DEUTSCHER PRÄVENTIONSTAG

„The Anti-Botnet Advisory Centre“

von

Sven Karge
Cornelia Schildt

Dokument aus der Internetdokumentation
des Deutschen Präventionstages www.praeventionstag.de
Herausgegeben von Hans-Jürgen Kerner und Erich Marks im Auftrag der
Deutschen Stiftung für Verbrechensverhütung und Straffälligenhilfe (DVS)

Zur Zitation:
Sven Karge, Cornelia Schildt: The Anti-Botnet Advisory Centre, in: Kerner, Hans-Jürgen u. Marks, Erich (Hrsg.), Internetdokumentation des Deutschen Präventionstages. Hannover 2011, www.praeventionstag.de/Dokumentation.cms/1611

Anti-Botnet Beratungszentrum

eco

Bundesamt für Sicherheit in der Informationstechnik

The Anti-Botnet Advisory Center

Cornelia Schildt

Department of Internet Security

Federal Office for Information Security (BSI)

Sven Karge

Head of Content Department

eco – Association of the German Internet Industry

Why an Anti-Botnet Advisory Center?

- There are several million computers worldwide that are part of a Botnet – unnoticed by computer owners
- Germany ranked within the Top Ten
- Botnets compose an infrastructure for organized Internet crime

Which dangers are involved within Botnets?

- Distribution of Spam
- Deployment of malicious software
- Server attacks (DDos-Attack)
- Tapping data (Phishing)

Goals of an Anti-Botnet-Advisory Center

- Support users on the subject of Internet security
- Reduce Botnets: Free infected computers from malicious software
- Withdraw cyber criminal foundations
- Get Germany out of the Top10 Ranking of malicious activity

General Framework

- Project setup started March 2010
- Project started 15th September 2010
- Start-up funding of 2 Million EUR in the first year
- eco, the association of German ISPs, acts as the exclusive project manager for the initiative
- eco guarantees the continuation for at least another year without additional funding of the government
- BSI provides technical expertise and supports eco
- ISPs takes the necessary technical and organisational steps to implement the initiative (informing users, ..)

What does the Anti-Botnet Advisory Center do?

- helps remove malicious botnet software from an affected users computer
- work together with Internet-Service-Providers (ISPs) and Anti-Virus Software Vendors
- target group: all users using Windows-Computers

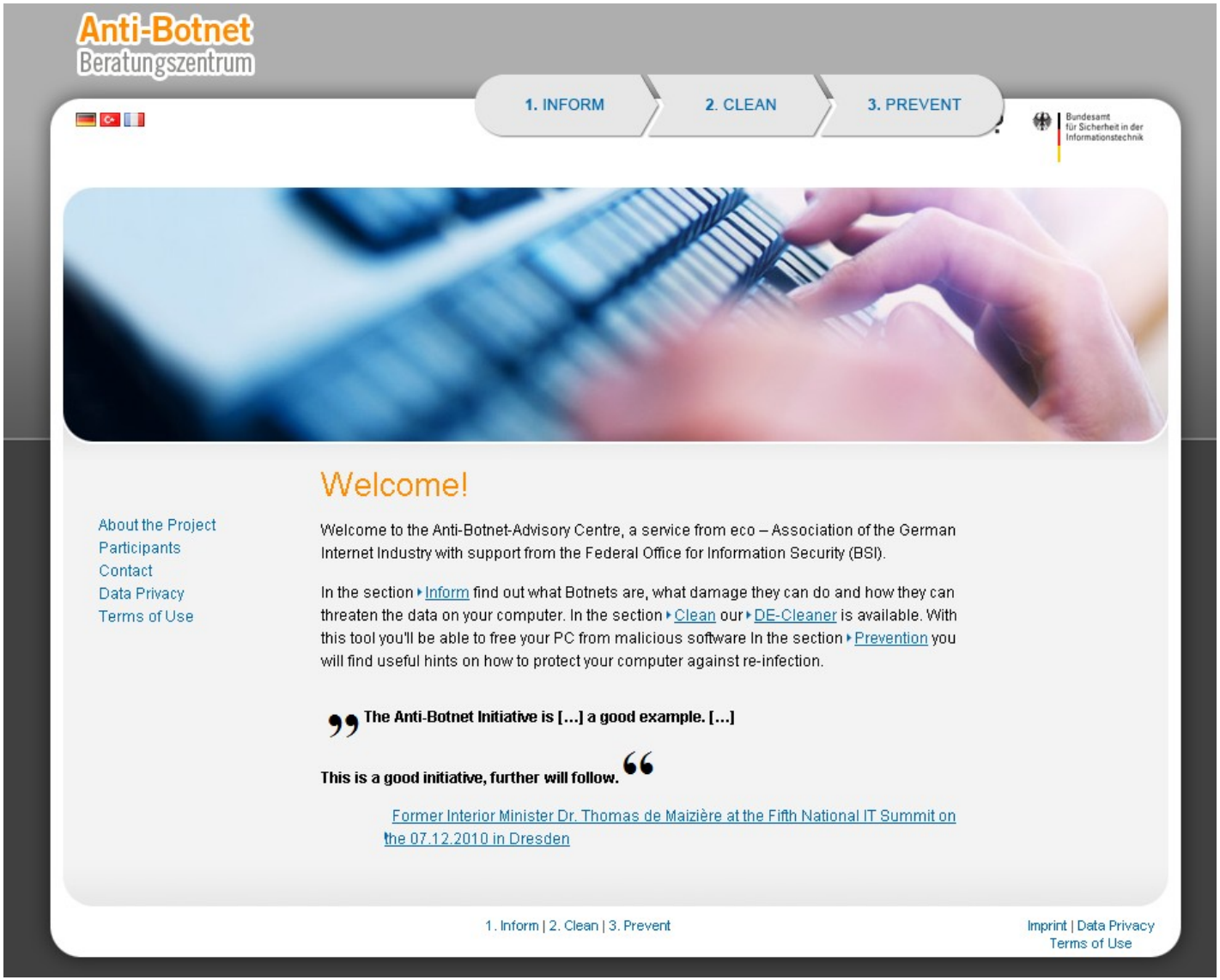
What does the Anti-Botnet Advisory Center do?

- ISPs/Banks detect and notify (various channels) infected customers and refer them to the website of the advisory center
- Call Center module: step-by-step guidance on the phone if necessary
- Ticket System without personal data (Ticket-ID) reports back to ISP

Anti-Botnet Beratungszentrum

eco

Bundesamt für Sicherheit in der Informationstechnik



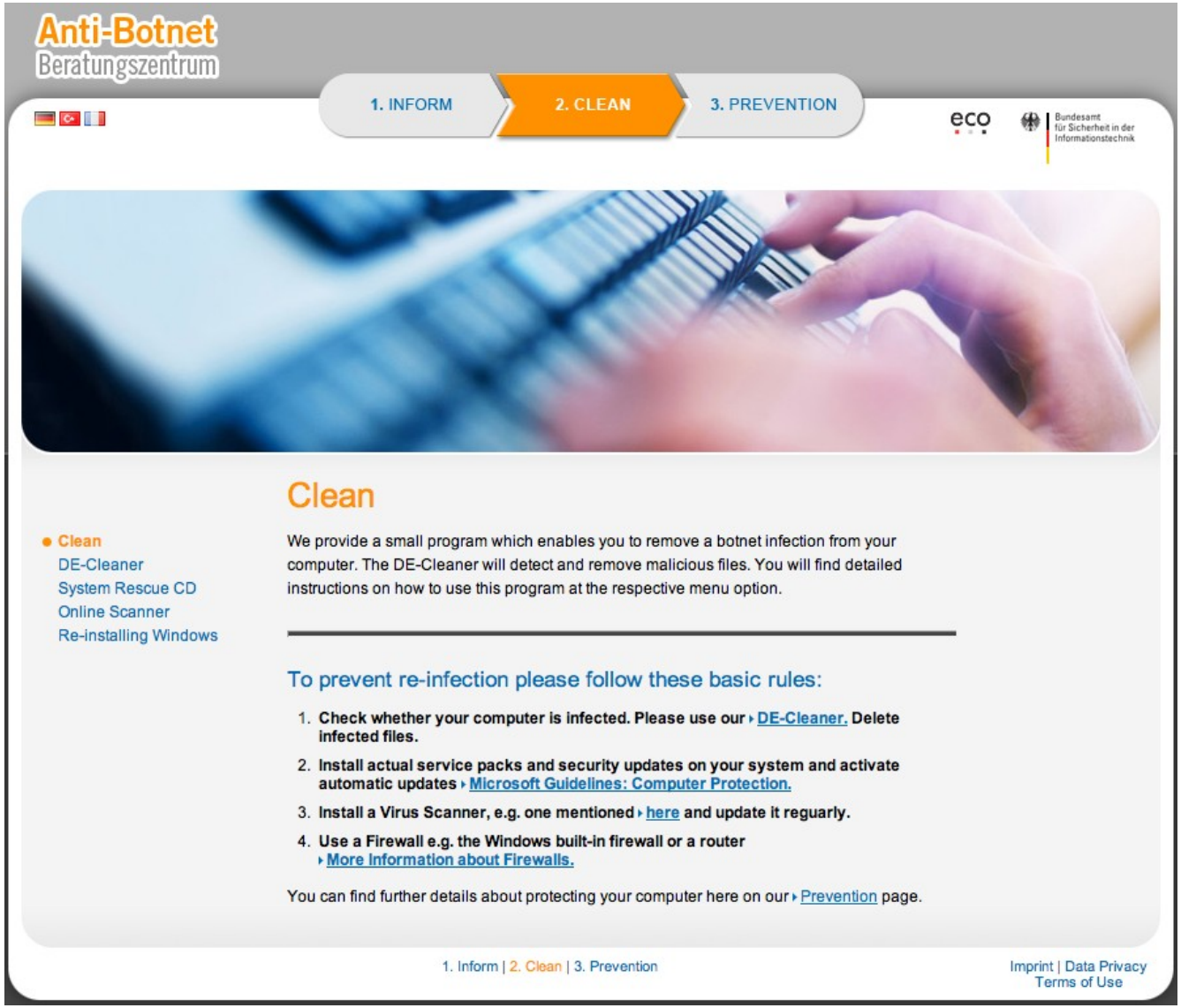
Inform → Clean → Prevention

- Internet Servic -Provider (ISP) and/or bank inform customers of a botnet infection on his/her computer
- A customer – including all others who are interrested too - should visit – www.botfrei.de (available so far in German, English, French and Turkish)
- Under *Inform* he/she receives detailed information about botnets, malicious software and internet security

Anti-Botnet Beratungszentrum

eco

Bundesamt für Sicherheit in der Informationstechnik



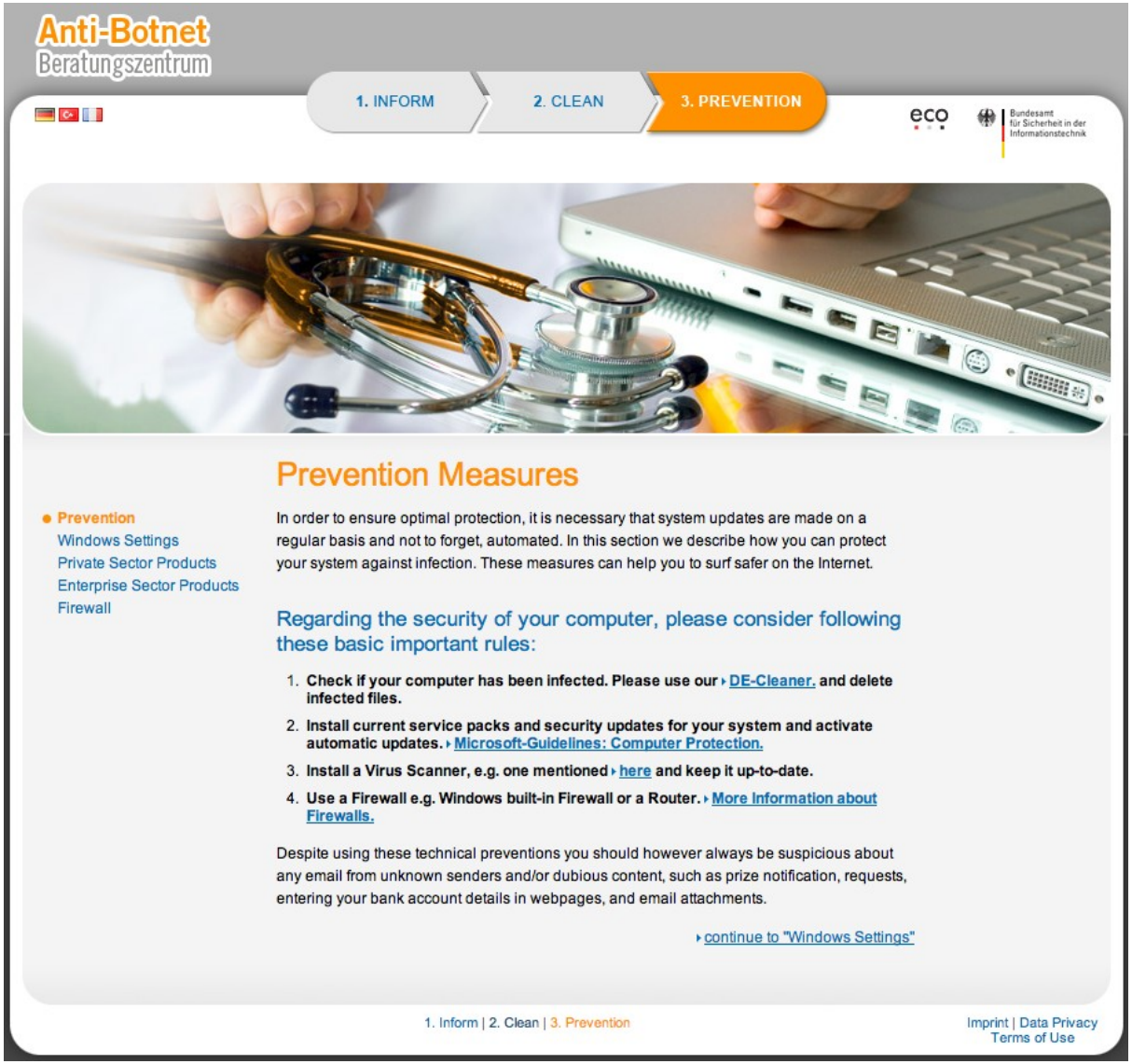
Inform → Clean → Prevention

- DE-Cleaner detects malicious software and removes it.
- The DE-Cleaner System Recovery-CD can be used for heavily infected computers
- Telephone support hotline help customers needing additional help

Anti-Botnet Beratungszentrum

eco

Bundesamt für Sicherheit in der Informationstechnik



Inform → Clean → Prevent

1. **Check** Computers on a regular basis
2. Install actual **Service-Packs and Security Updates** for that operating system including all other application software
3. Installation and regular updates of an efficient **Anti-Virus Scanner**
4. Use a Personal **Firewall** i.e. Windows built-in Firewall or a router Firewall

Partner

ISP participants and others

Customer info

- 1 & 1, GMX & Web.de
- Deutsche Telekom
- Vodafone
- Kabel BW
- Netcologne
- QSC
- Versatel
- Unitymedia
- VZ-Netzwerke

Support hotline

- 1 & 1, GMX & Web.de
- Kabel Baden-Württemberg
- Unitymedia
- VZ-Netzwerke

In short participating Financial Service Providers

signed agreements with / currently being implemented:

- SSK Solingen
- Naspa
- KSK Köln
- KSK Düsseldorf

Partner

- DE-Cleaner provided by Avira (since Mar 2011), Kaspersky (Dec 2010) and Norton/ Symantec (Sept 2010)
- DE-Cleaner System Rescue CD i.e. Anti-Bot-CD: Avira, BSI, Computerbild and eco

Statistics (15th Sept.10 – 30th April 2011)

- **Website Access:**
  - **994.389** Visitors
  - **5.145.617** Pages viewed

- **Activations of DE-Cleaner:**

  - powered by Symantec (15. Sept 10 – 30. April 11) **420.627**
  - powered by Kaspersky (07. Dez 10 – 30. April 11) **41.966**
  - powered by Avira (01. Mar 11 - 30. April 11) **59.746**

  = 522.339 (!) Downloads & Activations

- Tickets in Ticketsystem = notified end users: **200.162**
  Less than 1% need telephone support; Call duration in average: **14** Min.

Statistics: Avira DE-Cleaner Logfile Analysis

sent Reports March 1st – May 2nd:

• scanned Systems:	**34.713**
• not infected Systems:	**25.115**
• infected Systems:	**9.598**
	(27,65%) !!!
• Total infected files	**66.329**
• infected files per System on average	**6,9**

Statistics: Kaspersky Malware Report Q1/2011

- Germany improved in Ranking (ranks on 6 now as regards countries with infected web ressources, 3,28% less)
- Japan and Germany rank 1 and 2 in the list of the most secure countries regarding the risk of a local infection

Statistics: Pallas GmbH

- Q1/2008 DE has highest bot infection rate worldwide
- Q1/2011 DE ranks only on 19 worldwide regarding bot infections
- Drastic decrease of the number of bots from Q4/2010 to Q1/2011 in DE

next steps

- Include other countries / languages
- intensify project promotion
- productline strectching: Mac OS X / Linux / mobile systems

Anti-Botnet
Beratungszentrum

eco

Bundesamt
für Sicherheit in der
Informationstechnik

Contact

Sven Karge
Head of Content Department

Lichtstr. 43h
50825 Köln

+49 221 / 70 00 48 – 190
sven.karge@eco.de
www.eco.de
www.botfrei.de

Cornelia Schildt
Department of Internet Security

Godesberger Allee 185-189
53175 Bonn

+49 22899 / 9582 – 5102
cornelia.schildt@bsi.bund.de
www.bsi.bund.de