Bundesamt
für Sicherheit in der
Informationstechnik

Starting the German Anti-Botnet Initiative

Willi Herzig
Federal Office for Information Security (BSI)

ENISA Workshop on Botnet Detection, Measurement, Disinfection & Defence
March 9th 2011

Goals of the initiative

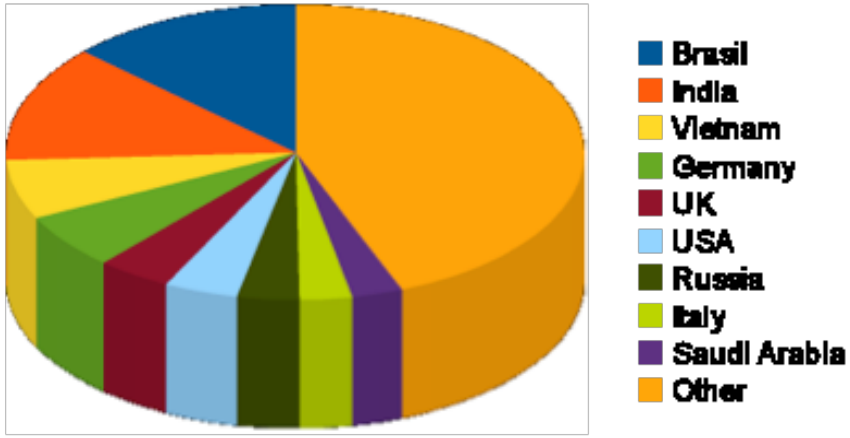
- Get Germany out of Top 10 botnet countries
- Help citizens
- Reduce threats to government networks
  - Raise Awareness
  - Detect user systems infected
  - Inform users with infected computers
  - Help users to get rid of infections

Participants

- eco – Association of the German Internet Industry has established the German Anti-Botnet advisory center
- German ISPs
- BSI supports eco in this context

Analysing the situation: Sources of Spam: July 2010

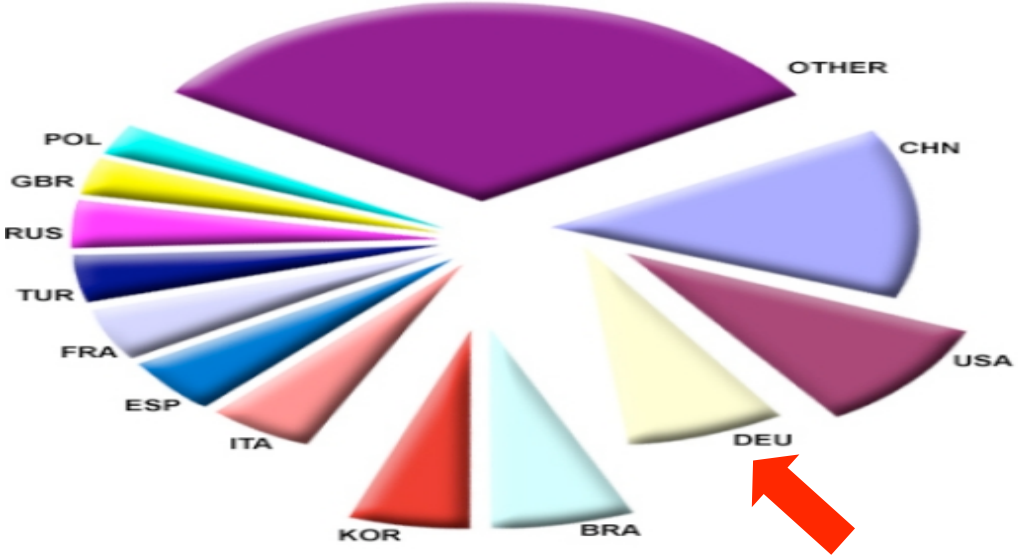
Rank	Country	Percentage
1	Brasil	13,05%
2	India	12,78%
3	Vietnam	6,51%
4	Germany	6,11%
5	UK	4,14%
6	USA	4,12%
7	Russia	3,49%
8	Italy	2,93%
9	Saudi Arabia	2,85%
10	Other	44,02%
	...	
49	Japan	0,31%



Source: BSI

Analysing the situation

Compromised systems by country (Source: Trendmicro)



Trendmicros analysis of approx. 100 million compromised IPs:

→ 80% of all IP addresses were infected for more than one month!

→ 50% of all IP addresses were infected for at least 300 days!

Source 2009/09/16 http://blog.trendmicro.com/the-internet-infestation-how-bad-is-it-really/

What can citizens do?

Basic defense

- Run anti-virus software and keep it up to date
- Install personal firewall software
- Keep Windows and applications up to date

- Be careful and use common sense before deciding to open e-mail attachments
- Be careful of active content (Consider using noscript on your browser)
- …

But why doesn't it work?

Why does basic defense not work? What is the problem?

- Obstacles
  - Users are overwhelmed
  - Users are not aware what botnets can do
  - Users imagine themselves to be save
  - Users do not notice that they are a part of a botnet
  - Bad guys are faster than basic defense

- **Users are victims & become offenders at the same time without knowing**
- **Users needs to be informed!**

Identifying a strategy

- Information collection
  - looked at other initiatives: Japan, Australia, Korea
  - joined congresses (BTF, DCC, MAAWG, ...)
  - International discussions (G8, EU, etc.)
  - statistics and papers
  - discussions with ISPs
  - .....

Take steps
What do we need?

- Identify infected systems
- Raise Awareness
- Notify users
- Support website to help cleaning the systems offering tools
- Offer support by a Call-Center
- Prevent new infections

Identify infected systems

- Needed: Infected systems are identified by Internet-Service-Providers (ISP)
  - Spamtraps
  - Honeypots
  - ...
  - Exchange of information among ISP
  - Use as many information as legally possible
- Before we started:
  - Some ISP already had honeypots and spamtraps
  - Only few exchanged informations between ISPs (why only few?)

Identify infected systems: Steps

- several workshops with Eco, BSI and ISPs (first 2008):
  - identified sources of abuse information
  - ISPs agreed to exchange information
  - ISPs do not want central exchange:
    - *„information does not get better by distributing it“*
  - Trust is the key factor on information exchange:
    - accurate time stamps, knowing the people, ...
- Problems:
  - common exchange format was needed
  - identify abuse contact for ISP
  - tools to parse and generate exchange format are needed

Setting up a Trusted Network to fight Botnets

Concept

- Global, efficient exchange of information across all ISPs
- ISPs exchange anonymized abuse reports with each other
- Abuse reports contains information about infected computers
- The provider decides on its own:
  - Whom to send
  - How to process and rate the received information
  - What do do with the information
  - About Customer notification

Setting up a Trusted Network to fight Botnets

- A typical ISP
  - operates Honeypots
  - operates Spamtraps
  - operates ....
  - gets abuse notifications
  - gets external abuse information
  - send abuse messages to other ISPs

Setting up a Trusted Network: Exchange format

Problem:

- We need something small, simple, extensible
- Needs to be processed automatically
- IODEF seems to be too complicated
- ARF (RFC 5965) looks fine, but only handles spam
- ARF people were asked to enhance ARF, but ....

Solution:

- Eco & BSI: enhances ARF: X-ARF
  See http://www.x-arf.org/
  - based on ARF
  - easily extensible via schemes
  - tools to generate and parse X-ARF

Setting up a Trusted Network: How to identify Abuse contacts

The next problem:

How do we identify abuse contacts of ISPs (e-mail addresses)?

- Problems:
  - many RIR databases (ARIN, RIPE, ...)
  - abuse contact mail adresses are not well maintained
- RIPE (European Registry) offers WHOIS-Service to query abuse contact

Interim Solution:

- Abusix () offers free contact database based on inverse DNS query

Setting up a Trusted Network: How to identify Abuse contacts

Abuse Contact DB:

- Uses only the biggest by RIRs (ARIN, RIPE, LACNIC, APNIC, AFRINIC) allocated ranges and the abuse contact address
- Service can be used like an RBL (Realtime Blackhole List) through DNS
-

Example:

```
>host -t TXT 117.116.227.212.abuse-contacts.abusix.org
117.116.227.212.abuse-contacts.abusix.org descriptive
  text "abuse@oneandone.net"
```

Notification

- ISPs flow:
  - ISP gets abuse message in X-ARF format →
  - rating/scoring depending on trust →
  - escalation process →
  - customer notification about infection

- Notification of infected customers by
  - e-mail, mail, preposed websites, ...
  - No general blocking of users!

State of play

- German government welcomes and supports the ISPs driven initiative with a start-up funding of 2 million EUR in the first year
- ISPs takes necessary technical and organizational steps (information exchange, informing users, ..)
- 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

Why does the government support this?

- Previous initiatives failed
- Some reasons:
  - Provider market is fiercely competed for in Germany
  - Fear of damaged reputation or of customer annoyance
  - ISP Call-Center can not handle additional users requests
- Call-Center to support users and to assist ISPs is needed!
- Cooperative initiative / partnership
- Start-up funding by the government made it possible to start this important initiative
- eco will develop a business model to continue a successful intitiative on a long term base

Enhancing the initiative:

- Support-Website is available in different languages:
  - German: Willkommen!
  - English: Welcome!
  - French: Bienvenue !
  - Turkish: Hoş geldiniz!
- Cooperations with countries worldwide are appreciated
- All Countries are welcome to participate the initiative!

Thank you very much for your attention!

Contact