
security is not an island
HILTONMALTA
24th Annual
FIRST
Conference
MALTA
17 - 22 June 2012
FIRST
Improving Security Together

Malware Free Switzerland

Michael Hausding – SWITCH
Philipp Rütsche – Swisscom

SWITCH
Serving Swiss Universities

swisscom

24th Annual FIRST Conference
MALTA
17 - 22 June 2012

Malware Free Switzerland (MAFRECH)

24th Annual FIRST Conference
MALTA
17 - 22 June 2012

„I wonder if we can get a whole country malware free“

Jeff Williams (Microsoft) FIRST conference 2011 Vienna

24th Annual FIRST Conference MALTA 17 - 22 June 2012

MAFRECH

Participants:

- 4 Major ISPs (Swisscom, Cablecom, Sunrise, Orange)
- Registry, NREN (SWITCH)
- GovCERT (MELANI)
- Law Enforcement
- Microsoft

Malware Free Switzerland

„Our vision is a malware free Switzerland“

How to get a country free of Malware?

1. Remove existing Infections
2. Prevent new Infections

#Removed Infections > #New Infections
=> Success

Malware Free Switzerland

- Raising awareness in Switzerland
- Communication
- Official Website
- Data sharing about infected clients and malicious URLs

- Technical & administrative measures against malware by ISPs and the .ch registry

Fighting Drive-By-Infections

24th Annual FIRST Conference
MALTA
17 - 22 June 2012

World Map - PSI - Consum

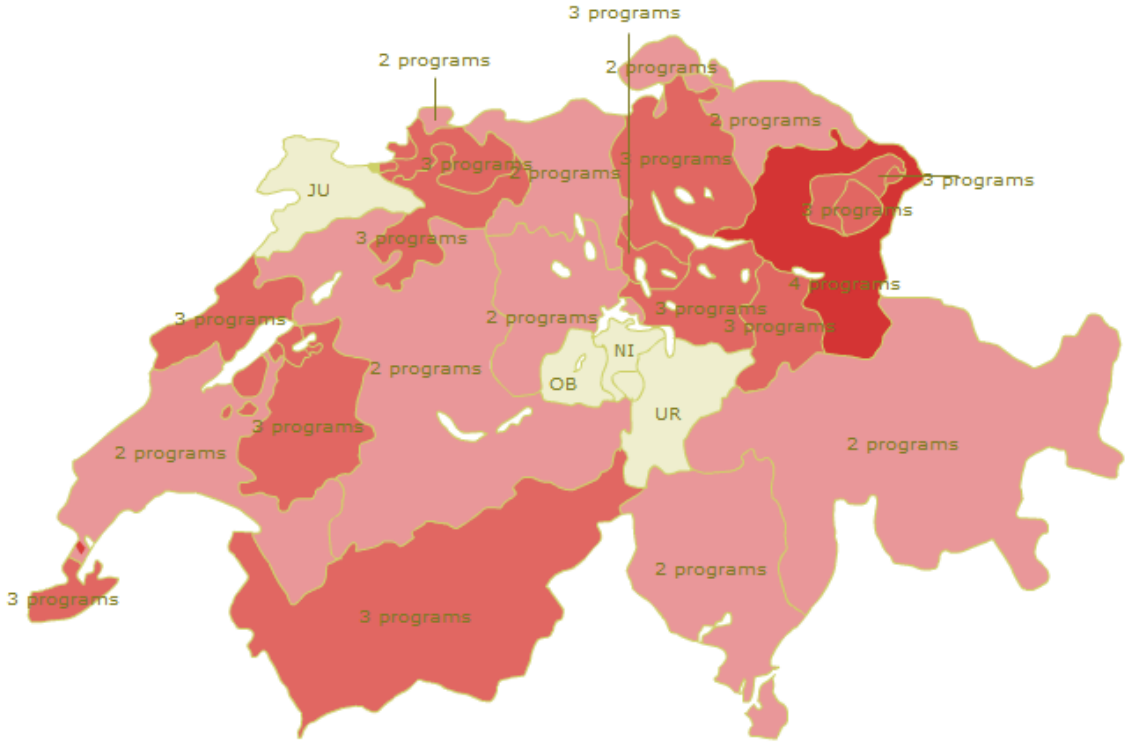
secunia.com/vulnerability_scanning/personal/worldmap/?view=EU.CH,insecure

- FAQ
- Testimonials

OSI

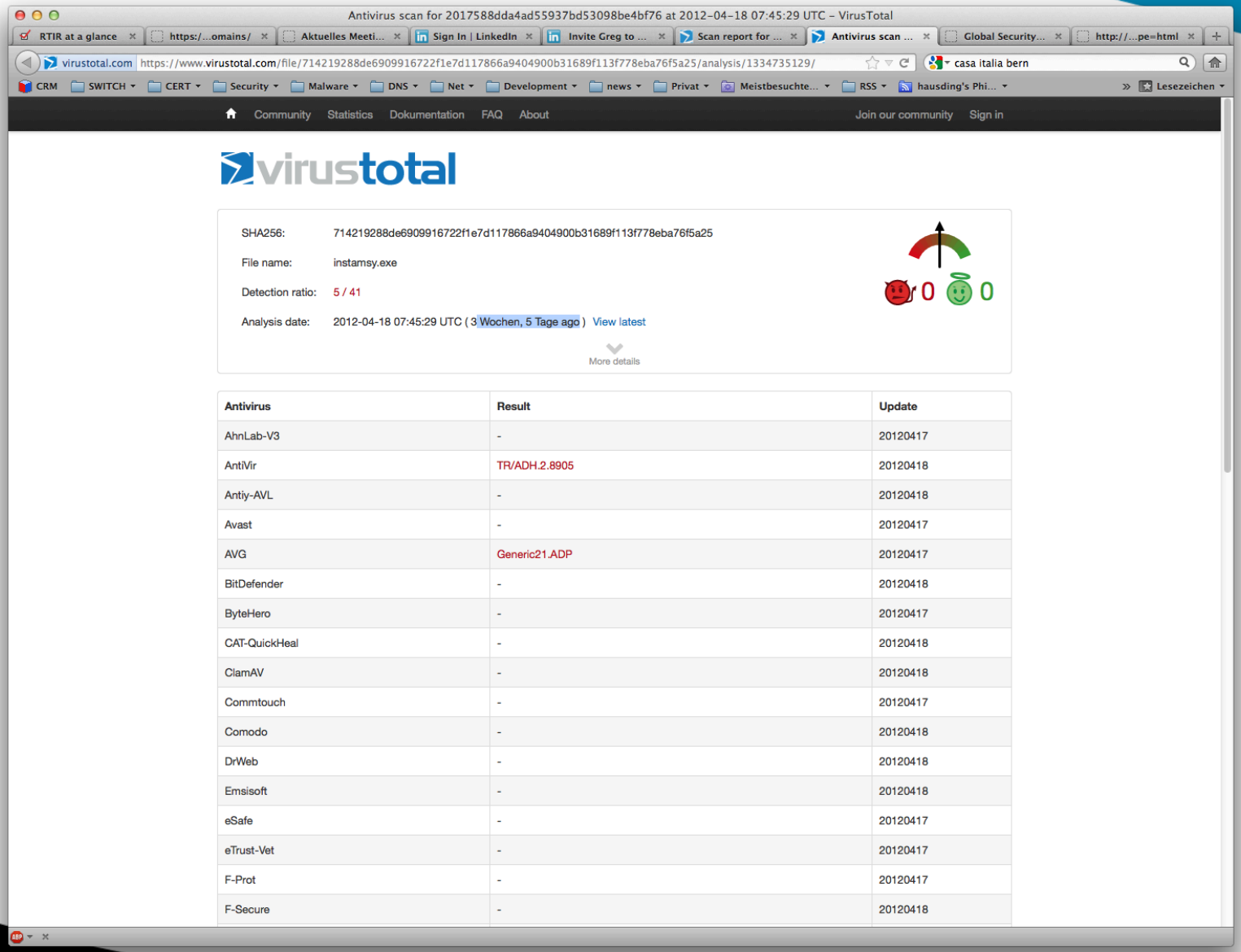
You are viewing Average Insecure Programs **for: World > Europe > Switzerland**

Click on the map to view in depth details for continents and certain countries.



Data Table for: World > Europe > Switzerland

Name	31 days ago	7 days ago	1 day ago	1 hour ago	Now
1. Sankt Gallen	(0) 4	(0) 4	(0) 4	(0) 4	4
2. Zurich	(-2) 5	(-2) 5	(0) 3	(0) 3	3
3. Zug	(-1) 4	(0) 3	(0) 3	(0) 3	3
4. Valais	(-1) 4	(-1) 4	(0) 3	(0) 3	3



Antivirus	Result	Update
AhnLab-V3	-	20120417
AntiVir	TR/ADH.2.8905	20120418
Antiy-AVL	-	20120418
Avast	-	20120417
AVG	Generic21.ADP	20120417
BitDefender	-	20120418
ByteHero	-	20120417
CAT-QuickHeal	-	20120418
ClamAV	-	20120418
Commtouch	-	20120417
Comodo	-	20120418
DrWeb	-	20120418
Emsisoft	-	20120418
eSafe	-	20120417
eTrust-Vet	-	20120417
F-Prot	-	20120417
F-Secure	-	20120418

Removing Drive-By-Code

- SWITCH operates the CC-TLD for .ch
- SWITCH runs a CERT with 10 security professionals
- Legal basis for suspending „malicious“ domains
- Program started November 2010

Cleaning Drive-By-Websites

- Information about malicious URLs
- Verify drive-by-code
- Notify owner/tech-c & hoster
- Remove NS if drive-by-code is not removed after 1 day
- Deblock after 5 days

Legal basis

For **malware-distributing** and **phishing** websites the registry can:

- Suspend the domain-name for 5 working days
- Suspend for 30 days with approval of accredited organization
- A court order is required after 30 days

http://www.admin.ch/ch/d/sr/784_104/a14bist.html

Fighting malware in Switzerland

SWITCH
Serving Swiss Universities

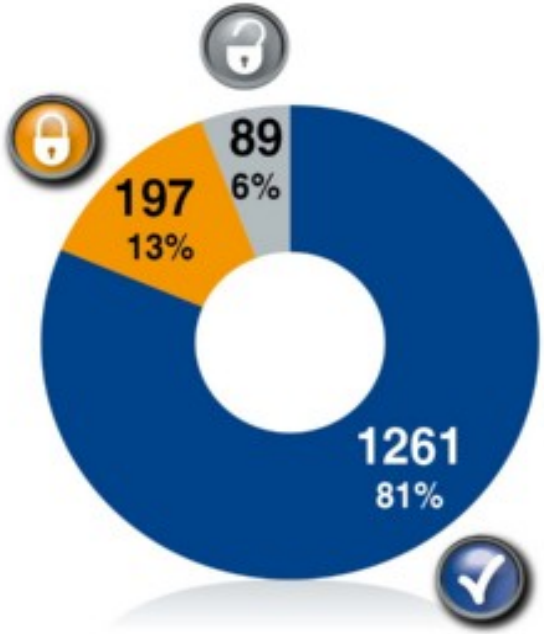
Websites spreading malware in 2011

Cleaned without blocking

Blocked and cleaned

Deblocked without cleaning

Total 2011

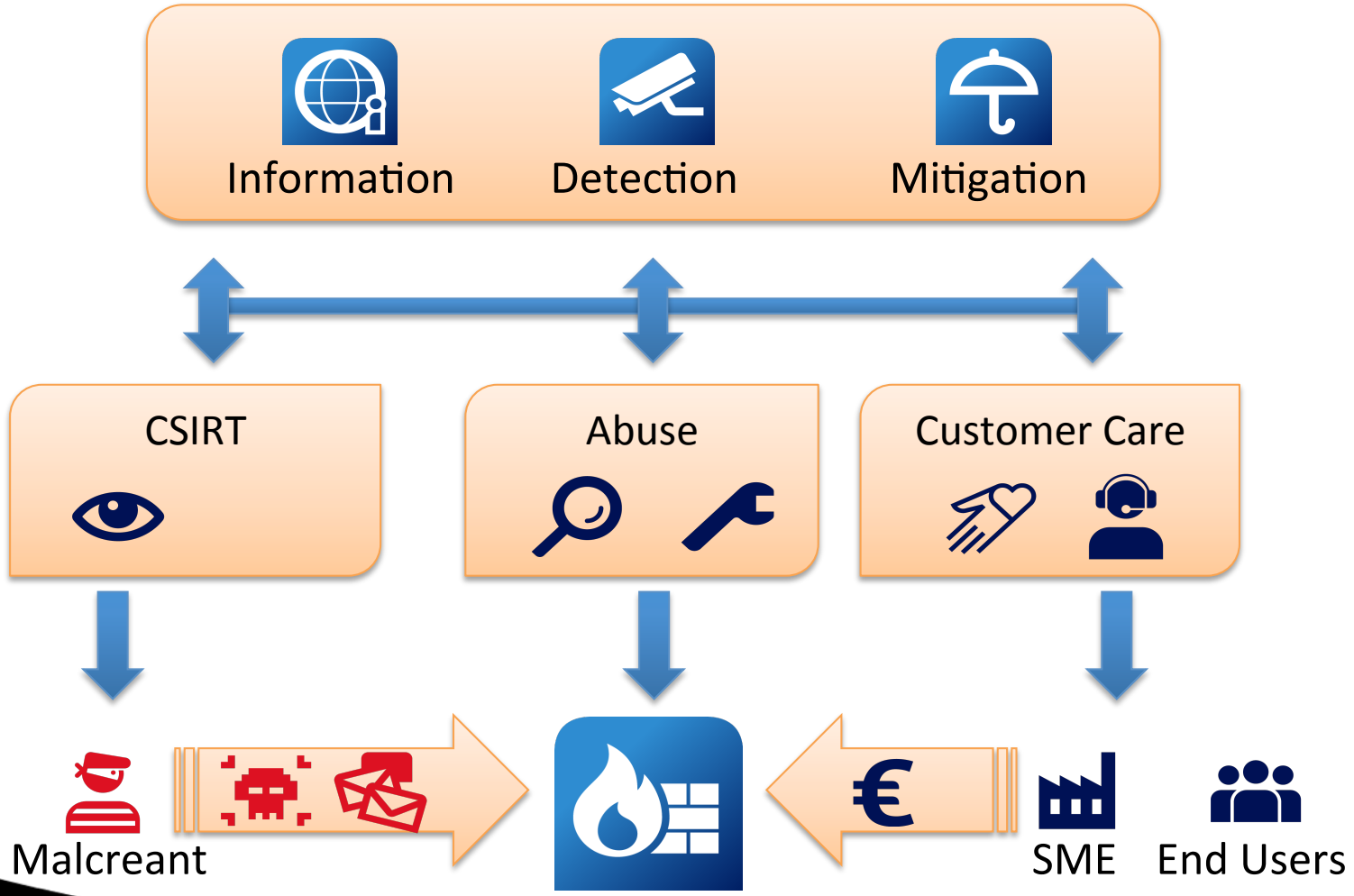


Source: SWITCH

sda

The ISP‘s Part of the Game

Detecting & Cleaning Infections



How to detect infected customers?

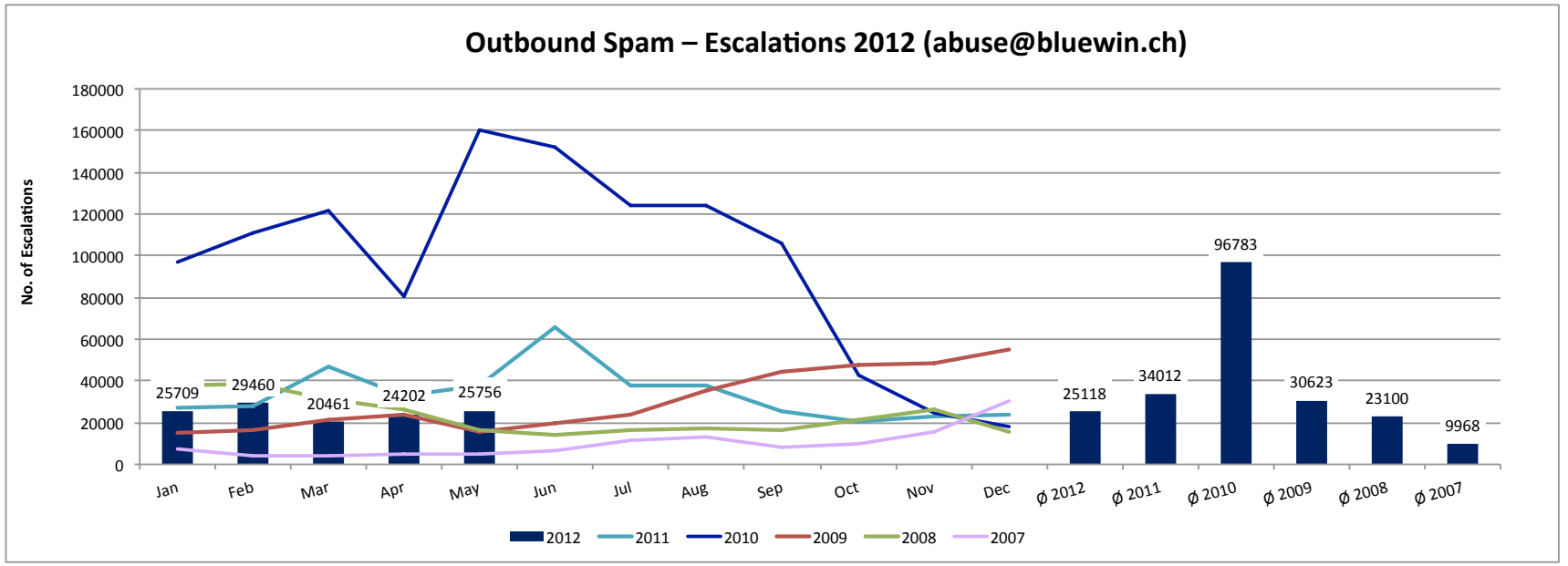
1. Reports from third parties
2. Network Antispam Filter
3. Mail Platform
4. Honeypots / Spamtraps
5. DNS Abuse Monitoring

1) Abuse Reports

- **Feedback Loops**
  - abuse.ch
  - abusix.org
  - aol.com
  - blocklist.de
  - clean-mx.de
  - comcast.com
  - hotmail.com / live.com
  - junkmail.com
  - shadowserver.org
  - spamcop.net
  - trendmicro.com

- **Other Reporters**
  - Customer Feedback: spamreport@bluewin.ch
  - SWITCH
  - MELANI
  - Team Cymru

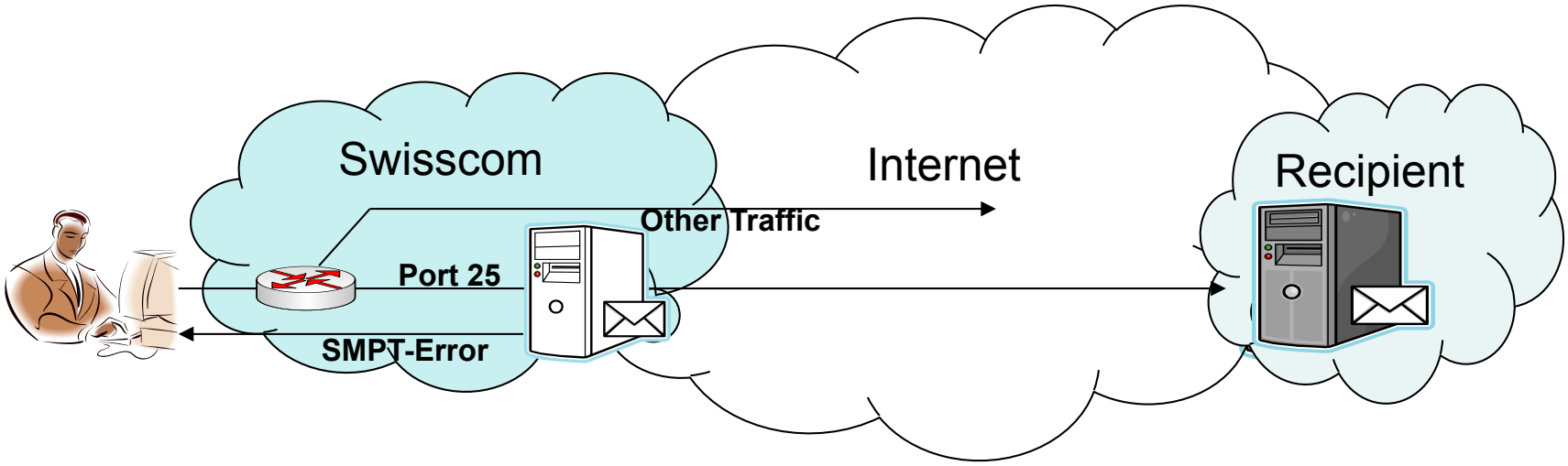
Abuse Escalations



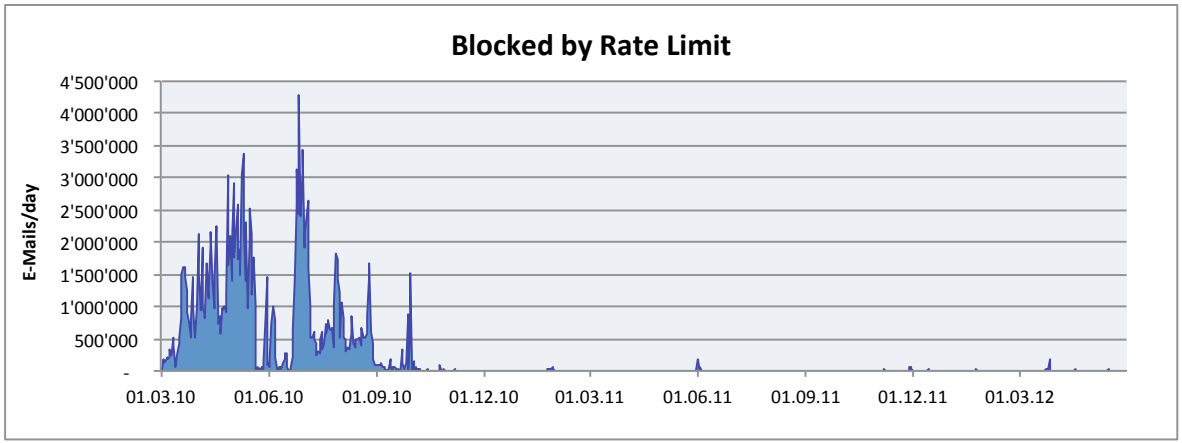
In 2010, there was a maximum of spam escalations.
After the botnet takedowns and introducing Network Antispam, the curve went down.

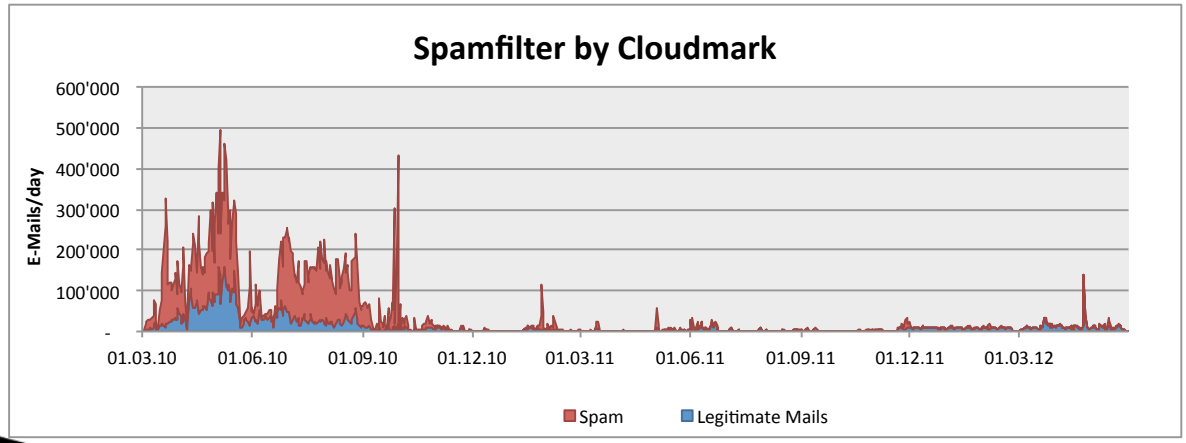
2) Network Antispam Filter

- Layer 4 redirect of port 25 (SMTP) to a dedicated mail platform with AV/spam filters
- Default setting is ‘on’, but individual per customer



Network Antispam Filter





Up to 4 millions spam mails per day blocked.

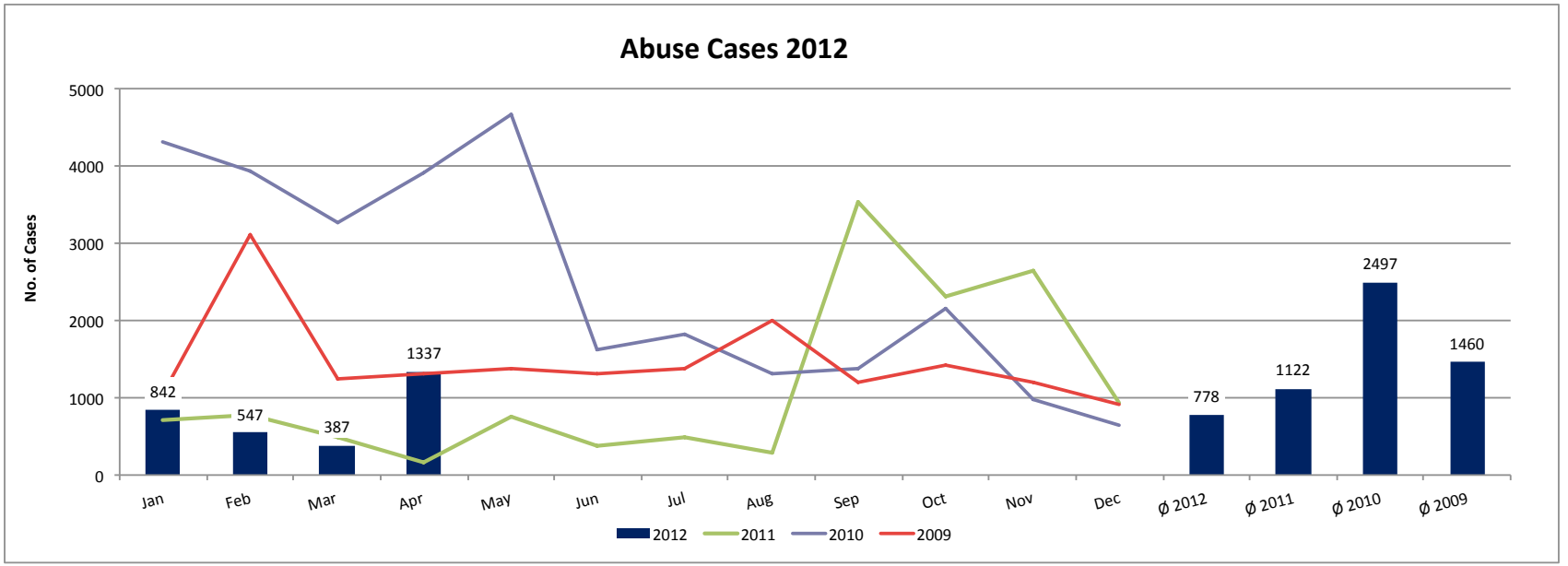
98% of all outgoing e-mails were spam!

...and then it became calm ☺

3) Bluewin Mail Platform

- Webmail Abuse
- SMTP-Auth Abuse
- SMS-Box Abuse

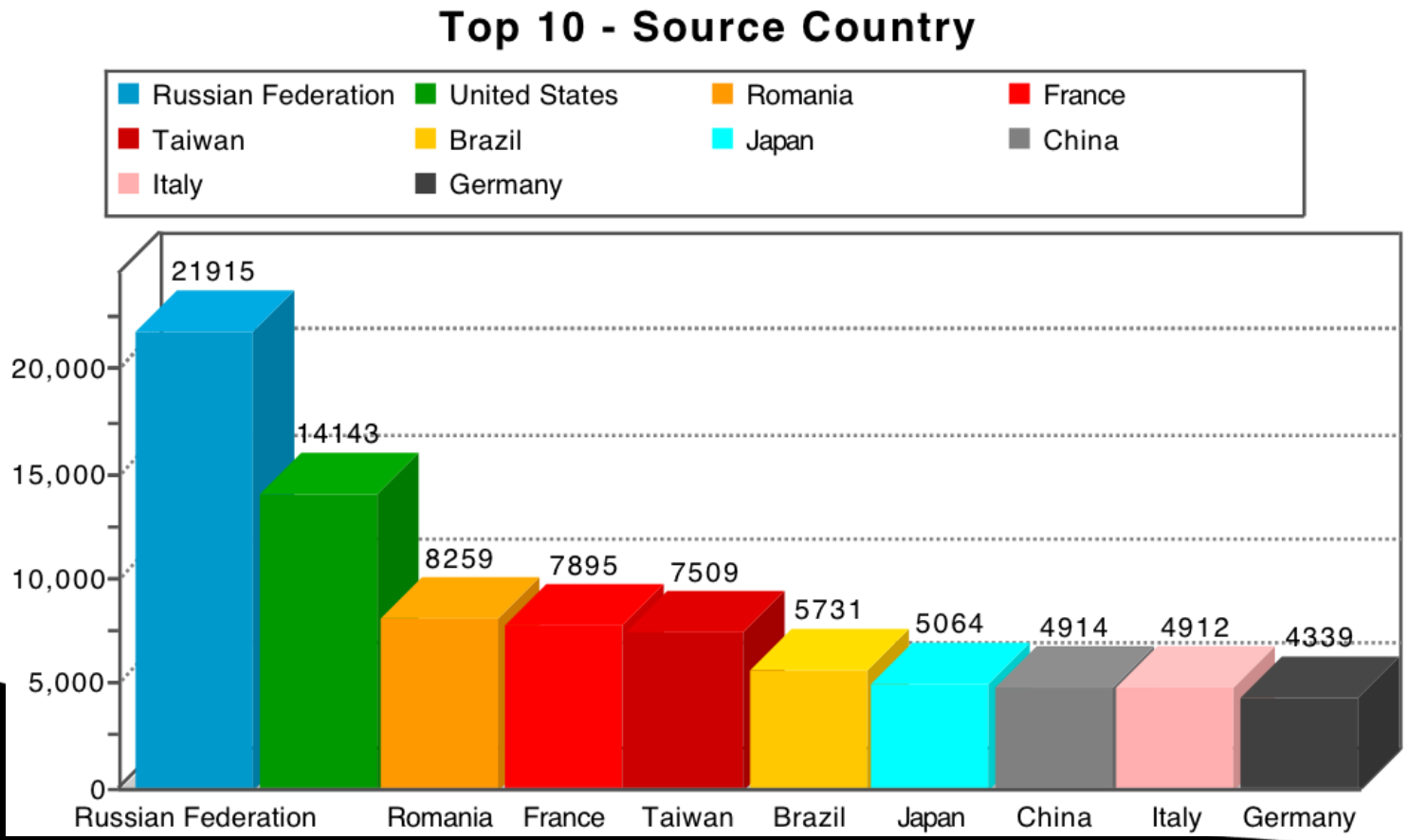
Abuse Cases



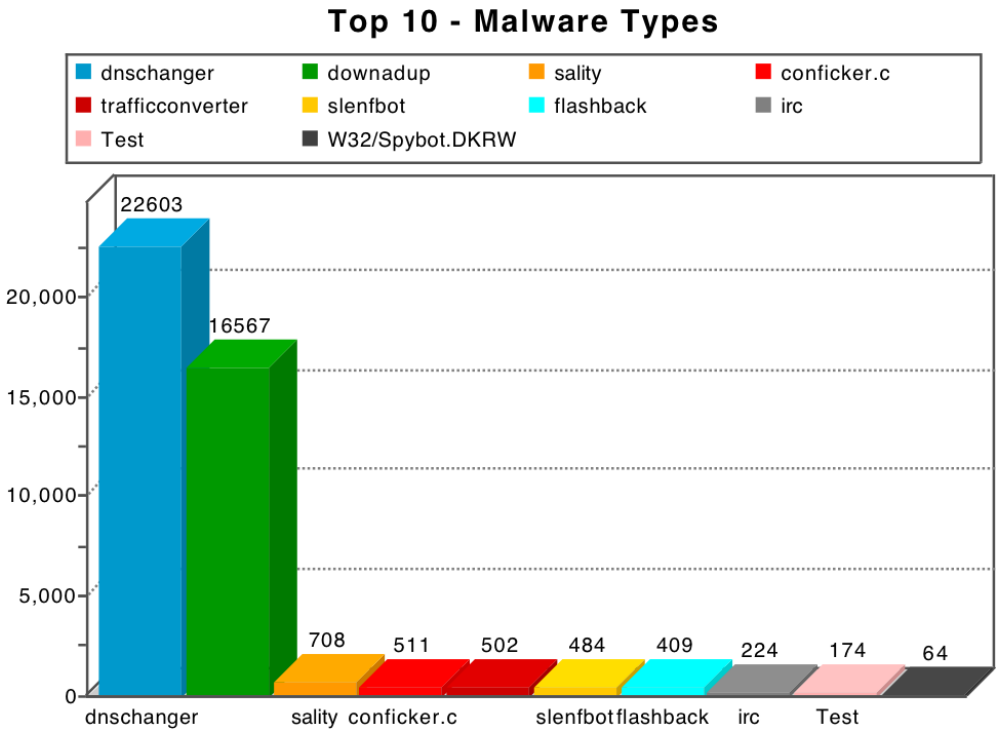
Since 2010 declining number of abuse cases.

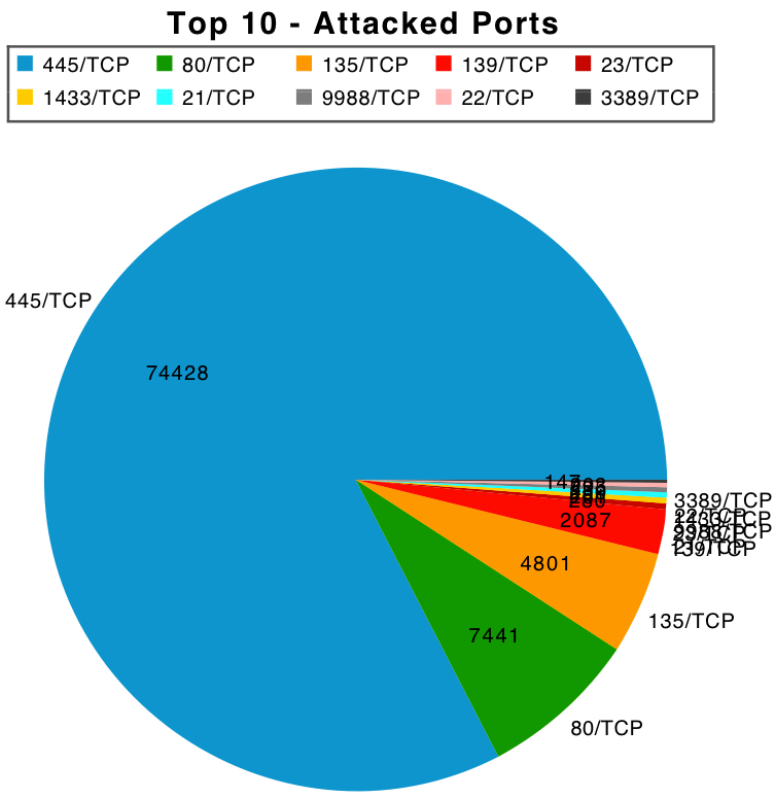
4) Honeynet

- Shadowserver (shadowserver.org)
- Dionaea (dionaea.carnivore.it)



Honeynet


Top 10 - Malware Types
dnschanger
downadup
sality
conficker.c
trafficconverter
slenfbot
flashback
irc
Test
W32/Spybot.DKRW
22603
16567
708
511
502
484
409
224
174
64
20,000
15,000
10,000
5,000
0
dnschanger
sality
conficker.c
slenfbot
flashback
irc
Test


Top 10 - Attacked Ports
445/TCP
80/TCP
135/TCP
139/TCP
23/TCP
1433/TCP
21/TCP
9988/TCP
22/TCP
3389/TCP
445/TCP
74428
3389/TCP
2087
4801
135/TCP
7441
80/TCP

5) DNS Abuse Monitoring

- DNS Query Log Analysis
- Customer DNS

TimeStamp	Count(Distinct Attacke...
1 May 2012 00:00:00 ...	31031
30 Apr 2012 00:00:00...	30482
29 Apr 2012 00:00:00...	33635
28 Apr 2012 00:00:00...	27438
27 Apr 2012 00:00:00...	26012
26 Apr 2012 00:00:00...	26719
25 Apr 2012 00:00:00...	27879
24 Apr 2012 00:00:00...	29474
23 Apr 2012 00:00:00...	30229
22 Apr 2012 00:00:00...	38884
21 Apr 2012 00:00:00...	34310
20 Apr 2012 00:00:00...	18057

- About 60’000 queries per second
- 30 k infected customers of 1.6 mio (1.875%)

Cleaning

1. Walled Garden / Sandbox
2. Customer Information

Victims of the Criminals

Escalation or our own monitoring:

- Internet-Account put into Quarantine (Sandbox/Walled Garden)
- Customer information via e-mail, webpage
- Customer solves the problems and unlocks his account by himself or Customer Care

Sandbox – 3 steps

swisscom

DE | FR | IT | EN

Dear Swisscom Customer,

Unwelcome e-mails (spam) were sent out via your Internet connection, which is most likely due to a virus, or viruses on your computer. This malicious programs damage your computer and the Internet without you even noticing it.

Your Internet access has therefore been temporarily blocked.
Please carry out the following two steps so that complete access to the Internet can be restored:

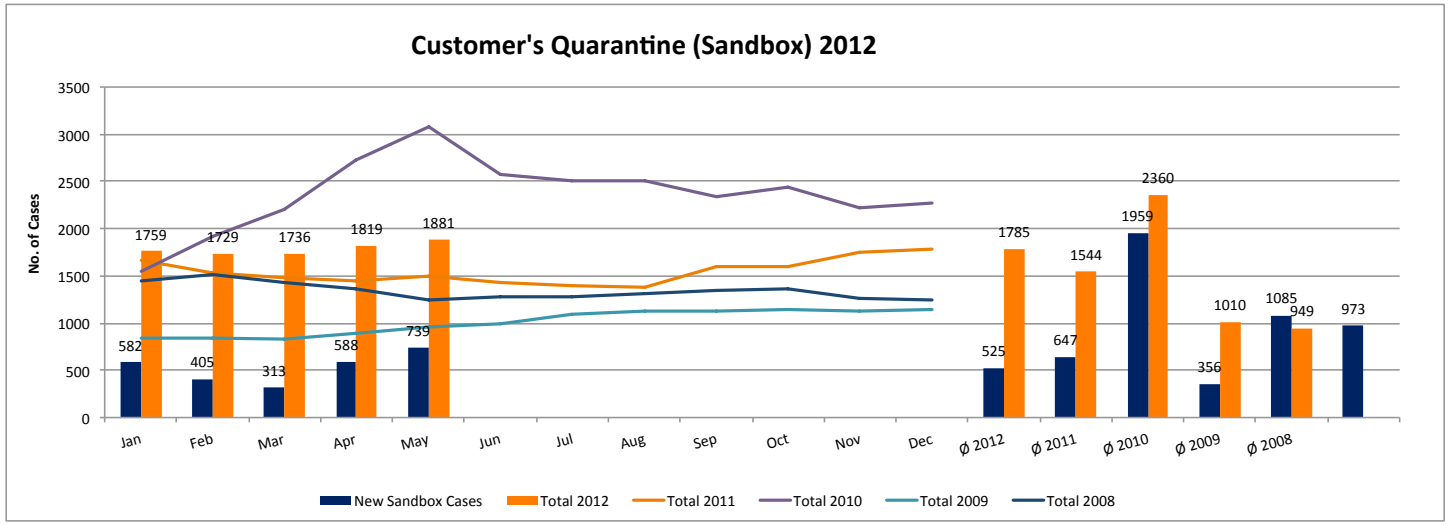
1. **Run the Online Virus Checker.**
   The Online Virus Checker scans your computer for malicious software and removes it.
2. **After that, have your Internet access activated.**
   Once you have confirmed that your computer has been checked for viruses, your Internet access will be reactivated.

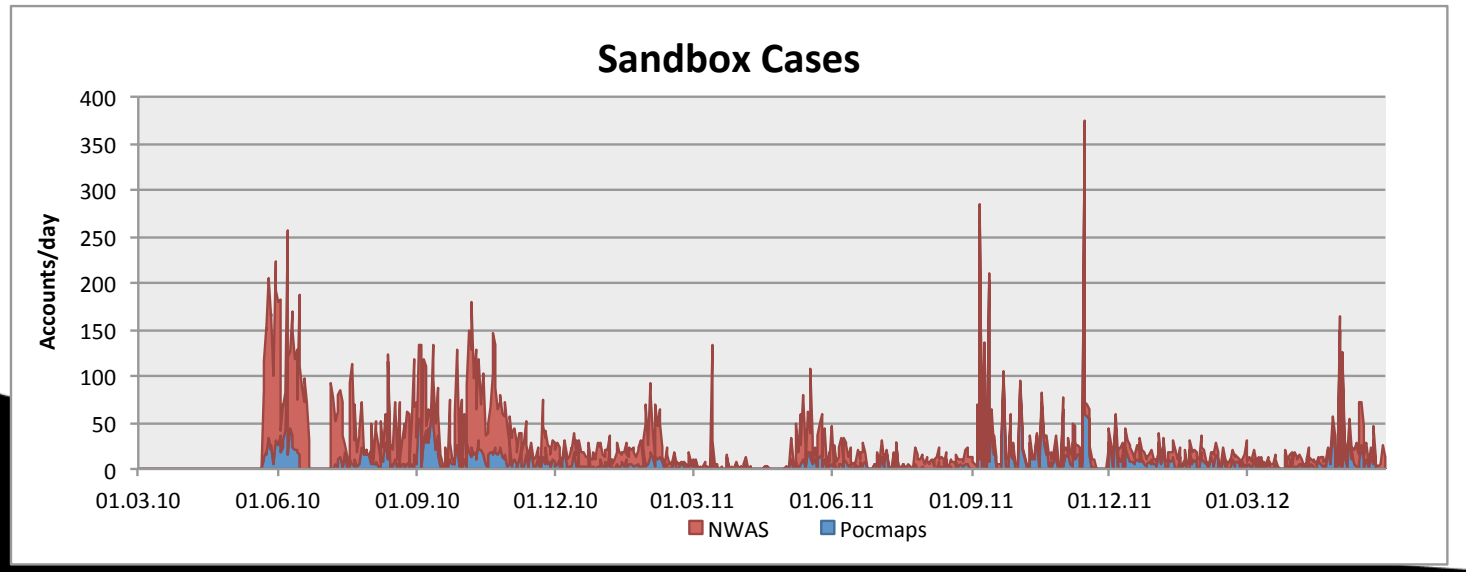
Please note:

- You do not have to change anything related to your DSL installation (cables, router). Your Internet access can only be activated by Swisscom.
- Do you operate a mail server on your Internet connection? In that case, please make sure that the mail server cannot be abused by unauthorised persons to send out spam.

Continue to the Online Virus Checker >

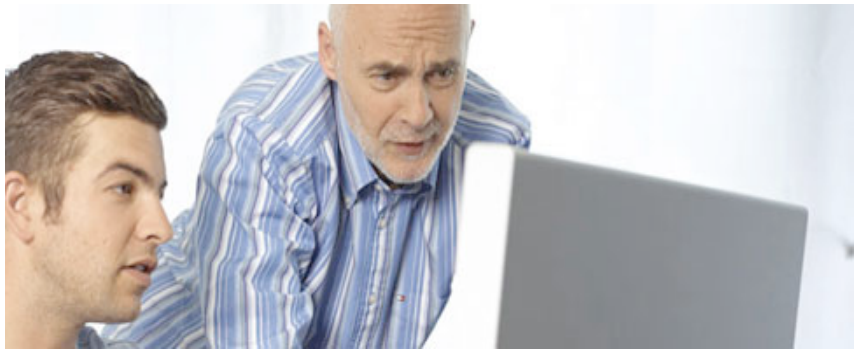
Sandbox Stats





Help for Dummies and others

- www.swisscom.ch/Amico
  - Security Check
  - Virus Cleaning
  - Backup
  - New installation



- Antivirus by F-Secure
- Help pages on www.swisscom.ch

Facts & Figures

- How many cases per month?
  - Ca. 800 abuse cases
  - Ca. 500 sandbox cases

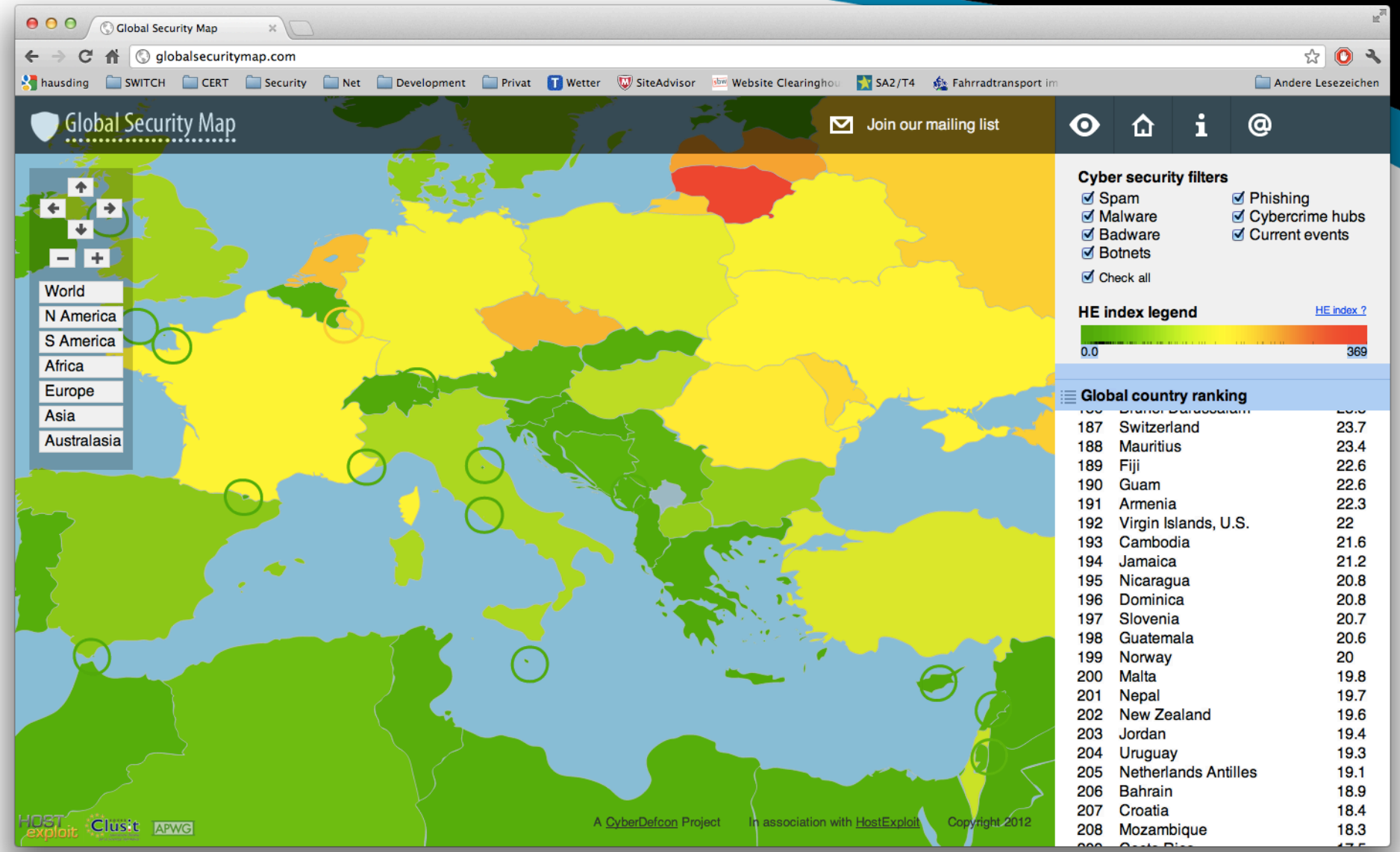
- How many customers are repeaters?
  - 3.5% (up to 10 or more times per day ;-)

- What does it cost?
  - Ca. 25 FTE (Security, Messaging, Customer Care)

Prevention

1. Customer information and awareness
2. DNS/IP Blackholing
3. Antivirus Tool

Results



24th Annual FIRST Conference
MALTA
17 - 22 June 2012

How can you support us

- Exchange Data about Clients & URLs
- Get your country malware free too

Thank you!