

# ECO AK Sicherheit

## Maßnahmen gegen Schadprogramme (Botnetz-Abwehr)

### Abuse-Management bei NetCologne

Identifizieren und Stoppen von Zombies



Dietmar Braun  
Gunther Nitzsche

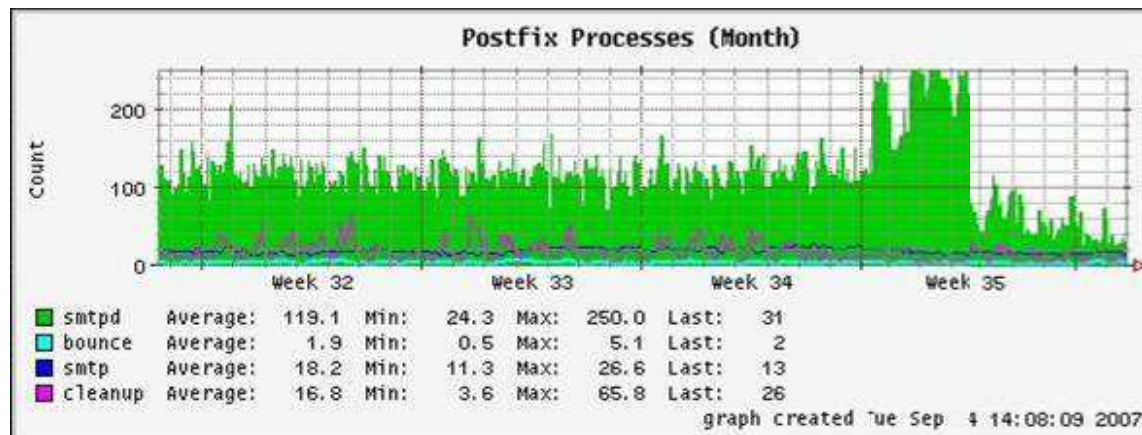
04.02.2009

# Agenda

- Anomalien und Botnetz-Entwicklung
- "hauseigene" Zombies
- das "enforced Portal"
- Feedback-Loops
- Tools (ANANAS)
- weitere Massnahmen
- das Honeypot-System
  - Schritt 1: der Honeypot
  - Schritt 2: der mwdb-Server (Malware Database)
  - Schritt 3: PHREAK (User-Aktionen)
  - Visualisierung
- Zusammenfassung und Ausblick

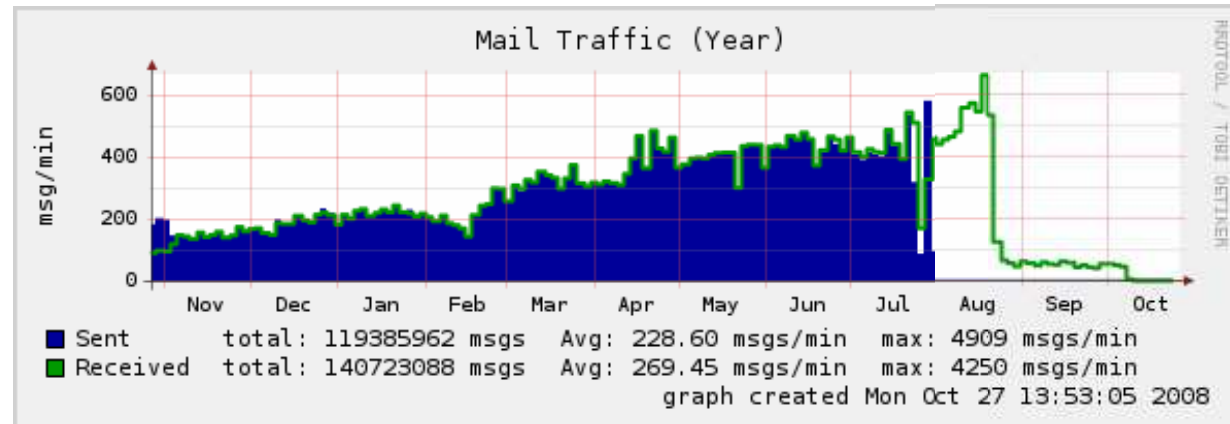
## Anomalien und deren Erkennung

- Traffic-Analyse (IDS, (Firewall-)Logs, Proxies, ...)
- Monitoring, Auditing
- Statistische Auswertungen, Vorausschätzungen
- Beispiel aus der täglichen Praxis:

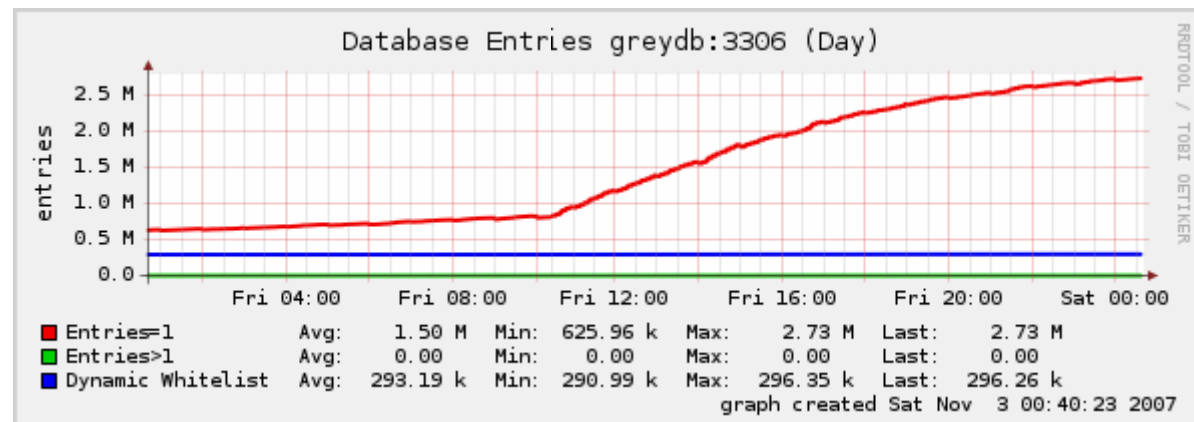


## Botnetz-Entwicklung, Bsp. Email

- Mailverkehr auf einer „spam only“-Domain:



- „bot counter“ nach Hinzufügen eines weiteren Netzes:

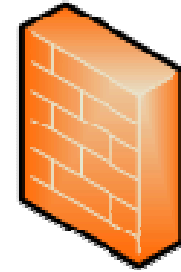


## Was tun mit „eigenen“ Zombies?

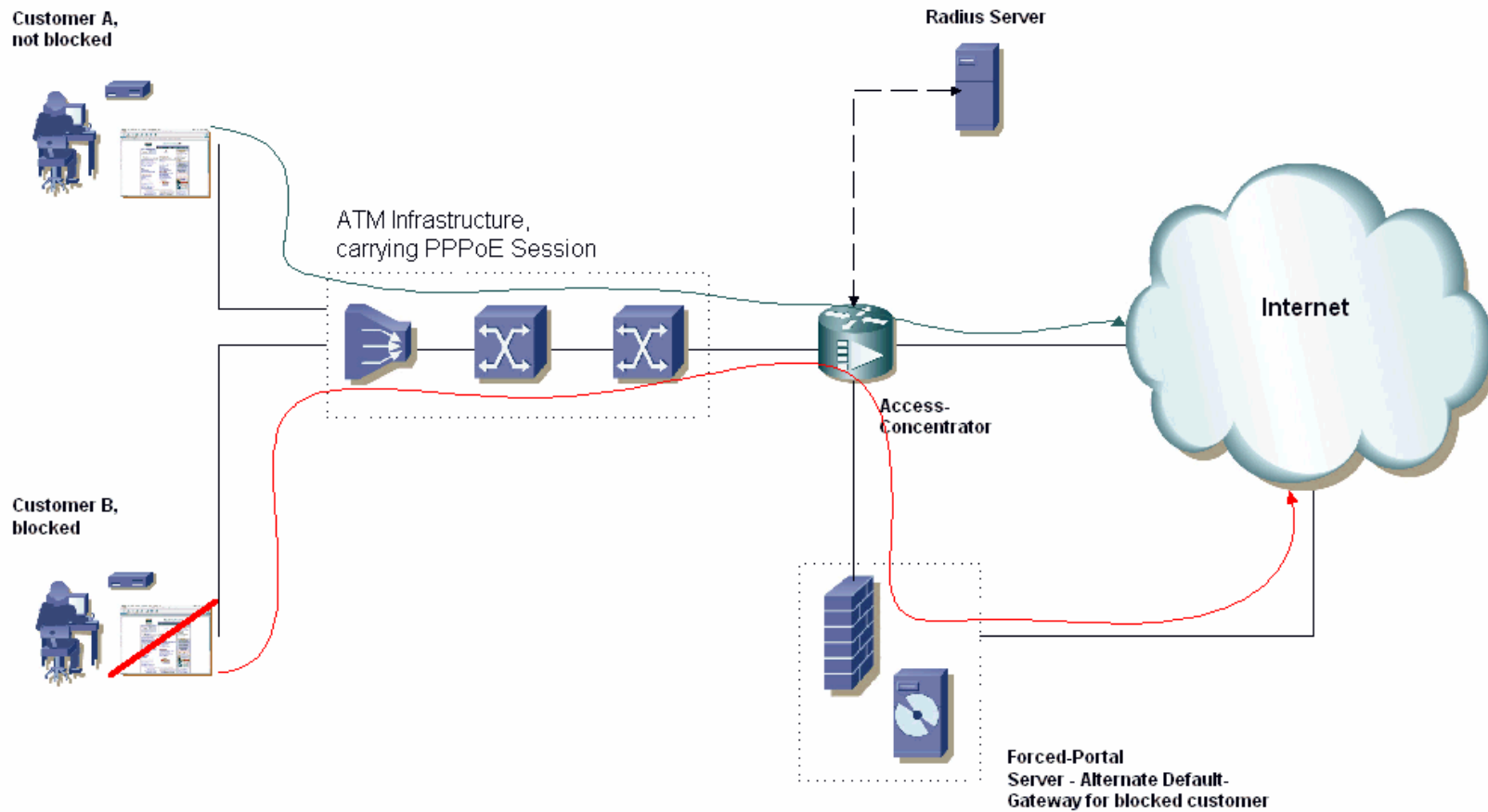
- User-Account sperren
  - bis auf Ausnahmen kein Internet-Verkehr mehr möglich
- Gesperrte User in das „enforced portal“ setzen
  - erlaubt dennoch das Herunterladen von Patches etc.
- Gesperrte User aktiv informieren
  - findet i.d.R. telefonisch durch den Support statt
- Honeypot, um Bots automatisch zu finden und zu sperren
- „fremde“ Zombies: Beschwerde an ISP (feedback loop)

## Das „enforced portal“

- blockiert nahezu komplett die Internet-Kommunikation – verhindert u.a. weiteren Spam
- klemmt den Benutzer sofort vom Netz ab, verhindert somit weiteren Netzmissbrauch
- informiert den Benutzer über eine Webseite, wenn er versucht, sich neu einzuwählen
- erlaubt Herunterladen des NC-Sicherheitspaketes
- erlaubt Zugriff auf gängige Update-Server, um Patches etc. herunterladen zu können
- erlaubt selbständiges Freischalten des Benutzers (!)



# Funktion des „enforced portal“





## Beschwerden bei anderen ISPs

- „feedback loop“: erkannter Netzmissbrauch führt zu
  - untersuchen
  - Quelle analysieren
  - Meldung des Vorfalls an den verantwortlichen ISP
  
- beim ISP sollte passieren:
  - untersuchen
  - verantwortlichen Verursacher ermitteln
  - Einleiten von Massnahmen gegen Verursacher

**beides geschieht teilweise vollautomatisch!**



# Abuse-Management-Tools

- A.N.A.N.A.S.: Beschwerden halbautomatisch bearbeiten



## A.N.A.N.A.S.

Automatic Network Abuse Notification Analyzing System

*v1.00 by Dietmar Braun, Aug 2007*

*Requesting tickets from RT - please be patient...*

<input type="checkbox"/> Ticket #	<input type="checkbox"/> Subject	Created
<input type="checkbox"/> 209484	<input type="checkbox"/> Possible Spam Abuse Report - netcologne.de - 87.79.226.196	2007-09-04 11:15:00
<input type="checkbox"/> 209488	<input type="checkbox"/> Possible Spam Abuse Report - netcologne.de - 213.196.205.109	2007-09-04 12:21:06
<input type="checkbox"/> 209490	<input type="checkbox"/> Possible Spam Abuse Report - netcologne.de - 213.196.205.109	2007-09-04 12:21:08
<input type="checkbox"/> 209491	<input type="checkbox"/> Possible Spam Abuse Report - netcologne.de - 87.78.34.159	2007-09-04 12:25:05
<input type="checkbox"/> 209492	<input type="checkbox"/> Possible Spam Abuse Report - netcologne.de - 87.78.34.159	2007-09-04 12:25:13
<input type="checkbox"/> 209493	<input type="checkbox"/> [auto-generated] Spam aus Ihrem Adressbereich: 195.14.205.150	2007-09-04 12:28:39
<input type="checkbox"/> 209496	<input type="checkbox"/> [SpamCop (87.78.89.154) id:2479972843]pkr poker	2007-09-04 12:56:25
<input type="checkbox"/> 209498	<input type="checkbox"/> Possible Spam Abuse Report - netcologne.de - 87.79.107.54	2007-09-04 13:04:44

Found **8** records.

Resolve tagged tickets



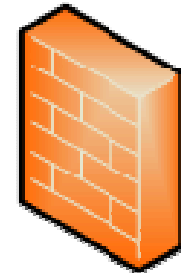
# „ein Klick – ein abgeklemmter Bot“

Ticket Data		User Data		Blacklist Data
Ticket number	217807 (Type: SpamCop)	IP & timestamp	87.78.98.233 (xdsI-87-78-98-233.netcologne.de) Sat, 3 Nov 2007 08:32:40 -0700 Sat, 03 Nov 2007 16:32:40 +0100	No blacklist entries found!
Subject	[SpamCop (87.78.98.233) id:2597044620]More sexual partners. More orgasms. More pleasure	Username	[REDACTED]	Blocked because: Versand von Spam-E-Mails Blocking comment: #217807: Spam, offener Proxy?
Created	2007-11-03 15:45:20	Login	since 2007-11-03 08:06:03	Charge: <input type="text"/> EURO

- block user
- resolve RT
- resolve SpamCop
- resolve multiple:
- 217753
- 217754
- 217773
- 217787
- 217815
- 217820
- 217825
- 217828
- 217829
- 217844
- 

Content: [ SpamCop V640 ]  
 This message is brief for your comfort. Please use links below for details.  
 Email from 87.78.98.233 / Sat, 3 Nov 2007 08:32:40 -0700  
<http://www.spamcop.net/w3m?i=z2597044620z3d5729d04c0078090a18d08b990f82f3z>  
 [ Offending message ]

## Blocken von weiteren Ports



- Gründe für die Idee:
  - ISPs wollen Traffic nicht komplett beschneiden
  - nur „reaktive“ Massnahmen
    - man reagiert leider erst hinterher...
    - nicht alle Bots werden vom Honeynet „erschlagen“
  - ständig weitere Entwicklungsarbeit notwendig
    - auch entwickelte Tools haben ihre Grenzen
- ist Port-Blocking eine wirksame Massnahme gegen Botnetze (Bsp.: Port 25-Block)?

**generell: nein (von Ausnahmen abgesehen)**

## Weitere Massnahmen

- Intensivierung der Kooperation zwischen ISPs und anderen Gremien
- Verkürzen der Dienstwege und der Kommunikation
- Intensivierung der technischen Beratung von Legislative, Judikative und Exekutive
- beste Massnahmen nach wie vor: Aufklärung / Informierung der Kunden / Zielgruppe!



## Das NetCologne Honeypot-System

- **Überblick:**

Die NetCologne GmbH betreibt einen Honeypot-Server, der in verschiedenen IP-Adressnetzen „lauscht“.

Ziel ist es, Angriffe durch PC's aus NetCologne – eigenen IP-Adressräumen zu erkennen und darauf (mit Sperren und Informieren des Angreifers) zu reagieren.



## Das NetCologne HoneyPot-System

- **Schritt 1: der HoneyPot**

kleiner (virtueller) Server mit Debian Linux

HoneyPot-Software: „nepenthes“ der mwcollect – Allianz:

<http://nepenthes.mwcollect.org>

- low interactive HoneyPot
- konfigurierbare Module für Übermittlung und Exploits



# Das NetCologne Honeypot-System

```
sys-136
File Edit View Options Transfer Script Tools Help
sys-136
#netstat -ap
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 *:1025                  *:                       LISTEN      24172/nepenthes
tcp        0      0 *:imaps                 *:                       LISTEN      24172/nepenthes
tcp        0      0 *:pop3s                 *:                       LISTEN      24172/nepenthes
tcp        0      0 *:3140                  *:                       LISTEN      24172/nepenthes
tcp        0      0 *:loc-srv               *:                       LISTEN      24172/nepenthes
tcp        0      0 *:5000                  *:                       LISTEN      24172/nepenthes
tcp        0      0 *:nameserver            *:                       LISTEN      24172/nepenthes
tcp        0      0 *:netbios-ssn           *:                       LISTEN      24172/nepenthes
tcp        0      0 *:3372                  *:                       LISTEN      24172/nepenthes
tcp        0      0 *:pop3                  *:                       LISTEN      24172/nepenthes
tcp        0      0 *:imap2                 *:                       LISTEN      24172/nepenthes
tcp        0      0 *:webmin                *:                       LISTEN      24172/nepenthes
tcp        0      0 *:www                   *:                       LISTEN      24172/nepenthes
tcp        0      0 *:6129                  *:                       LISTEN      24172/nepenthes
tcp        0      0 *:ssmtp                 *:                       LISTEN      24172/nepenthes
tcp        0      0 *:5554                  *:                       LISTEN      24172/nepenthes
tcp        0      0 *:27347                 *:                       LISTEN      24172/nepenthes
tcp        0      0 *:17300                 *:                       LISTEN      24172/nepenthes
tcp        0      0 *:ftp                   *:                       LISTEN      24172/nepenthes
tcp        0      0 *:ssh                   *:                       LISTEN      2062/sshd
tcp        0      0 *:3127                  *:                       LISTEN      24172/nepenthes
tcp        0      0 *:2103                  *:                       LISTEN      24172/nepenthes
tcp        0      0 *:postgresql            *:                       LISTEN      24172/nepenthes
tcp        0      0 *:eklogin               *:                       LISTEN      24172/nepenthes
tcp        0      0 *:2745                  *:                       LISTEN      24172/nepenthes
tcp        0      0 *:smtp                  *:                       LISTEN      24172/nepenthes
tcp        0      0 localhost:5433          *:                       LISTEN      1872/postmaster
tcp        0      0 *:2107                  *:                       LISTEN      24172/nepenthes
tcp        0      0 *:https                 *:                       LISTEN      24172/nepenthes
tcp        0      0 *:imap3                 *:                       LISTEN      24172/nepenthes
tcp        0      0 *:microsoft-ds         *:                       LISTEN      24172/nepenthes
tcp        0      0 *:1023                  *:                       LISTEN      24172/nepenthes
tcp        0      0 [REDACTED].netcologne:55877 mwdb1.netcol:postgresql ESTABLISHED 24172/nepenthes
tcp        0      0 3888 [REDACTED].netcologne.d:ssh doku.netcologne.d:58349 ESTABLISHED 10369/sshd: gnitzzc
udp        0      0 localhost:32768        localhost:32768        ESTABLISHED 1872/postmaster
udp        0      0 *:ms-sql-m              *:                       LISTEN      24172/nepenthes
```





## Das NetCologne Honeypot-System

Die empfangenen Angriffsinformationen (IP, Malware, Zeit..) werden übermittelt:

- durch das Modul „submit-postgres“ an einen „malware database server“ (mwdb), auf dem ein „gdsd“ – Daemon läuft (für: generic do something daemon), geschrieben von Emre Bastuz, der die weitere Analyse vornimmt. Siehe Schritt 2 ..
- durch das Modul „submit-norman“ an sog. „Sandboxes“ wie „cwsandbox“ zur externen Analyse der Daten
- durch das Modul „submit-http“ an einen (GUI) Frontend-server → nepenthesFE (von Emre Bastuz) für die Visualisierung der Angriffe

<http://www.emre.de/wiki/NepenthesFE>



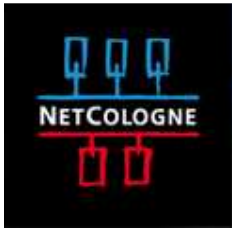
## Das NetCologne HoneyPot-System

### ▪ Schritt 2: Der mwdb – Server

Ein weiterer Server (mwdb) erhält die Angriffsinformation über eine postgres-Verbindung und speichert diese lokal.

Der Software-Daemon „gdsd“ kümmert sich um die gespeicherten Daten:

- prüft die Daten mittels AV Software BitDefender
- prüft die Daten mittels AV Software ClamAV
- prüft die Daten mit ‚objdump‘
- prüft die Daten mit ‚file‘
- prüft die Daten mit ‚upx ‚
- prüft die Daten mit ‚strings‘
- sendet die gesammelten Informationen über eine SOAP-Schnittstelle an einen internen Server -> Schritt 3 ...



## Das NetCologne HoneyPot-System

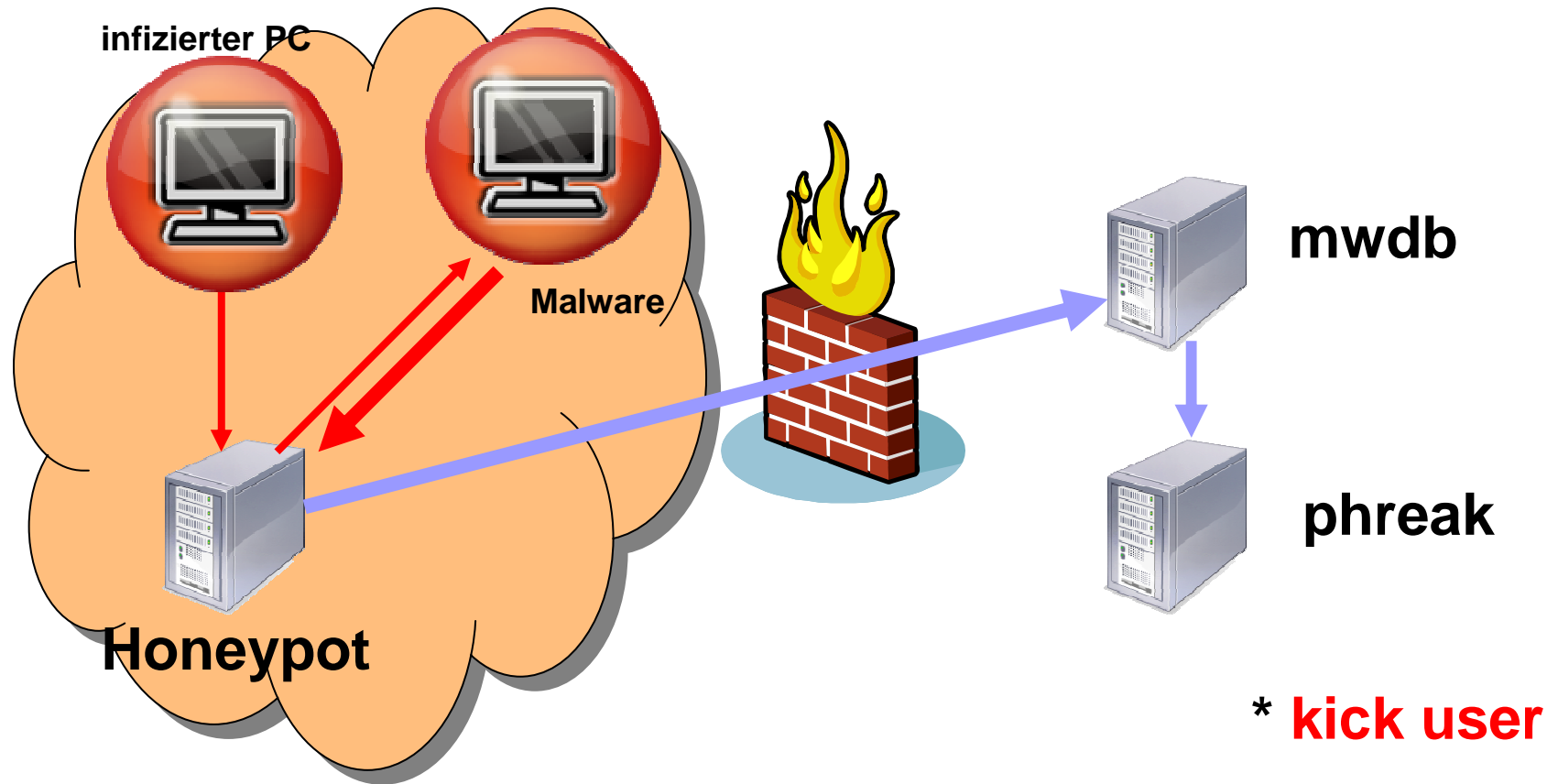
### ▪ Schritt 3: PHREAK

„Program for honeypot induced reaction ending in automated kill“

nimmt den SOAP-Aufruf auf einem zentralen Server entgegen und handelt bei einer erfolgreichen Angriffsinformationsübermittlung:

- der User wird identifiziert
- ein Ticket im Abuse-Ticket-System wird erzeugt (Request Tracker)
- zugehörige Tickets im System (Beschwerden z.B.) werden auf abgeschlossen gesetzt
- Phreak ermittelt die Mahnstufe des betroffenen Users (letzte 6 Monate) und erhöht diese
- wirft den User aus dem System (mittels ANANAS)
- generiert eine Mail an den Kundensupport, damit dieser den User telefonisch kontaktiert und ihm bei der Beseitigung des Problems unterstützt (evtl. Verkauf eines AV-Produkts)

# Das NetCologne Honeypot-System





## Das NetCologne HoneyPot-System

- **Visualisierung:**































Die Frontend-Software „nepenthesFE“ (von Emre Bastuz) liefert ein schönes Web-Frontend zur Visualisierung der Angriffe. Eine Sortierung z.B. nach dem Ursprungs – AS ist möglich.



## NepenthesFE - Version 0.03

[Hits](#)
[Malware](#)
[Users](#)
[Sensors](#)
[Logout](#)

[1](#)
[«](#)
[3](#)
[|](#)
[4](#)
[|](#)
[5](#)
[»](#)
[\[5\]](#)

Hash	Source IP <input type="checkbox"/>	Target IP <input type="checkbox"/>	Date <input type="checkbox"/>	City
<a href="#">d3820c57ffb93f4ee5d281b10c09ff0d</a>	78.X.X.X	78.X.X.X	2008-04-18 16:05:30	 Vilnius
<a href="#">692b242ffa3312f2bf289ed8cd404b8c</a>	78.X.X.X	78.X.X.X	2008-04-18 16:04:52	 Ankara
<a href="#">f7b957a81c0fb7119e023f6b524638ac</a>	78.X.X.X	78.X.X.X	2008-04-18 21:30:33	 Cologne
<a href="#">f7b957a81c0fb7119e023f6b524638ac</a>	78.X.X.X	78.X.X.X	2008-04-18 21:31:11	 Cologne
<a href="#">f7b957a81c0fb7119e023f6b524638ac</a>	78.X.X.X	78.X.X.X	2008-04-18 21:25:35	 Cologne
<a href="#">f7b957a81c0fb7119e023f6b524638ac</a>	78.X.X.X	78.X.X.X	2008-04-18 21:30:55	 Cologne
<a href="#">0d39e417aa13754627f599ced9a4f6ff</a>	78.X.X.X	78.X.X.X	2008-04-18 16:04:54	 Budapest
<a href="#">f7b957a81c0fb7119e023f6b524638ac</a>	78.X.X.X	78.X.X.X	2008-04-18 21:31:05	 Cologne
<a href="#">f7b957a81c0fb7119e023f6b524638ac</a>	78.X.X.X	78.X.X.X	2008-04-18 21:31:03	 Cologne
<a href="#">f7b957a81c0fb7119e023f6b524638ac</a>	78.X.X.X	78.X.X.X	2008-04-18 21:31:05	 Cologne
<a href="#">f7b957a81c0fb7119e023f6b524638ac</a>	78.X.X.X	78.X.X.X	2008-04-18 21:22:49	 Cologne
<a href="#">d3820c57ffb93f4ee5d281b10c09ff0d</a>	78.X.X.X	78.X.X.X	2008-04-18 16:02:14	 Vilnius
<a href="#">f7b957a81c0fb7119e023f6b524638ac</a>	78.X.X.X	78.X.X.X	2008-04-18 21:31:21	 Cologne
<a href="#">f7b957a81c0fb7119e023f6b524638ac</a>	78.X.X.X	78.X.X.X	2008-04-18 21:31:17	 Cologne
<a href="#">f7b957a81c0fb7119e023f6b524638ac</a>	78.X.X.X	78.X.X.X	2008-04-18 21:24:05	 Cologne
<a href="#">f7b957a81c0fb7119e023f6b524638ac</a>	78.X.X.X	78.X.X.X	2008-04-18 21:31:29	 Cologne
<a href="#">f7b957a81c0fb7119e023f6b524638ac</a>	78.X.X.X	78.X.X.X	2008-04-18 21:31:23	 Cologne
<a href="#">692b242ffa3312f2bf289ed8cd404b8c</a>	78.X.X.X	78.X.X.X	2008-04-18 16:03:02	 Camarate
<a href="#">f7b957a81c0fb7119e023f6b524638ac</a>	78.X.X.X	78.X.X.X	2008-04-18 21:31:21	 Cologne
<a href="#">f7b957a81c0fb7119e023f6b524638ac</a>	78.X.X.X	78.X.X.X	2008-04-18 21:24:33	 Cologne
<a href="#">3952d4ea6ccfdec211f5dfa1536efcdf</a>	78.X.X.X	78.X.X.X	2008-04-18 16:02:44	 Vilnius
<a href="#">f7b957a81c0fb7119e023f6b524638ac</a>	78.X.X.X	78.X.X.X	2008-04-18 21:31:35	 Cologne
<a href="#">692b242ffa3312f2bf289ed8cd404b8c</a>	78.X.X.X	78.X.X.X	2008-04-18 16:03:46	 Sofia
<a href="#">f7b957a81c0fb7119e023f6b524638ac</a>	78.X.X.X	78.X.X.X	2008-04-18 21:31:29	 Cologne
<a href="#">3952d4ea6ccfdec211f5dfa1536efcdf</a>	78.X.X.X	78.X.X.X	2008-04-18 16:04:52	 Vilnius
<a href="#">692b242ffa3312f2bf289ed8cd404b8c</a>	78.X.X.X	78.X.X.X	2008-04-18 16:03:56	 Sofia
<a href="#">f7b957a81c0fb7119e023f6b524638ac</a>	78.X.X.X	78.X.X.X	2008-04-18 21:22:27	 Cologne
<a href="#">f7b957a81c0fb7119e023f6b524638ac</a>	78.X.X.X	78.X.X.X	2008-04-18 21:31:29	 Cologne
<a href="#">62819008a008f3d16ec7b56486e3c7c8</a>	78.X.X.X	78.X.X.X	2008-04-18 16:04:58	 Bratislava
<a href="#">b39ed154a8ceee8624d805239546ec55</a>	78.X.X.X	78.X.X.X	2008-04-18 16:05:02	 Rostock

### NepenthesFE - Version 0.03

[Hits](#) [Malware](#) [Users](#) [Sensors](#) [Logout](#)

#### Details obtained from Nepenthes

Hash MD5	<a href="#">d3820c57ffb93f4ee5d281b10c09ff0d</a>		
Date of occurrence	2008-04-18 16:05:30	URL	ftp://1:1@78.X.X.X:30636/Win
E-Mail	gnitzsche@netcologne.de	Sensor	██████.netcologne.de
Source IP Address	78.X.X.X	Target IP Address	78.X.X.X
Trigger	ftp://1:1@78.X.X.X.exe	Filename	WinTcpiops.exe
Filetype	MS-DOS executable PE for MS Windows (GUI) Intel 80386 32-bit		
Hash SHA512	b7dd10314451c32870bf3da3d56871ec54279f9ddb1863782a8f7bf367c38e1853c68d7ef708e1		

#### GeolIP Details

Country	 Lithuania
City	Vilnius

#### Autonomous System Details

Autonomous System Number	18764
Network	78.56.128.0/17
IP Registry	ripence



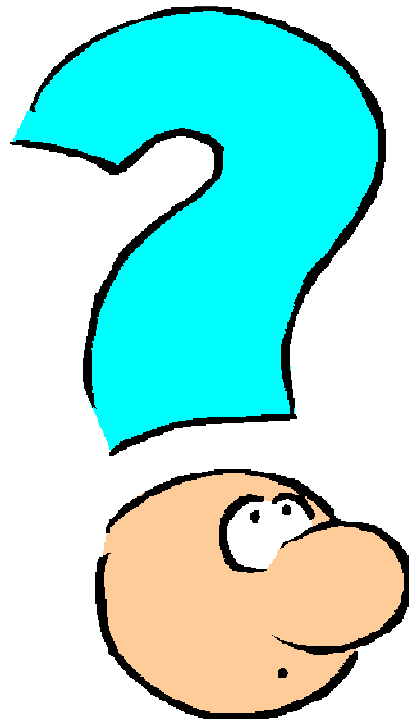


## Das NetCologne Honeypot-System

- Zusammenfassung und Ausblick:
  - Es ist möglich, trojanisierte PC's mittels Honeypotsystemen zu erkennen und diese zu blocken. NetCologne hat ein solches System erfolgreich im Einsatz.
  - Informationen über erkannte infizierte IP-Adressen könnten auch an verschiedene Adressen je nach AS gesendet werden.
  - Es wäre daher möglich, ein „trusted ISP-honeynet“ aufzubauen, in dem erkannte Zombie-Rechner „on the fly“ geblockt werden können.

Die Anzahl infizierter PC's könnte drastisch reduziert werden!

**Vielen Dank für die Aufmerksamkeit!**



**Dipl.-Inf. Dietmar Braun**  
**Dipl.-Phys. Gunther Nitzsche**  
**NetCologne GmbH**

Fon: +49 221 2222 0

Fax: +49 221 2222 5330

Mail: [dietmar.braun@netcologne.de](mailto:dietmar.braun@netcologne.de)  
[gnitzsche@netcologne.de](mailto:gnitzsche@netcologne.de)

Web: <http://www.netcologne.de>