

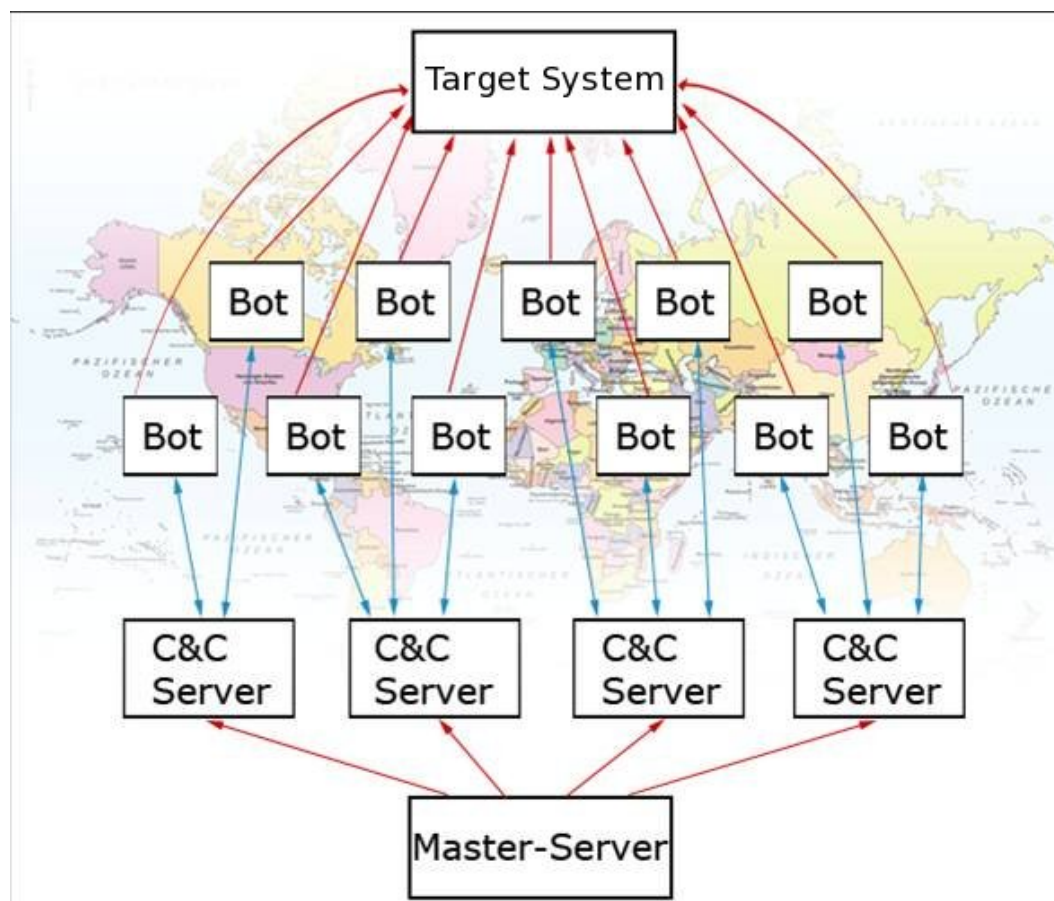
The Anti-Botnet Advisory Center

**Randolph Morawe
Mümin Gözenoglu**

**Workshop on Botnet Detection, Measurement, Disinfection &
Defence**

09./ 10. March 2011

The Botnet



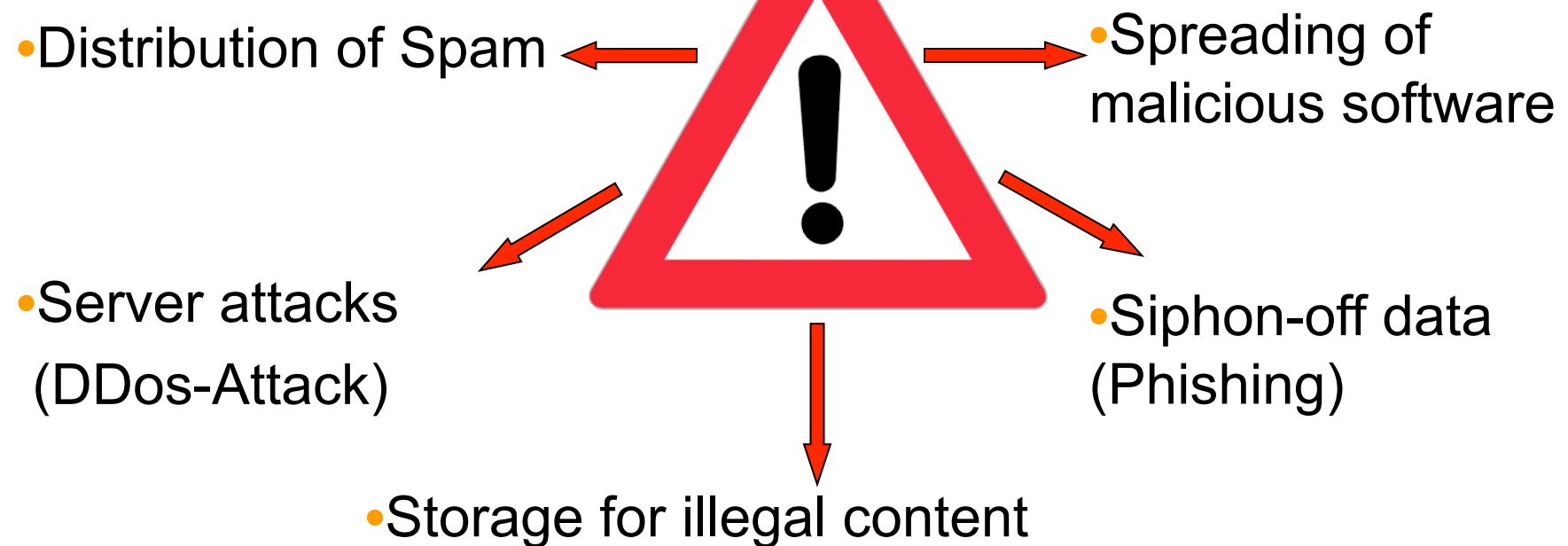
Malware Description

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 arise from Botnets ?

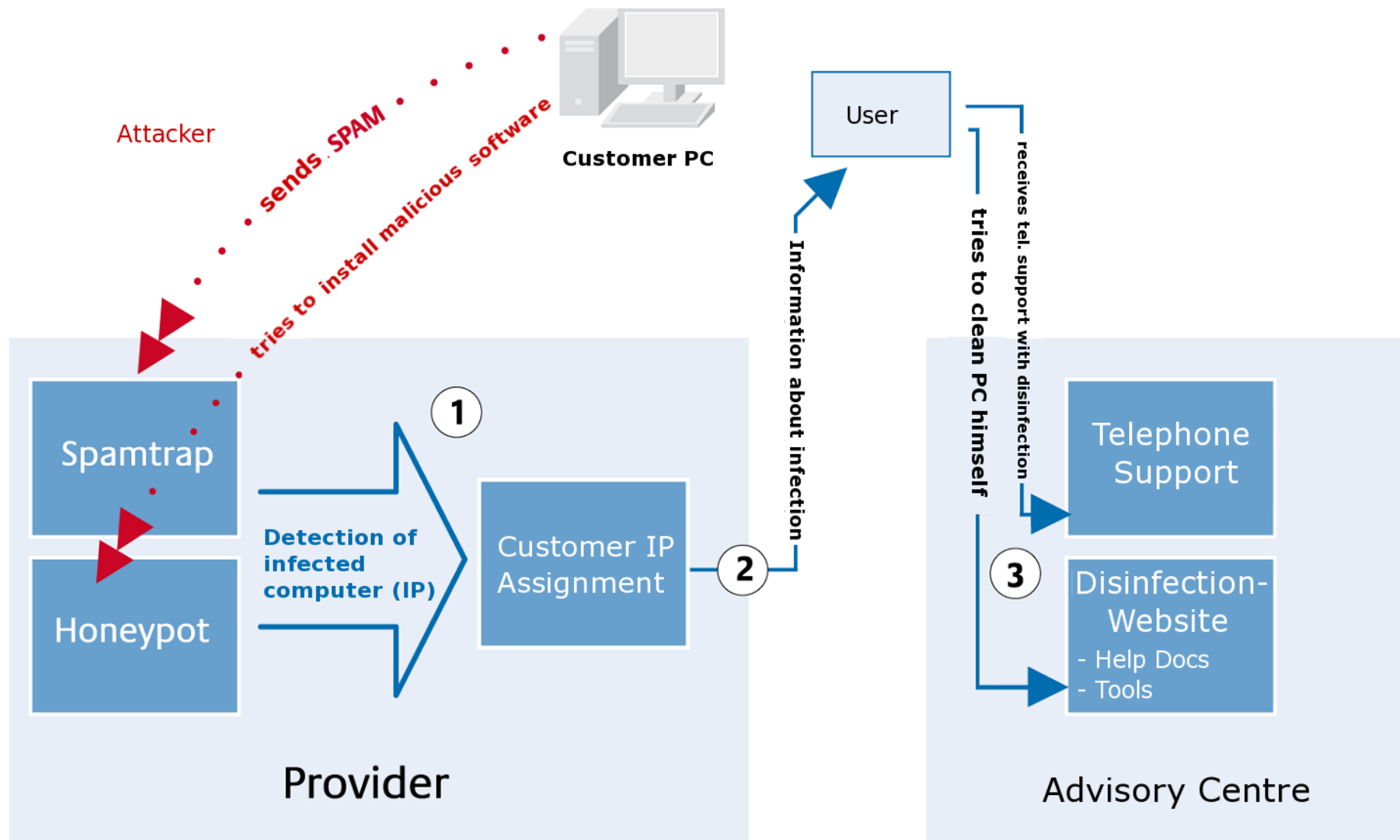


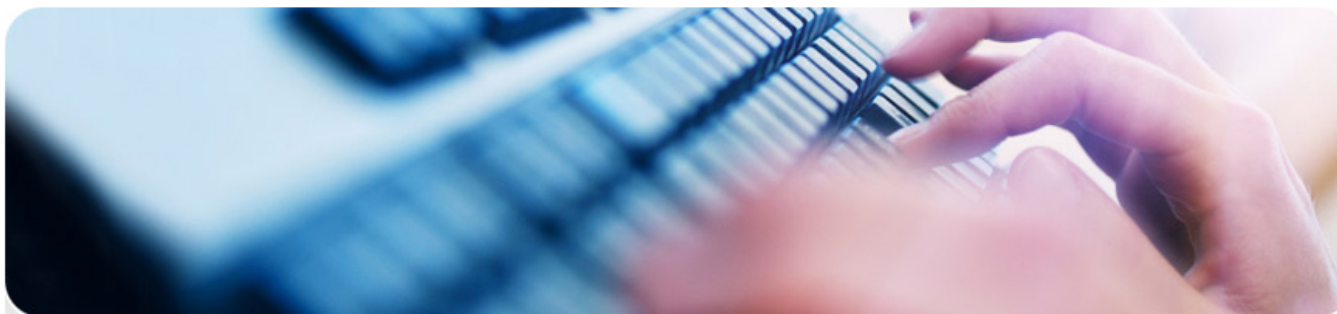
Goals of an Anti-Botnet-Advisory Center

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

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





Welcome!

About the Project
Participants
Contact
Data Privacy
Terms of Use

Welcome to the Anti-Botnet-Advisory Centre, a service from eco – Association of the German Internet Industry with support from the Federal Office for Information Security (BSI).

In the section [Inform](#) find out what Botnets are, what damage they can do and how they can threaten the data on your computer. In the section [Clean](#) our [DE-Cleaner](#) is available. With this tool you'll be able to free your PC from malicious software. In the section [Prevention](#) you will find useful hints on how to protect your computer against re-infection.

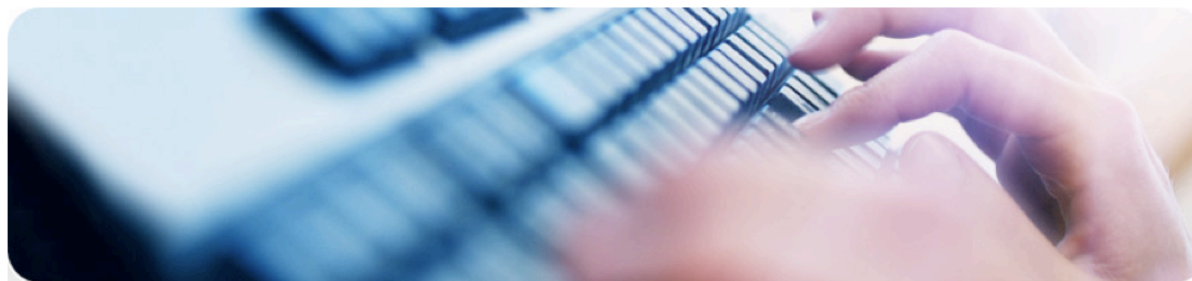
“ The Anti-Botnet Initiative is [...] a good example. [...]

This is a good initiative, further will follow. ”

[Interior Minister Dr. Thomas de Maizière at the Fifth National IT Summit on the 07.12.2010 in Dresden](#)

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 interested, to visit – www.botfrei.de
- Under *Advice* one receives detailed Information about Botnets, Malicious Software and Internet-Security



Säubern

- **Säubern**
 - DE-Cleaner
 - Online Scanner
 - Windows neu installieren

Hier stellen wir Ihnen Programme bereit, mit denen Sie Ihren Computer von Botnetz-Infektionen befreien können. Der DE-Cleaner erkennt Schadprogramme und entfernt sie. Ausführliche Anleitungen zu den Programmen finden Sie unter dem jeweiligen Menüpunkt.

Um eine erneute Infektion zu verhindern beachten Sie bitte diese wichtigen Regeln:

1. Überprüfen Sie Ihren Computer auf Befall. Benutzen Sie hierzu den [DE-Cleaner](#). Löschen Sie gefundene Schädlinge.
2. Installieren Sie aktuelle Service Packs und Sicherheitsupdates für Ihr System und aktivieren Sie automatische Updates. [Microsoft Anleitung: Schützen des Computers](#).
3. Installieren Sie einen Virens Scanner, z.B. einen der [hier](#) genannten und aktualisieren Sie ihn regelmäßig.
4. Benutzen Sie eine Firewall wie z.B. die windowseigene Firewall oder einen Router. [Microsoft Anleitung: Firewall Konfiguration](#).

Weitere Details zur Absicherung Ihres Computers finden Sie in der Kategorie [Vorbeugen](#) dieser Webseite.

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



Vorbeugende Maßnahmen

• Vorbeugen

Windows Einstellungen
Produkte für Privatpersonen
Produkte für Unternehmen
Firewall

Um einen optimalen Schutz zu gewährleisten, ist es notwendig, dass Systemaktualisierungen täglich und automatisiert eingespielt werden. In dieser Kategorie beschreiben wir Ihnen, wie Sie Ihr System vor Infektionen schützen können. Diese Maßnahmen können Ihnen helfen, sich sicherer im Internet zu bewegen.

Im Hinblick auf die Sicherheit Ihres Computers beachten Sie bitte folgende Grundregeln:

1. Überprüfen Sie Ihren Computer auf Befall. Benutzen Sie hierzu den [DE-Cleaner](#). Löschen Sie gefundene Schädlinge.
2. Installieren Sie aktuelle Service Packs und Sicherheitsupdates für Ihr System und aktivieren Sie automatische Updates. [Microsoft-Anleitung: Computer schützen](#).
3. Installieren Sie einen Virens Scanner, z.B. einen der [hier](#) genannten und aktualisieren Sie ihn regelmäßig.
4. Benutzen Sie eine Firewall wie z.B. die windowseigene Firewall oder einen Router. [Microsoft-Anleitung: Firewall Konfiguration](#).

Trotz dieser technischen Schutzmaßnahmen sollten Sie immer ein gesundes Misstrauen gegenüber E-Mails von fremden Absendern und/oder mit dubiosen Inhalt (Gewinnbenachrichtigungen, Aufforderungen, seine Kontodaten auf einer Webseite einzutragen usw.) oder mit Dateianhängen haben.

[weiter zu "Windows-Einstellungen"](#)

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
- Frasca & 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.

Thank you for your attention



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