

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>

Chapter 12

Cybercrime



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

Phishing and Spamming



- **Gone Phishing**



**DeepSec Vienna 2007
7 Layers of Insecurity**

Mimicking original sites



C.a.T.

■ Phishing example Paypal

The screenshot shows a phishing website designed to look like the PayPal homepage. At the top, it features the PayPal logo and navigation links for Sign Up, Log In, Help, and Security Center. Below this is a horizontal menu with buttons for Welcome, Send Money, Request Money, Merchant Tools, and Auction Tools. The main content area is divided into several sections: a Member Log-In form with fields for Email Address and Password, a 'Join PayPal Today' section with a 'Sign Up Now!' button, and a 'Send money NOT your financial info' section with a 'Watch how PayPal works' button. A central banner reads 'Shop Without Sharing Your Financial Information' with a 'Learn more' link. Below the banner are three columns for Buyers, eBay Sellers, and Merchants, each with promotional text and links. A 'What's New' section at the bottom right lists recent updates. The footer contains a long list of links including About, Accounts, Fees, Privacy, Security Center, Contact Us, Legal agreements, Developers, Jobs, Billing, Plan Local, Technical, Sites, and Help Us.

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



```
mIRC IRC-Client - #ccpower [238] [+c]n[rt] 275: | [+ ] + [+ ] - [+ ] - [+ ] Only ENGLISH :: [#CCPower Rules]: +/@ Can Verify First! :: Don't ente |
File Tools DCC Commands Window Help
#ccpower
#ccpower
[5:47am] *** Looking up your hostname...
[5:47am] *** Checking ident...
[5:47am] *** No ident response; username prefixed with ~
[5:47am] *** Couldn't resolve your hostname; using your IP address instead
[5:47am] * Rejoined channel #ccpower
[5:47am] * Topic is '[x] -!- ONeCrew_CC -!- |[*] ... Only ENGLISH ... [#CCPower Rules]: +/@ Can Verify First! ... Don't enter to URLs pasted on the main (May be virus) ... Rippers report in @/#Rippers ...'
[5:47am] * Set by [redacted] on Tue May 15 01:28:47
[5:47am] -Global- [Logon News - Feb 19 2007] To be NETWork Admins and help to us in people safely stay, please contact directly with [redacted] and talk about. If you want to create new channel, talk with any NETWork Admin on-line about.
[5:47am] -Global- [Logon News - Feb 19 2007] Welcome to our professional trading network, to all carders and salesman! Here you will to get any stuff and sell your merchandise quickly, on safety channel #CCPower with excellents OPst
[5:47am] -Global- [Logon News - May 15 2007] Our server got longer down, in cause to one internal fails but right now fixeds, you can access to #CCPower and if your nick has been unregistered, please register again because all databases was released and someones could be keep. Channel #vHost is off for sometimes, in server upgrading.
[5:47am] -Global- [Random News - Feb 19 2007] Remember, invite your friends here to make good trading on our Network! - You are welcome here!
[5:47am] Welcome to , Rules: No flood, No Clones, No advertisest! - IF you wanna to see my functions type !commands
[5:47am] < [redacted] > Welcome To Our Network Please Use !commands And Join To Our Foru...
[5:47am] -NickServ- Your nick isn't registered.
[5:47am] I Got Usa Fresh Cvv2 2$ Amex Fresh 3$ Full Cvv2 With Dob,MMn,SSn 6$ Uk Full 12$ Fresh Email List 2$ Per Mb . VBV
Cvv2 6$ Maste And Visa Photocopy 5$ passport 6$ utility bill 7$ and army ID 12$ Undetectable Keylogger 10$
[5:47am] Paypal Verified All INFO 20$ Pyapl Verified Login/Pass 10$ Paypal Unverified 5$ juniper Bank Login 2K bance 40$ Boa Login 3K Balance 40$ Wellsafarogo Login 40$ Declined Full 100 Item 20$ NOW ( WAMU) LOGIN 21K
[5:47am] <<< << << I Can Buy Laptops , Electronics , Camera, Play Station And More... BOA Bank Login 30$ Halifax Bank Login 30$ Citibank Login 50$ Wamu with 21K and Less 80$ ~ 30$ Can Buy Anything With Paypal... Ebay Account with 45 Feedback 15$ Dedicated Ser ver 60$ per year
```

DeepSec Vienna 2007
7 Layers of Insecurity

Bot Herding



- **Modern Cowboys
(But malicious)**



**DeepSec Vienna 2007
7 Layers of Insecurity**

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



```
!udpattack [redacted] 5000
N> Performing udp flood attack against [redacted] with
5000 bots, no time limit.
V> - 5s - 853 bots active, total output 958Mbps
V> - 10s - 2105 bots active, total output 5227Mbps
V> - 15s - 3490 bots active, total output 7065Mbps
V> - 30s - 4273 bots active, total output 13485Mbps
V> - check - not answering to ping or on port 80 within 10 secs
V> - 60s - 4304 bots active, total output 14016Mbps
V> - 90s - 4308 bots active, total output 13466Mbps
V> - check - not answering to ping or on port 80 within 10 secs
V> - 120s - 4305 bots active, total output 14254Mbps
[192.0] [redacted] [2: [redacted]]
```

DeepSec Vienna 2007
7 Layers of Insecurity

Communication via IRC



```
mIRC [356983] [+CmMnstu]
File View Favorites Tools Commands Window Help
[Redacted]
[Redacted]
* [2K3|USA]50507145 has joined
* [XP|USA]88899812 has joined
* [2K|USA]19369043 has quit IRC (Connection reset by peer)
* [XP|USA]348398706 has joined
* [2K|USA]05035720 has joined
* [2K|USA]58505503 has quit IRC (Connection reset by peer)
* [2K|USA]97293378 has quit IRC (Connection reset by peer)
* [XP|USA]71057940 has joined
* [XP|USA]62263802 has quit IRC (Connection reset by peer)
* [2K|USA]193945167 has quit IRC (Connection reset by peer)
* [XP|USA]29125843 has quit IRC (Connection reset by peer)
* [XP|USA]73625442 has joined
* [XP|USA]93100059 has joined
* [XP|USA]25502583 has quit IRC (Connection reset by peer)
* [XP|USA]37774925 has quit IRC (Connection reset by peer)
* [XP|USA]19712721 has quit IRC (Connection reset by peer)
* [2K|USA]23808828 has quit IRC (Connection reset by peer)
* [2K|USA]37194548 has quit IRC (Connection reset by peer)
* [2K|USA]12091301 has quit IRC (Connection reset by peer)
* [XP|USA]67876432 has joined
* [2K|USA]13888067 has quit IRC (Connection reset by peer)
* [XP|USA]15106092 has quit IRC (Connection reset by peer)
* [2K3|USA]4628946 has joined
* [2K|USA]56377502 has joined
* [2K|USA]70798176 has joined
* [2K|USA]36697646 has joined
* [2K|USA]35325721 has quit IRC (Connection reset by peer)
* [XP|USA]79053641 has quit IRC (Connection reset by peer)
* [2K|USA]31608006 has joined
* [2K|USA]31896371 has joined
* [2K|USA]26348182 has joined
* [XP|USA]80331747 has joined
* [XP|USA]08391724 has quit IRC (Connection reset by peer)
* [2K|USA]193435010 has joined
* [2K|USA]18317119 has joined
* [2K|USA]07713611 has quit IRC (Connection reset by peer)
* [2K|USA]35401458 has quit IRC (Connection reset by peer)
* [2K|USA]44354555 has joined
* [2K|USA]21029524 has quit IRC (Connection reset by peer)
* [2K3|USA]46541951
* [2K3|USA]32405043
* [2K3|USA]00225565
* [2K3|USA]00787465
* [2K3|USA]01035702
* [2K3|USA]01265285
* [2K3|USA]02333711
* [2K3|USA]02927631
* [2K3|USA]03638723
* [2K3|USA]04395318
* [2K3|USA]06507555
* [2K3|USA]07917517
* [2K3|USA]08374933
* [2K3|USA]09913893
* [2K3|USA]10177973
* [2K3|USA]10325689
* [2K3|USA]10843550
* [2K3|USA]11176395
* [2K3|USA]11251967
* [2K3|USA]11692505
* [2K3|USA]12406605
* [2K3|USA]12608295
* [2K3|USA]13938417
* [2K3|USA]14128258
* [2K3|USA]14524213
* [2K3|USA]14878082
* [2K3|USA]14956279
* [2K3|USA]14985134
* [2K3|USA]15026298
* [2K3|USA]15189717
* [2K3|USA]15217466
* [2K3|USA]15845049
* [2K3|USA]16363078
* [2K3|USA]16964014
* [2K3|USA]16966148
* [2K3|USA]17440107
* [2K3|USA]17453764
* [2K3|USA]17973773
```

DeepSec Vienna 2007
7 Layers of Insecurity

Industrial Espionage



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



DeepSec Vienna 2007
7 Layers of Insecurity

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?



**DeepSec Vienna 2007
7 Layers of Insecurity**

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>

DeepSec Vienna 2007
7 Layers of Insecurity

© November 2007

12 - Cybercrime

2

This presentation is published under the Creative Commons License which can be viewed in detail on their homepage: <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

© November 2007

12 - Cybercrime

3

Phishing and Spamming



- **Gone Phishing**



**DeepSec Vienna 2007
7 Layers of Insecurity**

© November 2007

12 - Cybercrime

4

Mimicking original sites



- Phishing example Paypal



© November 2007

12 - Cybercrime

DeepSec Vienna 2007
7 Layers of Insecurity

5

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

© November 2007

12 - Cybercrime

6

Attacks on Payment Systems



- Credit cards at Risks



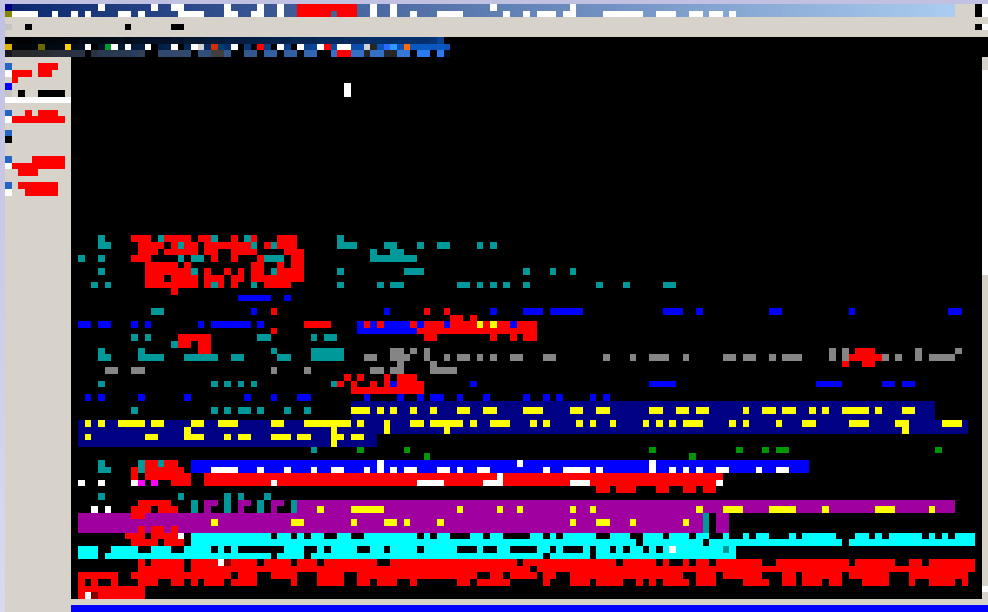
DeepSec Vienna 2007
7 Layers of Insecurity

Selling CC and Identities



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

Example



DeepSec Vienna 2007
7 Layers of Insecurity 6

Bot Herding



- **Modern Cowboys
(But malicious)**



DeepSec Vienna 2007
7 Layers of Insecurity
☞

Purpose of Bot Herding



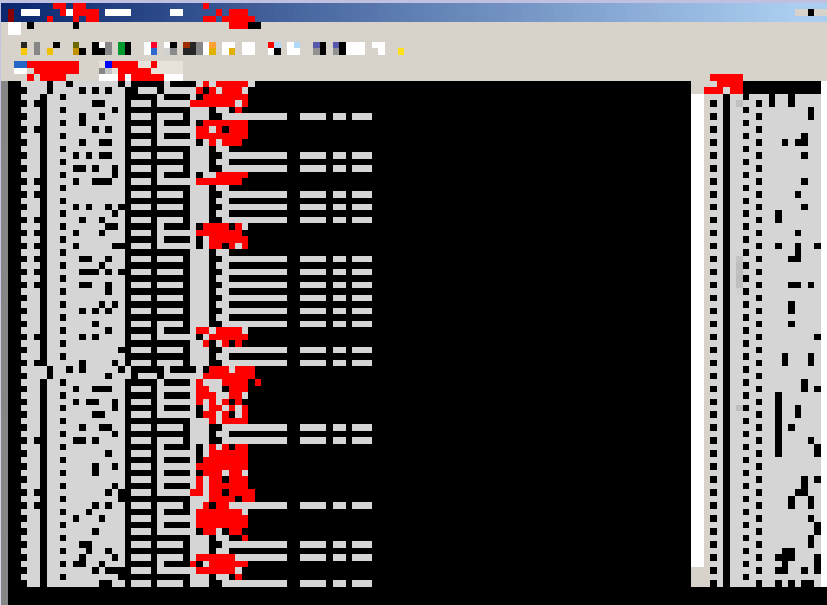
- **Gaining control over “Zombies”**
 - **Used for DDoS**
 - **Used for Spam**
 - **Traded with others**
- **Risk very high**
- **Impact Medium**

Botnet at Work



```
PutTY
!udpattack [redacted] 5000
> Performing udp flood attack against [redacted] with
5000 bots, no time limit.
- 5s - 853 bots active, total output 958Mbps
- 10s - 2105 bots active, total output 5227Mbps
- 15s - 3490 bots active, total output 7065Mbps
- 30s - 4273 bots active, total output 13485Mbps
- check - not answering to ping or on port 80 within 10 secs
- 60s - 4304 bots active, total output 14016Mbps
- 90s - 4308 bots active, total output 13466Mbps
- check - not answering to ping or on port 80 within 10 secs
- 120s - 4305 bots active, total output 14254Mbps
```

Communication via IRC



DeepSec Vienna 2007
7 Layers of Insecurity

Industrial Espionage



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



DeepSec Vienna 2007
7 Layers of Insecurity

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**

© November 2007

12 - Cybercrime

16

Thank You



- Questions?



**DeepSec Vienna 2007
7 Layers of Insecurity**

© November 2007

12 - Cybercrime

17