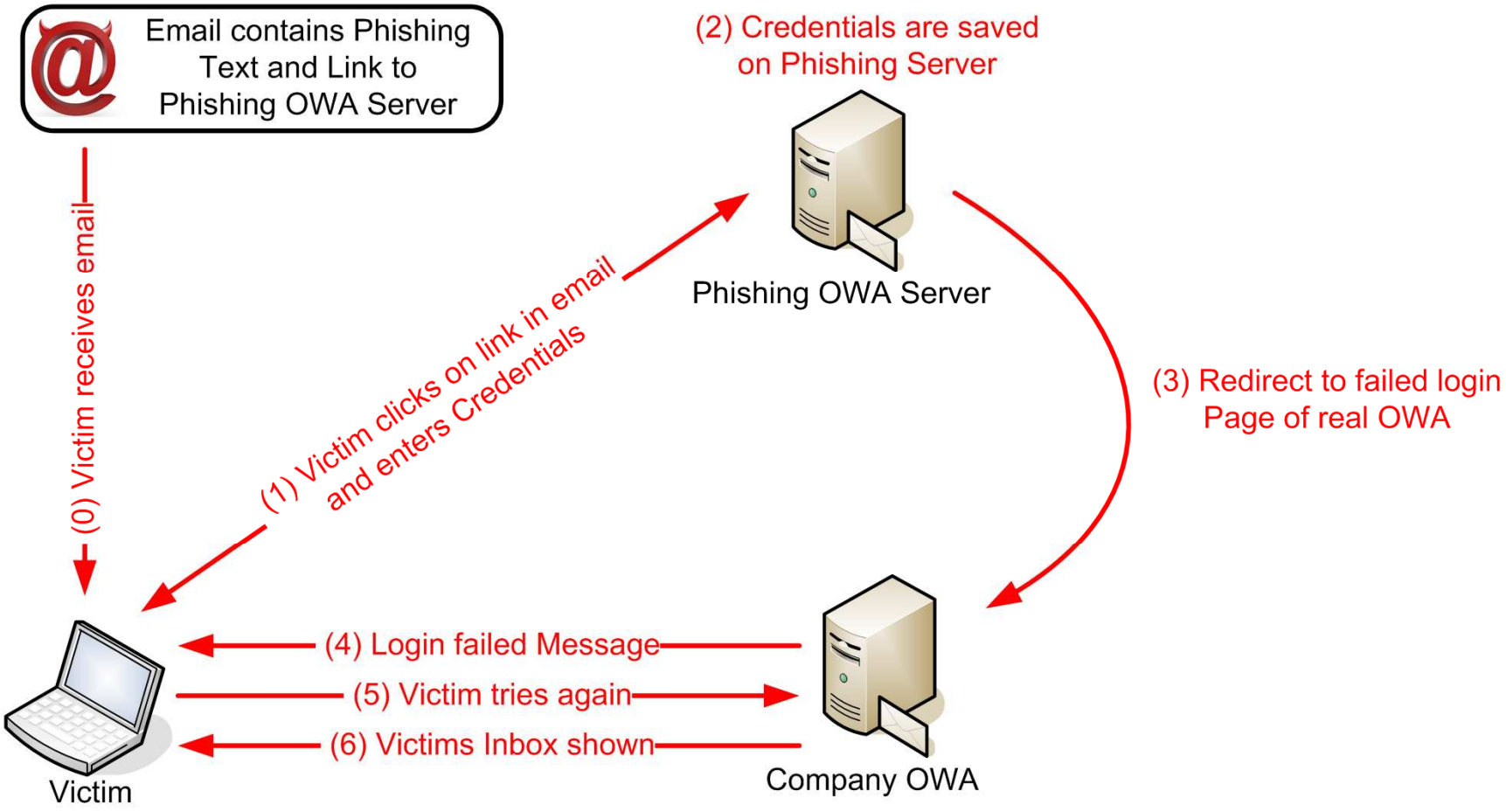
Phishing Sites

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

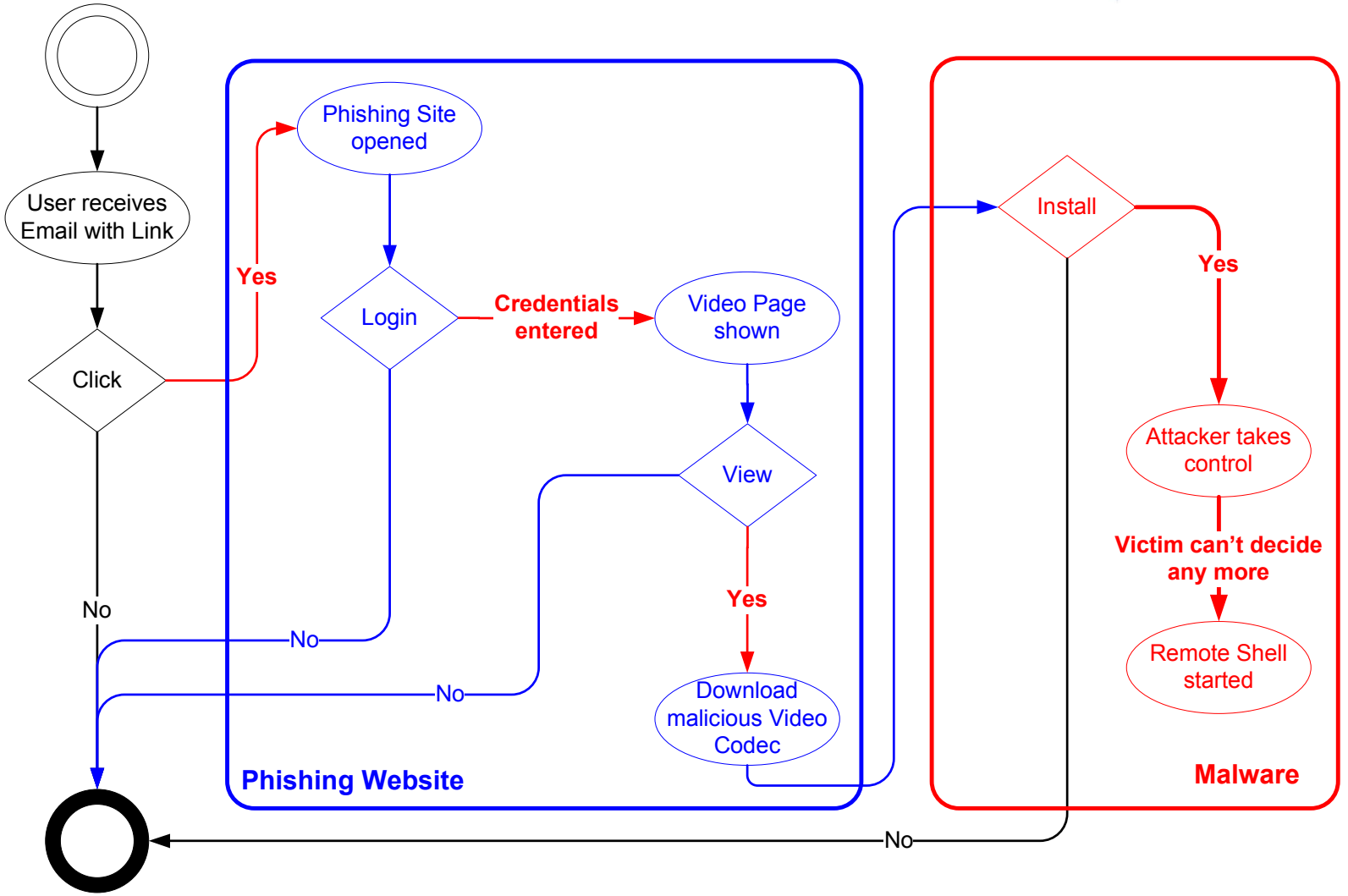
Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Simple Phishing Website

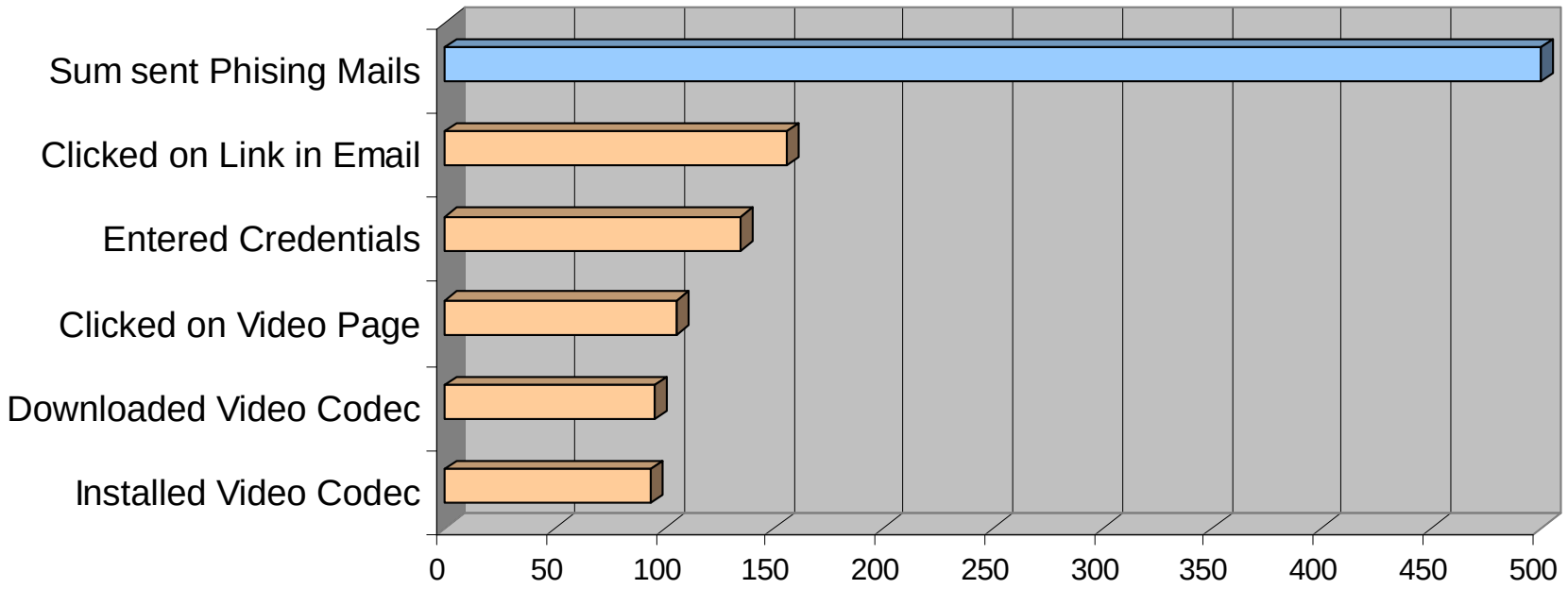
Simple Phishing Website explained



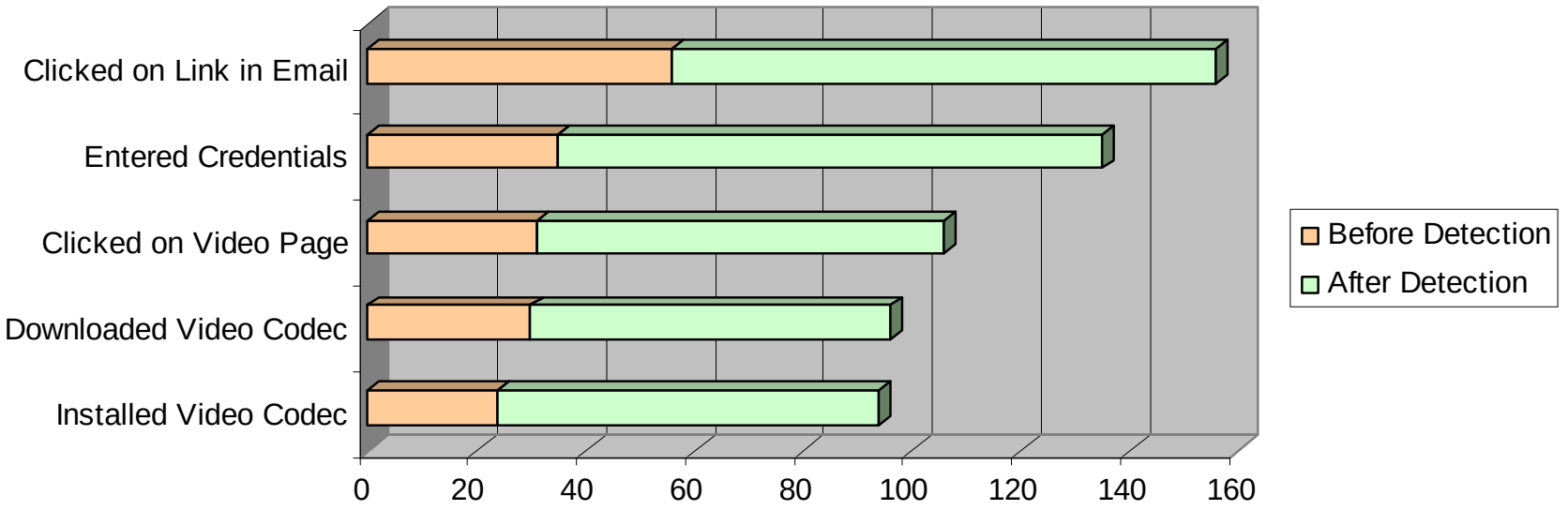
Example of complex Phishing Site



Analysis of complex Phishing Sites



Analysis of complex Phishing Sites (2)



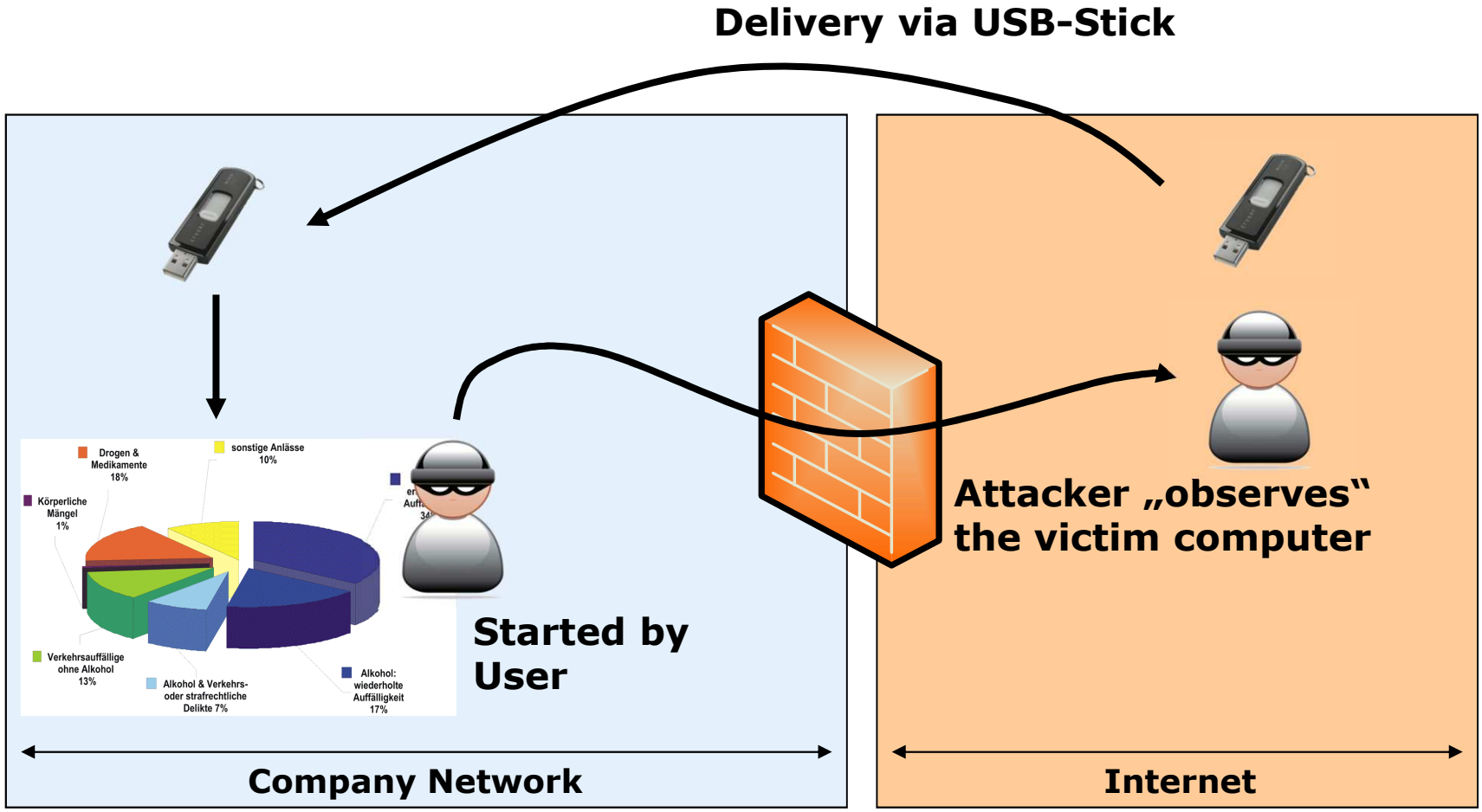
Trojan Horses

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

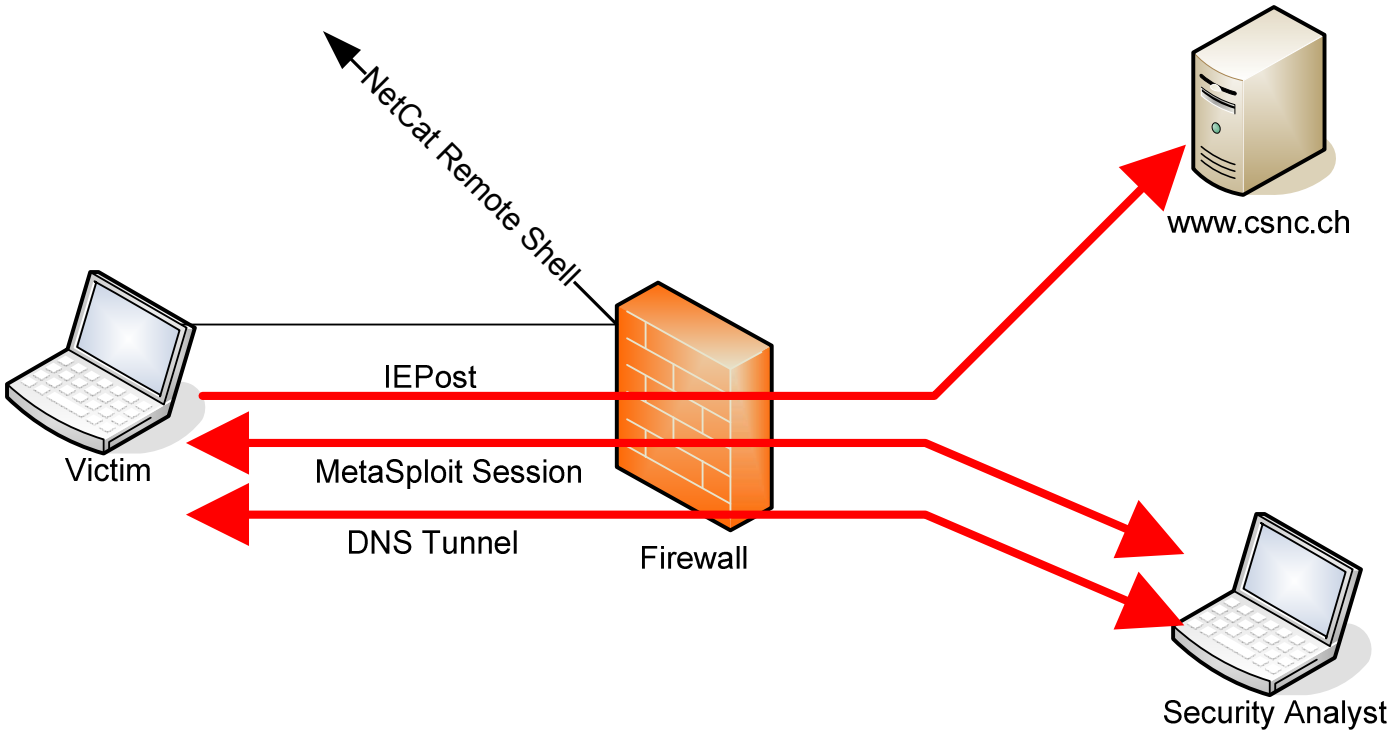
Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Trojan Horse

Covert Channel



Trojan Horse explained



Live Demos

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

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 – 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

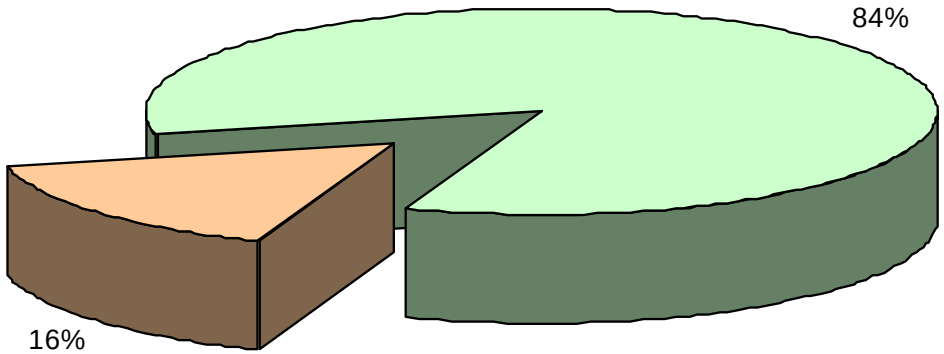
- Attack Vector:
  - Web site with URL
- Goal:
  - Remote control the workstation of the user

Numbers and Facts

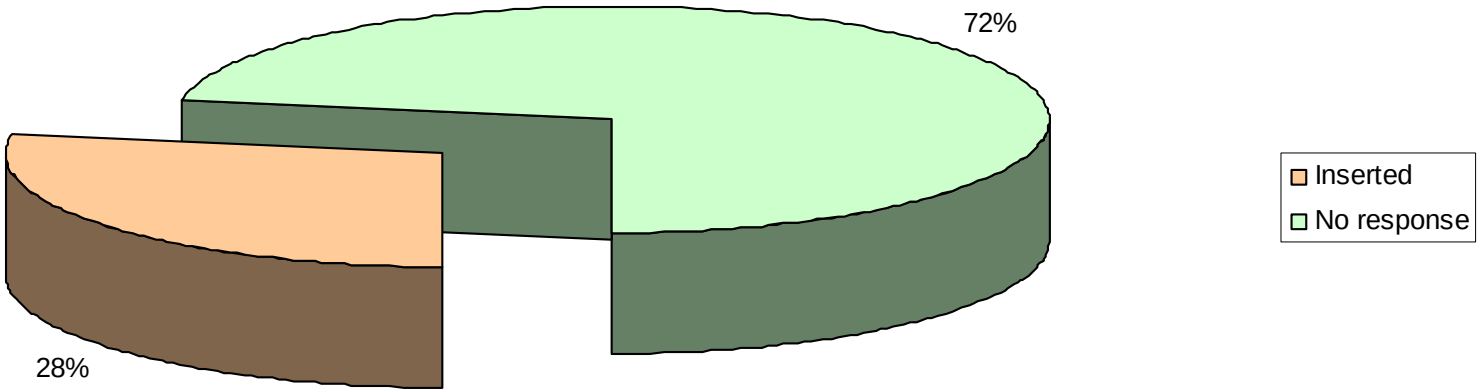
Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

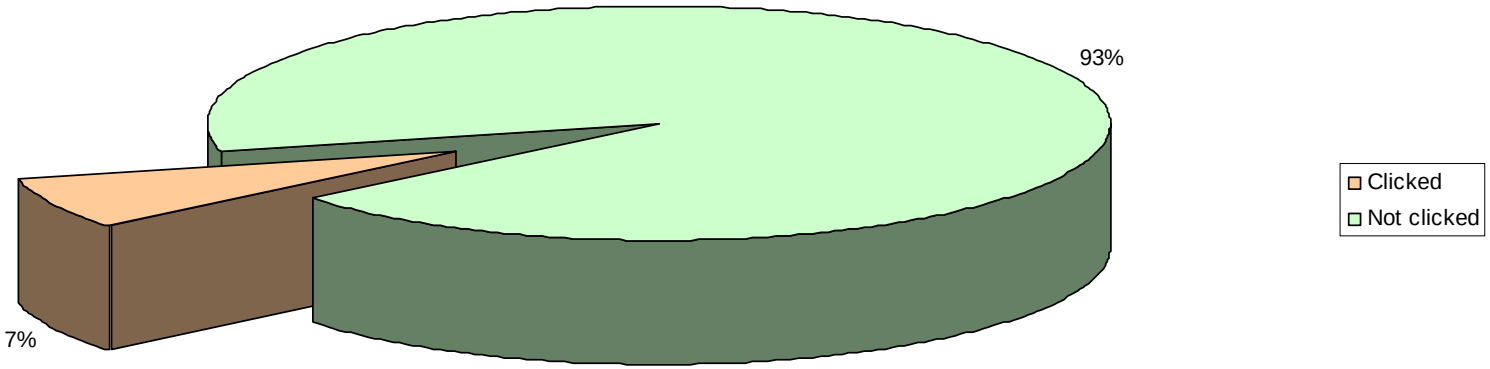
Phishing Website



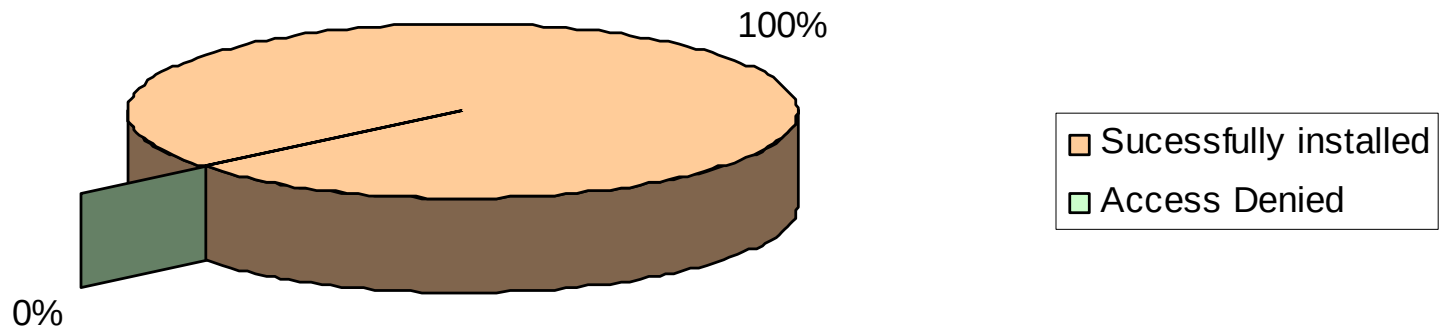
USB-Stick with Trojan Horse



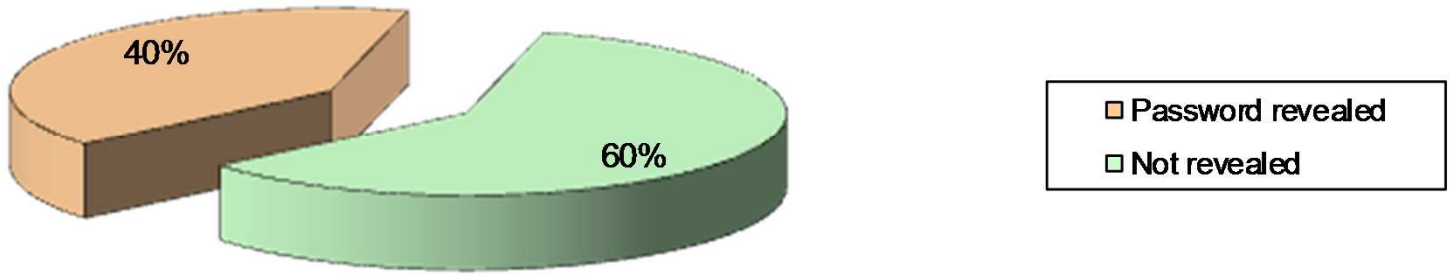
E-Mail with Trojan Horse



Installing Access Point



Phone – Give me your password



Social Engineering Pitfalls

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Social Engineering Pitfalls

- Technical Pitfalls
  - Firewalls (also Personal Firewall)
  - SPAM-Filter
  - URLs blocked
  - Virus/Process Scanner
  - IDS
  - Wireless Strength
- Organizational Pitfalls
  - System Administrator
  - Employees
  - Access Control
  - Legal
  - Bring somebody to shame

Countermeasures

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

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 Employes – User Awareness
  - Security Policies
  - Awareness Demo
  - Social Engineering Test

Social Engineering Test Benefits

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

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 Network Computing

Werkstrasse 20
Postfach 2038
CH - 8645 Jona

team@csnc.ch | www.csnc.ch | +41 55 214 41 60

Secure File Exchange: www.csnc.ch/filebox

PGP-Fingerprint:

41CC 087A BF87 832F 7F0C 5FC3 CC36 7645 DAC0 B1EE