Anti-Botnet Beratungszentrum

eco

Bundesamt für Sicherheit in der Informationstechnik

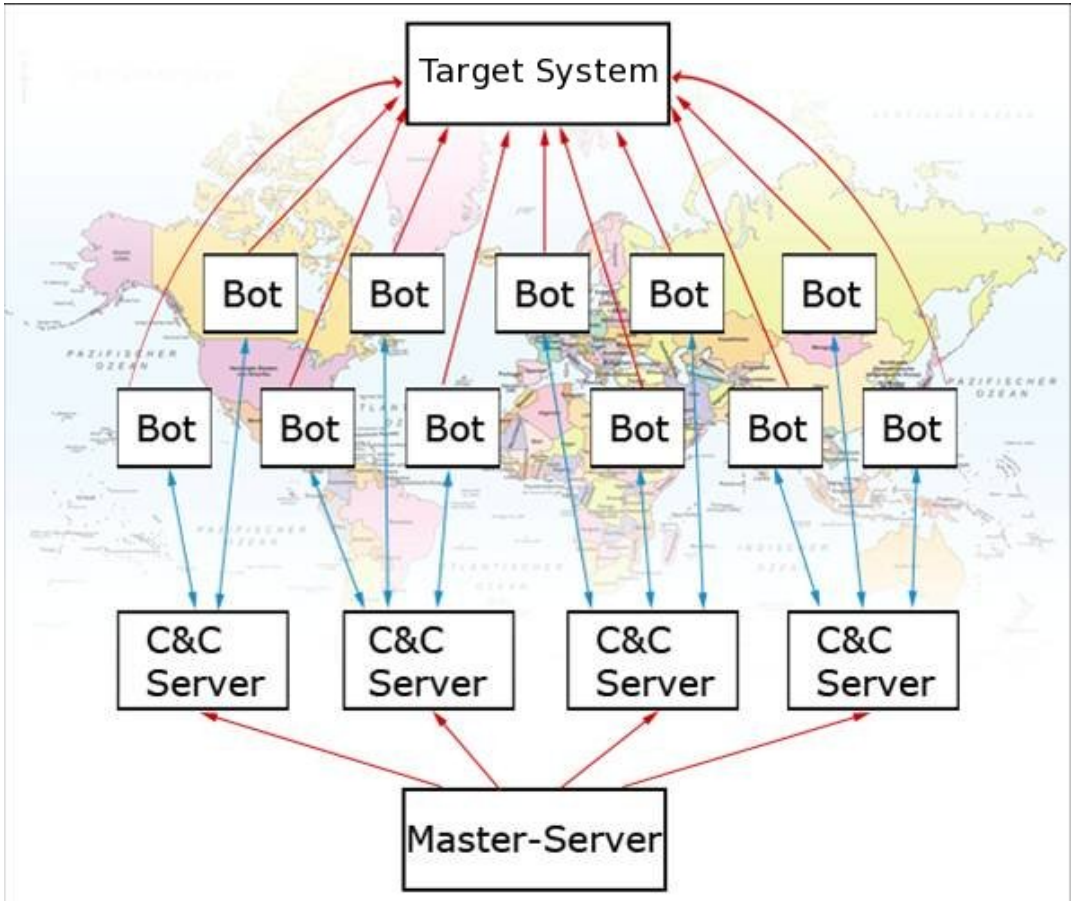
The Anti-Botnet Advisory Center

Randolph Morawe
Mümin Gözenoglu

Workshop on Botnet Detection, Measurement, Disinfection & Defence

09./ 10. March 2011

The Botnet


Target System
Bot
Bot
Bot
Bot
Bot
Bot
Bot
Bot
Bot
Bot
Bot
C&C Server
C&C Server
C&C Server
C&C Server
Master-Server

Malware Description

Schädling	Auch bekannt als	Nummer
unbekannt	-	0000
Rustock	RKRustok, Costrat	0001
Cutwail	Pandex, Mutant	0002
Ozdok	Mega-D	0003
Grum	Tedroo	0004
Lethic	Scar	0005
Xarvester	rlsloup, pixoliz	0006
Gheg	Tofsee, mondera	0007
Bobax	Bobic, Oderoor, Cotmonger, Hacktool.Spammer	0008
Storm2	Nuwar, Zhelatin, Pecoan	0009
Bagle	Tooso	0010
Conficker		0011
Waledac		0012
Bagel		0013
Zeus		0014
Avalanche		0015
TorPig		0016
Clampi		0017
Gozi		0018

Why an Anti-Botnet Advisory Center?

- There are several million computers worldwide that are part of a Botnetwork – unnoticed by computer owners
- Germany ranks in the Top Ten
- Germany belongs to the top 3 worldwide and ranked first of the countries within the EU, which emanates from malicious online activity.
- Botnets compose an Infrastructure for organized Internet crime

Which dangers arrise from Botnets ?

- Distribution of Spam
- Spreading of malicious software
- Server attacks (DDos-Attack)
- Siphon-off data (Phishing)
- Storage for illegal content

Anti-Botnet Beratungszentrum

eco

Bundesamt für Sicherheit in der Informationstechnik

Goals of an Anti-Botnet-Advisory Center

- Support users on the subject of Internet security
- Reduce Botnetworks: Free infected Computers from malicious software
- Withdraw cyber criminals‘ foundation

Anti-Botnet Beratungszentrum

eco

Bundesamt für Sicherheit in der Informationstechnik

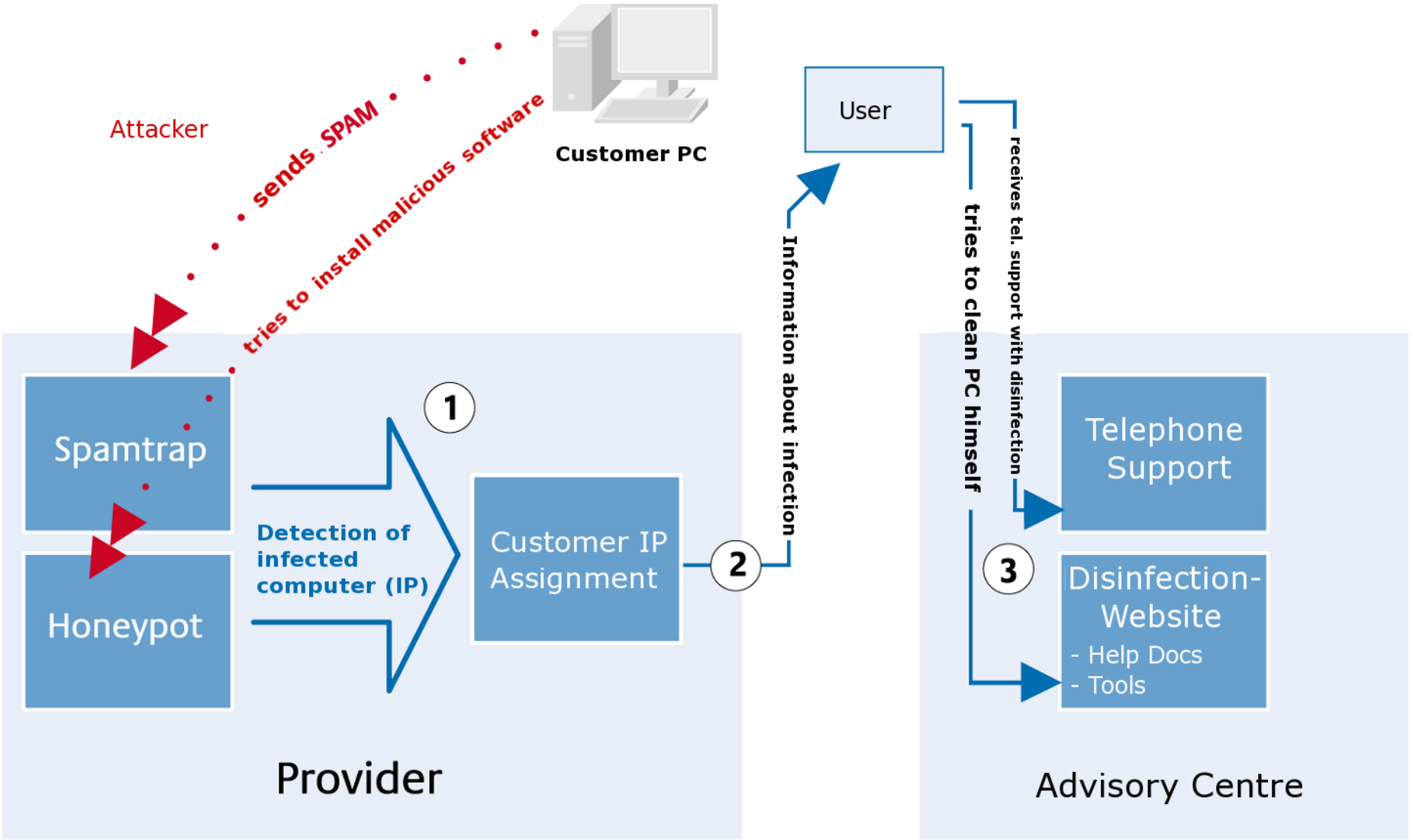
What does the Anti-Botnet Advisory Center do?

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

Anti-Botnet Beratungszentrum

eco

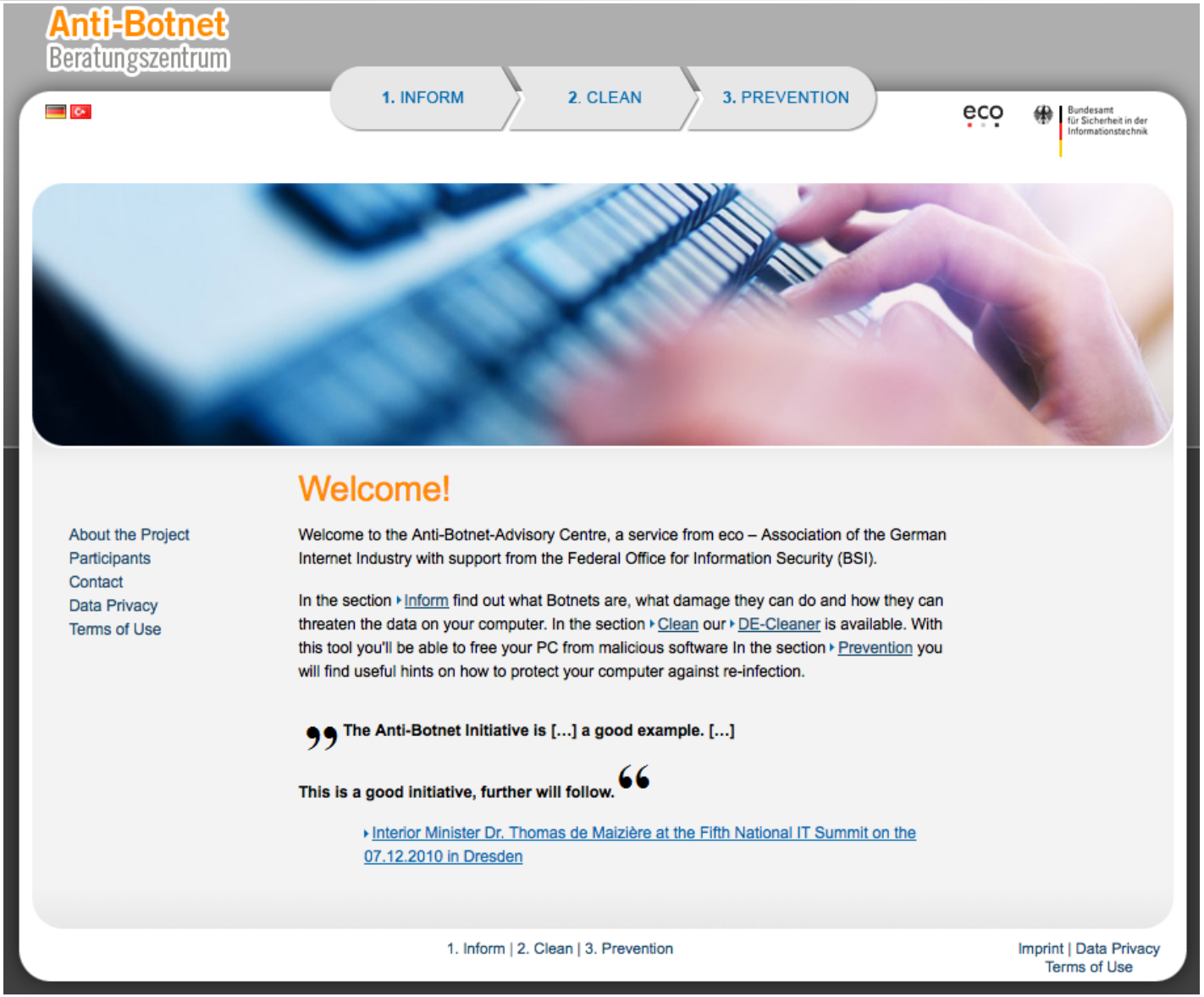
Bundesamt für Sicherheit in der Informationstechnik



Anti-Botnet Beratungszentrum

eco

Bundesamt für Sicherheit in der Informationstechnik



Anti-Botnet Beratungszentrum

eco

Bundesamt für Sicherheit in der Informationstechnik

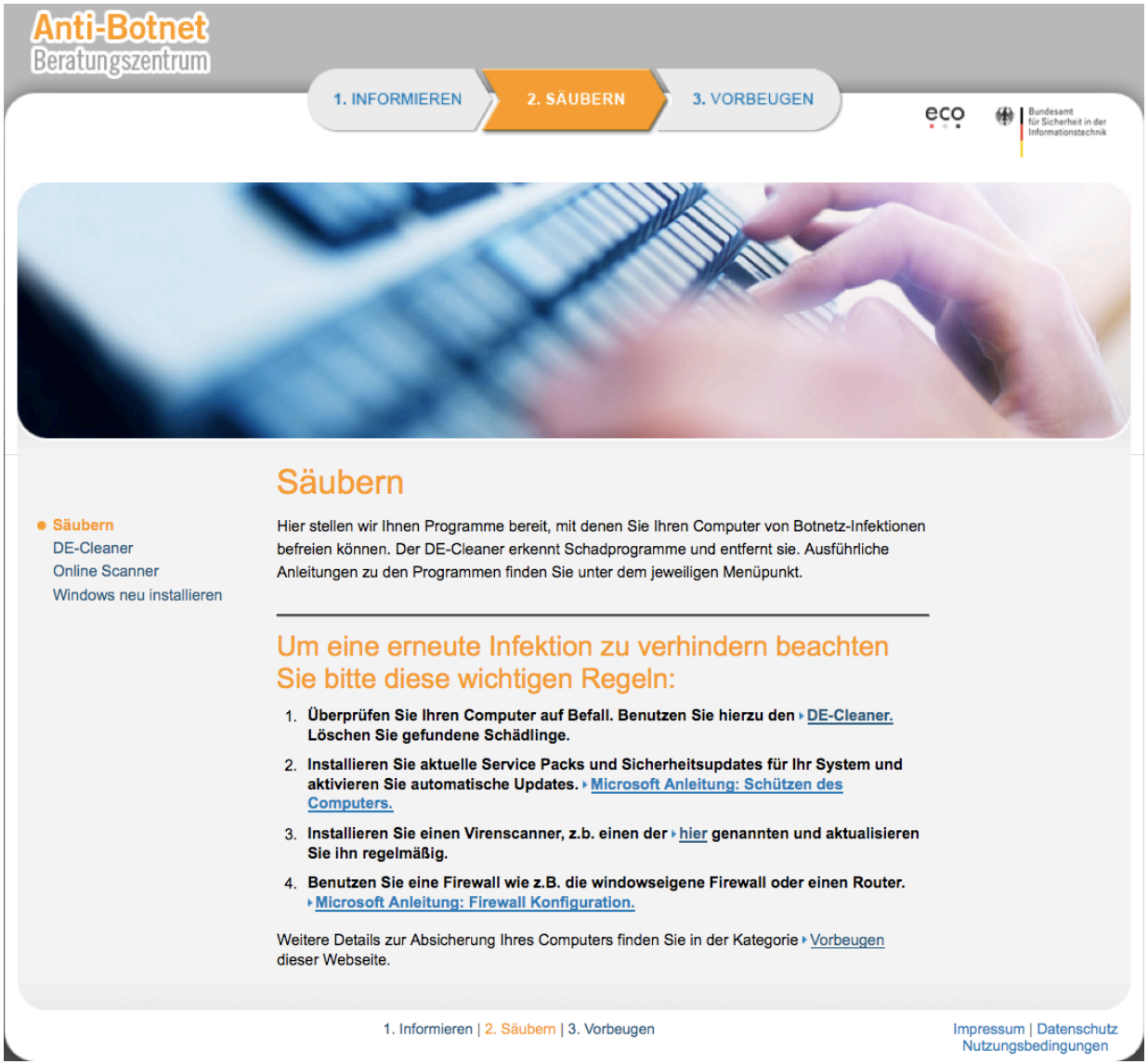
Inform → Clean → Prevention

- Internet-Service Provider (ISP) informs customers of a Botnet-Infection on his/her computer
- A customer can – as to all others who are interrested, to visit – www.botfrei.de
- Under *Advice* one receives detailed Information about Botnets, Malicious Software and Internet-Security

Anti-Botnet Beratungszentrum

eco

Bundesamt für Sicherheit in der Informationstechnik



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 who need additional help

Anti-Botnet Beratungszentrum

eco

Bundesamt für Sicherheit in der Informationstechnik

Inform → Clean → Prevention

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

Partner

ISPs participants and others

Customer info

- 1 & 1
- Deutsche Telekom
- Kabel Baden-Württemberg
- Netcologne
- QSC
- Versatel
- StudiVZ
- WEB.DE
- GMX
- Vodafone
- Unitymedia

Support hotline

- 1 & 1
- Kabel Baden-Württemberg
- Versatel (being planned)
- StudiVZ
- GMX
- Web.de

In short participating Financial Service Providers

intensive positive meetings with:

- Aachener Sparkasse
- Fraspa & 1822direkt
- Naspa

Partner

- DE-Cleaner provided by Avira, Kaspersky and Norton/ Symantec

- DE-Cleaner System Rescue CD i.e. Anti-Bot-CD: Avira, BSI, Computerbild and eco

Statistics

- Website Access:15.09.2010 - 31.01.2011
  - 763.300 Visitors and
  - 4.357.735 Pages Viewed
  - Activations of DE-Cleaner powered by Symantec: 386.458
- Activations of DE-Cleaner powered by Kaspersky 7.12.2010 - 31.01.2011: 11.470
- Call duration on average: 20-30 Min.

Anti-Botnet
Beratungszentrum

eco

Bundesamt
für Sicherheit in der
Informationstechnik

Thank you for your attention

Anti-Botnet
Beratungszentrum

eco

Bundesamt
für Sicherheit in der
Informationstechnik

M. Gözenoglu/ R. Morawe
Experts - 2nd Level

Lichtstr. 43h
50825 Köln

Tel.: 0221 / 70 00 48 – 0
Fax: 0221 / 70 00 48 – 111

muemin.goezonglu@eco.de
randolph.morawe@eco.de

www.eco.de
www.botfrei.de