

The German Anti-Botnet Advisory Center

Sven Karge

Head of 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 Botnetwork – unnoticed by computer owners
- Germany ranked within the Top Ten
- Botnets compose an infrastructure for organized Internet crime

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 criminal foundations
- Get Germany out of the Top10 Ranking of malicious activity

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

General Framework

- Project setup started March 2010
- Project started 15th September 2010
- Start-up funding of 2 Million EUR
- 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, ..)



Willkommen!

Über das Projekt
Projektteilnehmer
Kontakt
Datenschutz
Nutzungsbedingungen



Herzlich willkommen beim Anti-Botnet-Beratungszentrum, einem Service von eco – Verband der deutschen Internetwirtschaft e.V. mit Unterstützung des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

In der Rubrik [Informieren](#) erfahren Sie, was Botnetze sind, welchen Schaden sie anrichten können und wie sie die Daten auf Ihrem Computer bedrohen können. In der Rubrik [Säubern](#) steht der [DE-Cleaner](#) und die [DE-Cleaner Rettungssystem CD](#) zur Verfügung, mit dem Sie Ihren Rechner von Schadprogrammen befreien können. Unter [Vorbeugen](#) finden Sie viele hilfreiche Hinweise, wie Sie Ihren Computer nachhaltig vor neuen Infektionen schützen.

+++++Aus aktuellem Anlass stellen wir drei Anleitungen für die Bereinigung des BKA-Trojans bereit+++++

Weitere Informationen zum BKA-Trojaner finden Sie [hier](#). Für erfahrene Benutzer empfehlen wir die manuelle Methode. Unerfahrene Benutzer wählen eine der automatischen Varianten.

- [Manuell über die Registry \[pdf: 280 KB\]](#)
- [Automatisch mit dem Avira DE-Cleaner \[pdf: 470 KB\]](#)
- [Automatisch mit der Kaspersky Rescue-CD \[pdf: 955 KB\]](#)

Sollten Sie Hilfe benötigen, können Sie sich Montags bis Sonntags in der Zeit zwischen 9 und 21 Uhr unter 0231-1892650 (Festnetztarif) oder rund um die Uhr über technik@botfrei.de an das Anti-Botnet-Beratungszentrum wenden.

Inform → Clean → Prevention

- Internet-Service-Provider (ISP) and/or Bank inform customers of a Botnet infection on his/her computer
- A customer – including all others who are interested too - should visit – www.botfrei.de (available so far in German, English, French, Spanish, Danish and Turkish language)
- Under *Inform* he/she receives detailed Information about Botnets, Malicious Software and Internet-Security



Säubern

• Säubern

DE-Cleaner
Rettungssystem CD
Online Scanner
Windows neu installieren

Hier stellen wir Ihnen Programme bereit, mit denen Sie Ihren Computer von Botnetz-Infektionen befreien können. 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 Befehl. 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 Virenschanner, 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. [Mehr Informationen zu Firewalls](#).

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 needing 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 wichtige 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 windows eigene Firewall oder einen Router. [Mehr Informationen zu Firewalls](#).

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

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

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)
- (Fiducia)

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 – 31st May 2011)

- **Website Access:**
 - **1.056.880** Visitors
 - **5.362.734** Pages viewed
- **Activations of DE-Cleaner:**
 - powered by Symantec (15. Sept 10 – 31. May 11) **437.842**
 - powered by Kaspersky (07. Dez 10 – 31. May 11) **47.837**
 - powered by Avira (01. Mar 11 – 31. May 11) **60.739**

= **546.418 (!)** Downloads & Activations
- Tickets in Ticketsystem = notified end users: **213.155**
Less than 1% need telephone support; Call duration in average:
14 Min.

Statistics: Avira DE-Cleaner Logfile Analysis

sent Reports March 1st – May 31nd:

- scanned Systems: **42.552**
- not infected Systems: **31.025**
- infected Systems: **11.527**
(= 27,09%) !!!
- Total infected files **83.118**
- infected files per System on average **7,2**

Statistics: Kaspersky Malware Report Q1/2011

- Germany improved in Ranking (ranks on 6 now as regards countries with infected web resources, 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 stretching: Mac OS X / Linux / mobile systems

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