Chapter 12
Cybercrime

- **Module 1: Security Essentials**
  "What You Need to Know"

Money makes the World Go Around

Some Citation anyone?

Please state source

Copyright Information

- Some rights reserved / Einige Rechte vorbehalten
- Michael Kafka, René Pfeiffer, Sebastian Meier
  C.a.T. Consulting and Trainings, Vienna, Austria
- You may freely use, distribute and modify this work under following agreement:
- Diese Arbeit darf frei genutzt, verbreitet und bearbeitet werden unter folgenden Bedingungen:

Authors must be referenced (also for modification)
Autoren müssen genannt werden (auch bei Bearbeitung)

Only for non commercial use
Nur für nichtkommerzielle Nutzung

Derivative work under same licence
Derivative Arbeit unter selber Lizenz

creative commons http://www.creativecommons.com

DeepSec Vienna 2007
7 Layers of Insecurity

Chapter 12
Cybercrime

- Agenda
  - Phishing and Spamming
  - Attacks on Payment Systems
  - Bot Herding
  - Industrial Espionage

Phishing and Spamming

- Gone Phishing

Mimicking original sites

- **Phishing example Paypal**

DeepSec Vienna 2007
7 Layers of Insecurity

- Users can't Verify authenticity
- Implementation of CAs
  - Unsuitable for every day users
  - Certificates themselves badly managed
- High percentage of users will click
- Risk high, Impact high

Attacks on Payment Systems

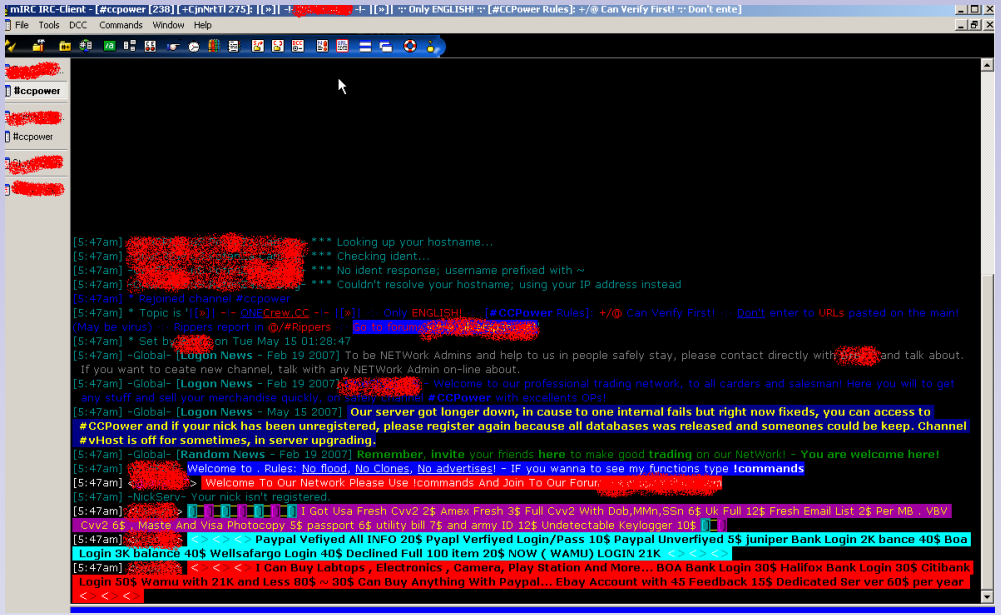
- Credit cards at Risks

DeepSec Vienna 2007
7 Layers of Insecurity

Selling CC and Identities

- Stolen Info:
  - Identities
  - CC Information
  - Banking information
- Risk: medium
- Impact very high

Example



DeepSec Vienna 2007
7 Layers of Insecurity

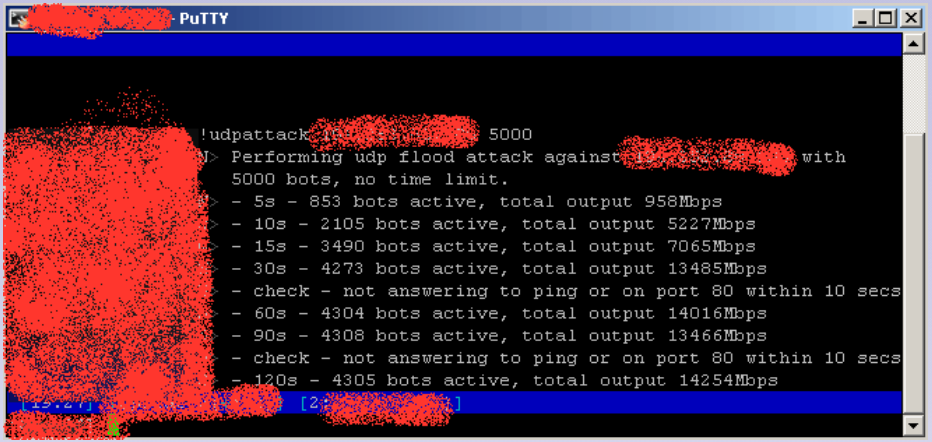
Bot Herding

- **Modern Cowboys (But malicious)**

Purpose of Bot Herding

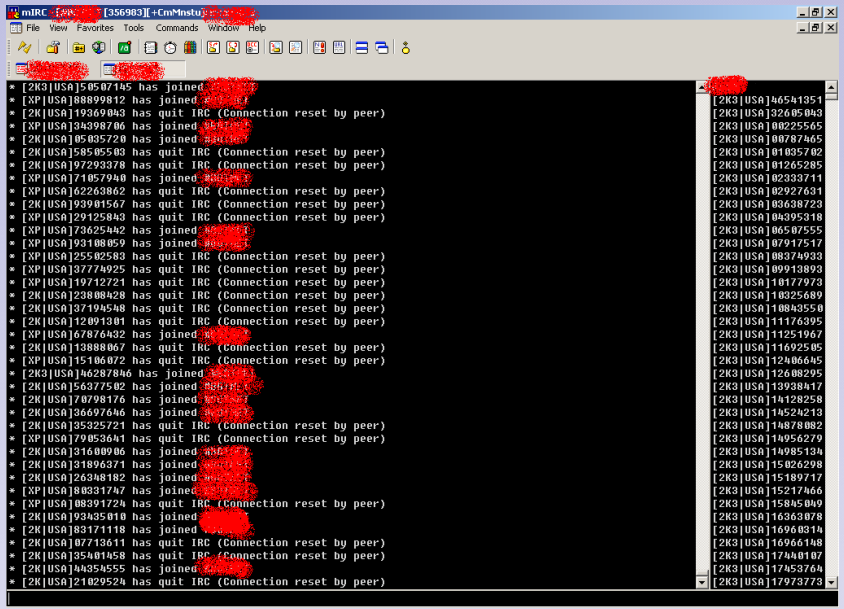
- Gaining control over “Zombies”
  - Used for DDoS
  - Used for Spam
  - Traded with others
- Risk very high
- Impact Medium

Botnet at Work



DeepSec Vienna 2007
7 Layers of Insecurity

Communication via IRC



DeepSec Vienna 2007
7 Layers of Insecurity

Industrial Espionage

- **Cyberspies**
  “With a license to kill”

Highly Specialized Attacks

- Very highly skilled
  - Sometimes hired hackers
- Not very common
- New risks emerging from Asia
- High impact, low risk

Chapter 12
Cybercrime

- Summary
  - Phishing and Spamming Targets Naive Users
  - Attacks on Payment Systems Cause Worldwide Losses
  - Bot Herding Affects All: Private Systems and Corporate Systems Behind Firewalls
  - Industrial Spies Are Rare but Dangerous

Thank You

- **Questions?**

Chapter 12
Cybercrime

- **Module 1: Security Essentials "What You Need to Know"**

Money makes the World Go Around

Some Citation anyone?

Please state source

DeepSec Vienna 2007
7 Layers of Insecurity

Copyright Information

- Some rights reserved / Einige Rechte vorbehalten
- Michael Kafka, René Pfeiffer, Sebastian Meier
  C.a.T. Consulting and Trainings, Vienna, Austria
- You may freely use, distribute and modify this work under following agreement:
- Diese Arbeit darf frei genutzt, verbreitet und bearbeitet werden unter folgenden Bedingungen:


Authors must be referenced (also for modification)
Autoren müssen genannt werden (auch bei Bearbeitung)


Only for non commercial use
Nur für nichtkommerzielle Nutzung


Derivative work under same licence
Derivative Arbeit unter selber Lizenz

http://www.creativecommons.com

© November 2007 12 - Cybercrime 2

DeepSec Vienna 2007
7 Layers of Insecurity

This presentation is published under the CreativeCommons License which can be viewed in detail on their hompage: http://creativecommons.org/licenses/by-nc-sa/2.0/at/

Read more on http://www.creativecommons.com

You are free:


to Share — to copy, distribute and transmit the work


to Remix — to adapt the work

Under the following conditions:


Attribution. You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).


Noncommercial. You may not use this work for commercial purposes.


Share Alike. If you alter, transform, or build upon this work, you may distribute the resulting work only under the same or similar license to this one.

- **For any reuse or distribution, you must make clear to others the license terms of this work. The best way to do this is with a link to this web page.**
- **Any of the above conditions can be waived if you get permission from the copyright holder.**
- **Nothing in this license impairs or restricts the author's moral rights.**

Chapter 12
Cybercrime

- Agenda
  - Phishing and Spamming
  - Attacks on Payment Systems
  - Bot Herding
  - Industrial Espionage

DeepSec Vienna 2007
7 Layers of Insecurity

Phishing and Spamming

- Gone Phishing

DeepSec Vienna 2007
7 Layers of Insecurity

Mimicking original sites

- Phishing example Paypal

DeepSec Vienna 2007
7 Layers of Insecurity

Click to add title

- Users can't Verify authenticity
- Implementation of CAs
  - Unsuitable for every day users
  - Certificates themselves badly managed
- High percentage of users will click
- Risk high, Impact high

DeepSec Vienna 2007
7 Layers of Insecurity

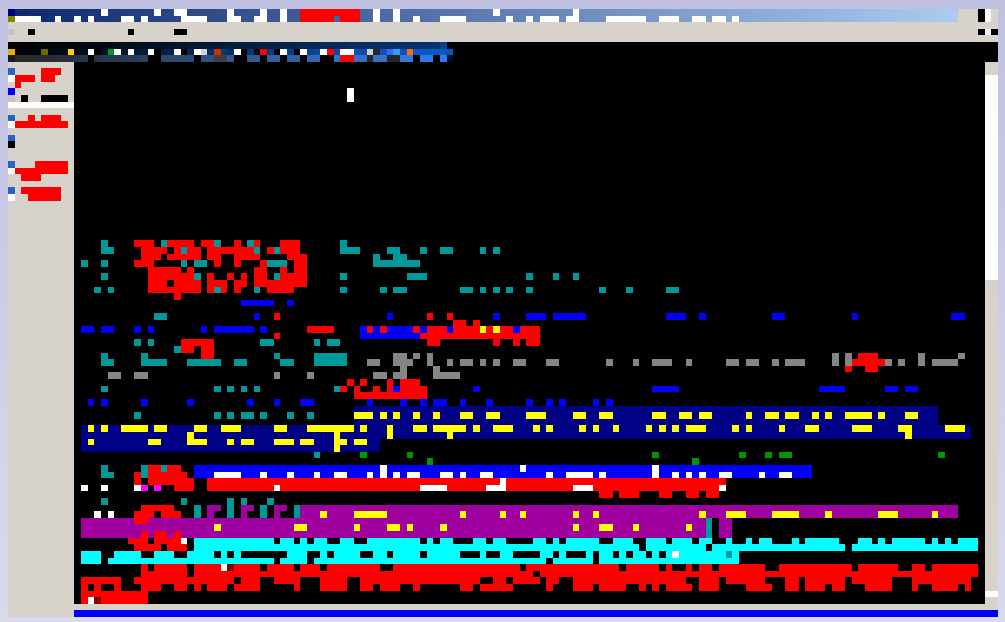
Attacks on Payment Systems

- Credit cards at Risks

Selling CC and Identities

- Stolen Info:
  - Identities
  - CC Information
  - Banking information
- Risk: medium
- Impact very high

Example



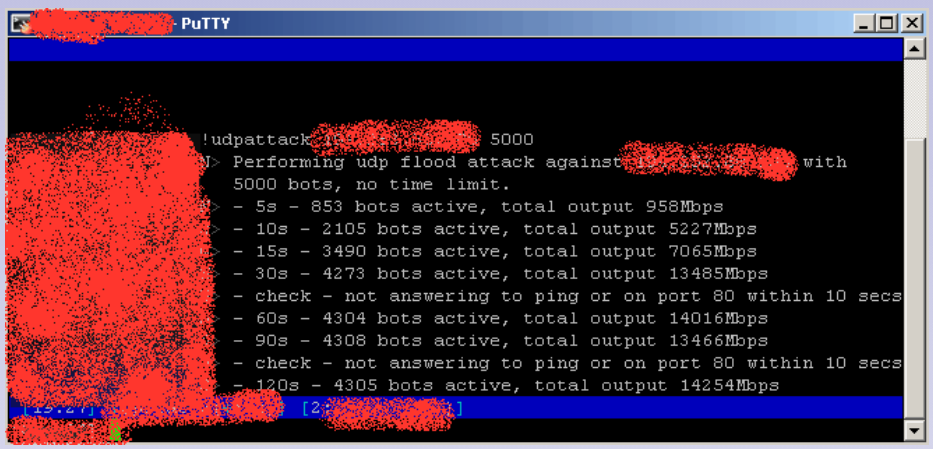
Bot Herding

- Modern Cowboys
  (But malicious)

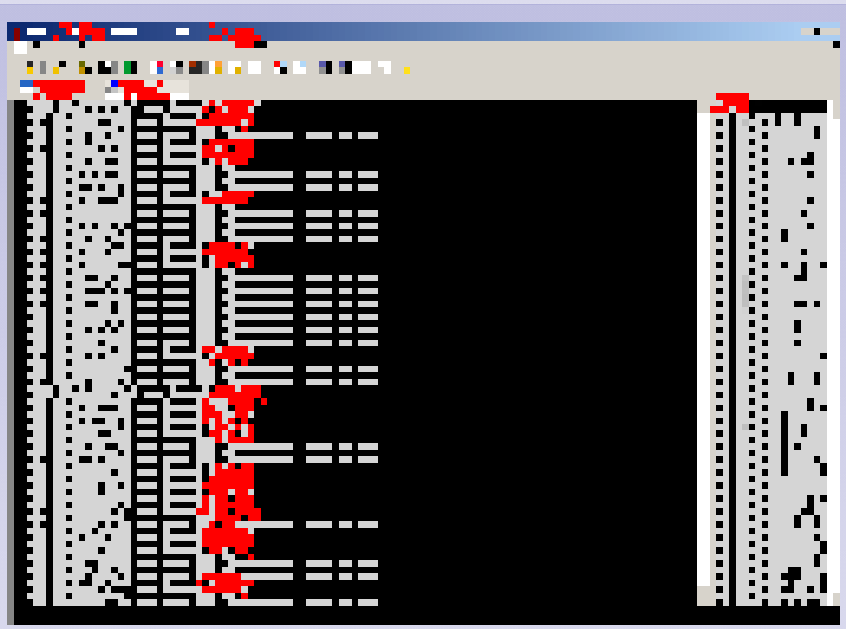
Purpose of Bot Herding

- Gaining control over “Zombies”
  - Used for DDoS
  - Used for Spam
  - Traded with others
- Risk very high
- Impact Medium

Botnet at Work



Communication via IRC



Industrial Espionage

- Cyberspies
  "With a license to kill"

Highly Specialized Attacks

- Very highly skilled
  - Sometimes hired hackers
- Not very common
- New risks emerging from Asia
- High impact, low risk

Chapter 12
Cybercrime

- Summary
  - Phishing and Spamming Targets Naive Users
  - Attacks on Payment Systems Cause Worldwide Losses
  - Bot Herding Affects All: Private Systems and Corporate Systems Behind Firewalls
  - Industrial Spies Are Rare but Dangerous

DeepSec Vienna 2007
7 Layers of Insecurity

Thank You

- Questions?

DeepSec Vienna 2007
7 Layers of Insecurity