INTECO

Instituto Nacional
de Tecnologías
de la Comunicación

NATIONAL NETWORK FOR SPAM MONITORING

Juan Díez González

Security Technician - INTECO-CERT

April, 2008

20th Annual FIRST Conference on Computer Security Incident Handling

Summary

INTECO
Instituto Nacional de Tecnologías de la Comunicación

1. **INTECO and INTECO-CERT**
2. **Spam Monitoring Network**
    1. Sensors Network in Spain
    2. Spam Network description
        1. Client side
        2. Server side
        3. Portal side
    3. Spam Web site
    4. Problems found

Instituto Nacional de Tecnologías de la Comunicación

The National Communications Technology Institute

- ✓ Promoted by the Ministry of Industry, Tourism and Trade,
- ✓ Platform for the development of the Knowledge Society
- ✓ **Foundation**: projects in the innovation and technology area.

INTECO

OBJECTIVES

- ✓ Convergence of the Spanish and European Information Society
- ✓ Promotion of regional development creating a high innovation "Cluster-TIC“
- ✓ Create communications solutions for companies and individuals.
- ✓ Consolidate as the main Spanish centre of innovative and reference programs and projects.

INTECO
Instituto Nacional de Tecnologías de la Comunicación

INTECO Security programs

e-trust

- Establish the bases for the coordination of different public initiatives in the information security area
- Promoting applied research and specialised training activities in the TIC security area.
- Become the national IT Security Reference Centre .

Services to SME's

Services to Citizens

Information Security Observatory

INTECO-CERT, Computer Emergency Response Team for SMEs and Citizens

Security Technologies Show-Room for SMEs

INTECO
Instituto Nacional de Tecnologías de la Comunicación

INTECO-CERT. Objectives

- Increase the level of awareness in the security area and enforce the usage of security solutions for SMEs and homes.
- Provide provision of reactive and preventive services and procedures for security incidents.
- Present training facilities on technology and information security.
- Provide best practices, recommendations and advice.
- Show available security solutions for SMEs and citizens

INTECO-CERT Services

INTECO
Instituto Nacional de Tecnologías de la Comunicación

- Information Services:
  - Subscription to security reports, alerts
  - News, events
  - Online virus warnings, software vulnerabilities, **spam**.
- Training Services: Tutorials, manuals, online courses.
- Protection Services: free tools, software updates.
- Response and Support Services:
  - Security Incidents management.
  - Malware infections.
  - Phishing attacks.
  - Legal support.
  - Security forums.

SPAM monitoring network

INTECO
Instituto Nacional de Tecnologías de la Comunicación

Objectives

- To obtain real-time information about SPAM to give a general view about how spam affects organizations and citizens
- To compare this information with other available sources of information on malware
- To share this information with other interested organizations

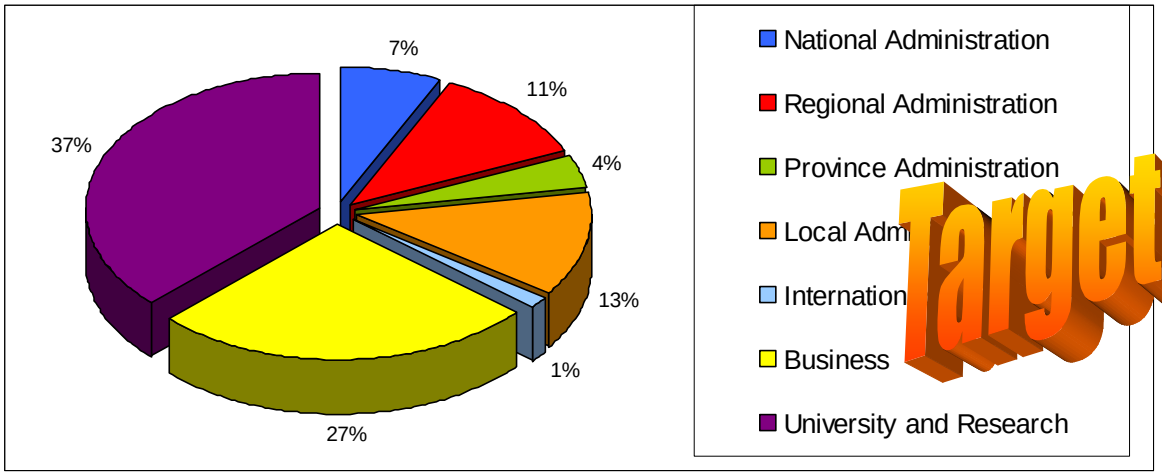
How?

INTECO's Sensor Network

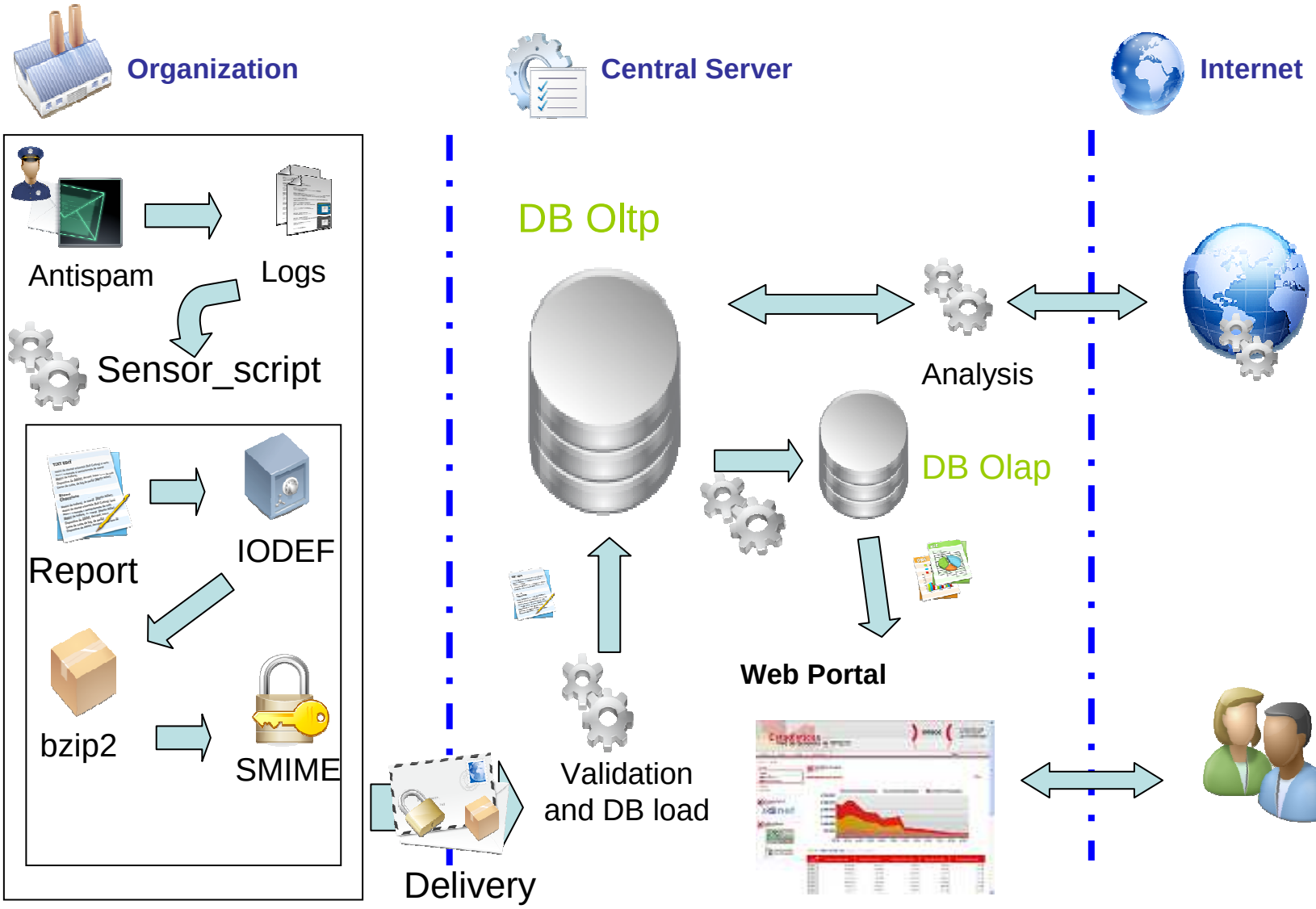
INTECO
Instituto Nacional de Tecnologías de la Comunicación

Sensors Network in Spain

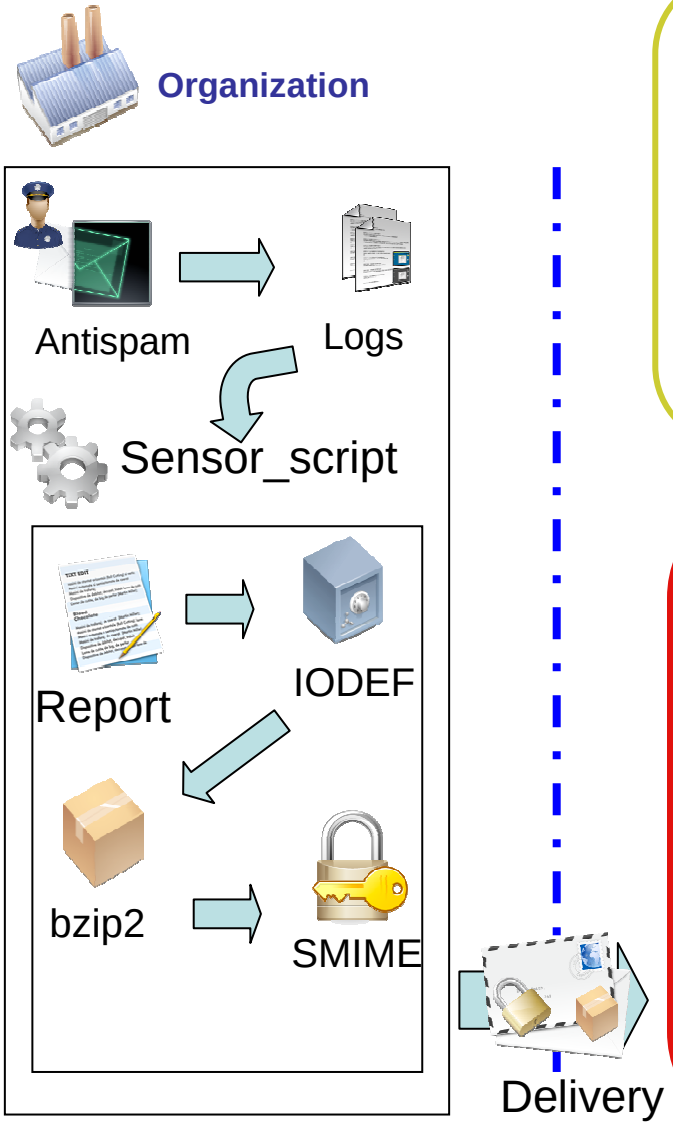
- More than **150** organizations → more than 100 **million** real e-mails processed per day.
- More than 5 years used to get **virus detection** information
- **2,26%** infected e-mails detected in almost 30 billion ones analyzed



Functional Diagram



Sensor Script



- Written in Perl.
- Tailored for every organization
- Spam detection Report using:
  - IODEF format
  - Zip or Bzip2 compression
  - SMIME delivery

- Report Contains:
  - Report Info. Date, server …
  - Totals Section
    - Per hour
    - Per method
  - Email origin IP for every email
  - Detection method used for every IP

Sensor Script

Report

```
Organizacion:                          Nombre_Organización
ASN:                                   Número_ASN
Sensor:                                Nombre del Sensor
Fecha:                               AAAA-MM-DDTHH:MM:SS±UMT
Tipo Origen:                           postfix
Version:                               3.0
Fecha inicio:                        2007-02-08T11:33:48+01:00
Fecha final:                         2007-02-08T11:35:31+01:00
Numero de relays:                            10
Mensajes Procesados:                         37
Spam Detectado:                              29        78.38
Spam Pasado:                                  0         0.00
Spam Rechazado:                              29       100.00
Spam Declarado:                               0         0.00
Spam por Analisis de Contenido:               0         0.00
Spam por Politica de Conexion:                0         0.00
Spam por otro metodo:                         0         0.00
Metodo                      Detectados  Rechazados        %
-------------------------------------------------------------
Bogofilter                                      25         25       86.21
DSBL                                             4          4       13.79
Horas            Procesados  Detectados  Rechazados  Declarados   Contenido    Conexion       Otros         %
-------------------------------------------------------------------------------------------------------------
2007-02-08T11            37          29          29          -1          -1          -1          -1       78.38
Relay            Procesados  Detectados  Rechazados  Declarados   Contenido    Conexion       Otros
-------------------------------------------------------------------------------------------------
127.0.0.4                25          25          25          -1          -1          -1          -1
127.0.0.2                 4           4           4          -1          -1          -1          -1
83.113.61.243             1           0           0          -1          -1          -1          -1
81.4.161.50               1           0           0          -1          -1          -1          -1
62.42.230.12              1           0           0          -1          -1          -1          -1
61.229.107.225            1           0           0          -1          -1          -1          -1
218.81.159.46             1           0           0          -1          -1          -1          -1
172.18.0.127              1           0           0          -1          -1          -1          -1
202.190.152.140           1           0           0          -1          -1          -1          -1
82.194.72.78              1           0           0          -1          -1          -1          -1
Relay               Metodos
-------------------------------------------------------------
127.0.0.2        DSBL
127.0.0.4        Bogofilter
```

Header

Summary

Ips

Methods

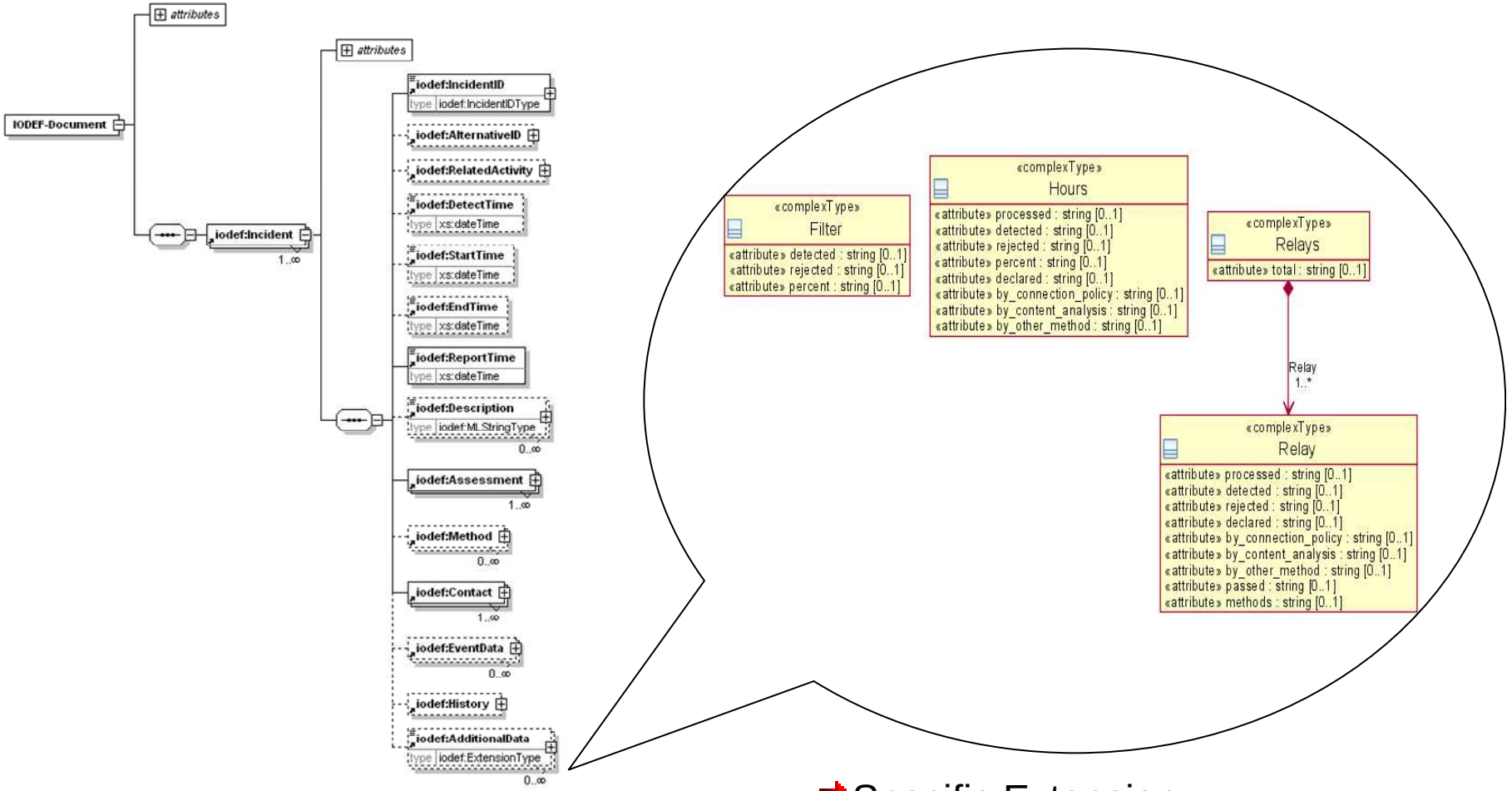
IODEF format

- IODEF (*Incident Object Description Exchange Format*), defines a data representation to exchange security incidents among different CSIRT.
- XML Syntax.
- Contains security incidents information

- Advantages.
- Increased automation in incident data processing, since the resources of security analysts to parse free-form textual documents will be reduced;
- Decreased effort in standardizing similar data (even when highly structured) from different sources;
- Common format on which interoperable tools for incident handling and subsequent analysis can be built, specifically when data comes from multiple constituencies.

INTECO
Instituto Nacional de Tecnologías de la Comunicación

IODEF schema



- Basic Model
- Specific Extension

XML-IODEF spam report

INTECO
Instituto Nacional de Tecnologías de la Comunicación

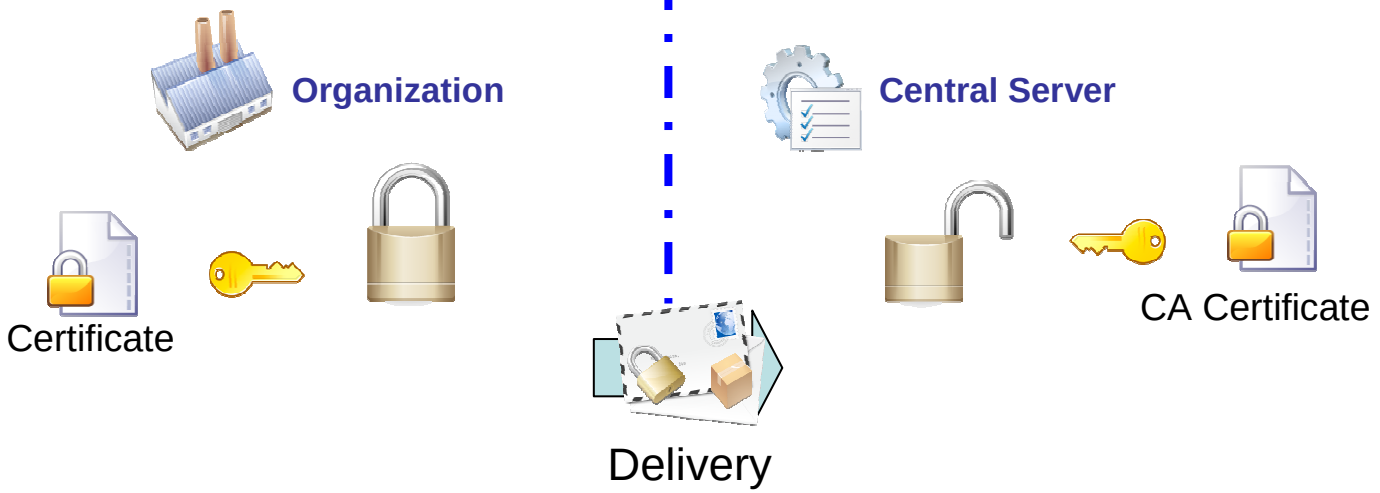
IODEF Report

Spam report

```
<?xml version="1.0" encoding="UTF-8" ?>
<IODEF-Document version="1.00" lang="en" formatid="sanet-2.1"
  xmlns="urn:ietf:params:xml:ns:iodef-1.0">
  <Incident purpose="ext-value" ext-purpose="spam-reporting">
            <IncidentID name="misensor1">2006-01-18T01:59:33+01:00</IncidentID>
            <StartTime>2006-01-18T01:59:02+01:00</StartTime>
            <EndTime>2006-01-18T01:59:33+01:00</EndTime>
            <ReportTime>2006-01-18T00:00:00+01:00</ReportTime>
            <Description>Spam report from Postfix mail server</Description>
            <Assessment>
              <Impact lang="en" severity="low" completion="failed" type="unknown" />
            </Assessment>
            <Contact role="creator" type="organization">
              <ContactName>ejemplo.es</ContactName>
              <Email>pepito@ejemplo.es</Email>
            </Contact>
            <EventData>
              <Method>
                <Reference>
                  <ReferenceName>e-mail</ReferenceName>
                </Reference>
              </Method>
              <Flow>
                <System category="sensor">
                  <Node>
                    <Address category="asn">22</Address>
                    <Location>Madrid-Spain</Location>
                    <NodeRole category="mail" />
                    <Counter type="message" meaning="processed">236</Counter>...
                     <Counter type="message" meaning="by_connection_policy">3</Counter>
                    <Counter type="ext-value" ext-type="percent"
                    meaning="by_connection_policy">100.00</Counter>
                    <Counter type="message" meaning="rejected">44</Counter>
                  </Node>
                </System>
              </Flow>
              <Expectation action="nothing" />
              <AdditionalData dtype="xml">
                <Filter detected="2" rejected="2" percent="66.67">SpamHouse</Filter>
                <Filter detected="1" rejected="1" percent="33.33">NoDamain</Filter>
                <Hours processed="236" detected="3" rejected="3" percent="1.27">2007-02-08T11</Hours>
                <Relays total="223">
                  <Relay processed="4" detected="0" rejected="0" declared="0"> 200.73.246.219</Relay>
                  <Relay processed="4" detected="3" rejected="2" declared="0" by_connection_policy="3"
                   by_content_analysis="0" methods="SpamHouse, SpamCop">72.184.53.128</Relay>
                </Relays>
              </AdditionalData>
            </EventData>
  </Incident>
</IODEF-Document>
```

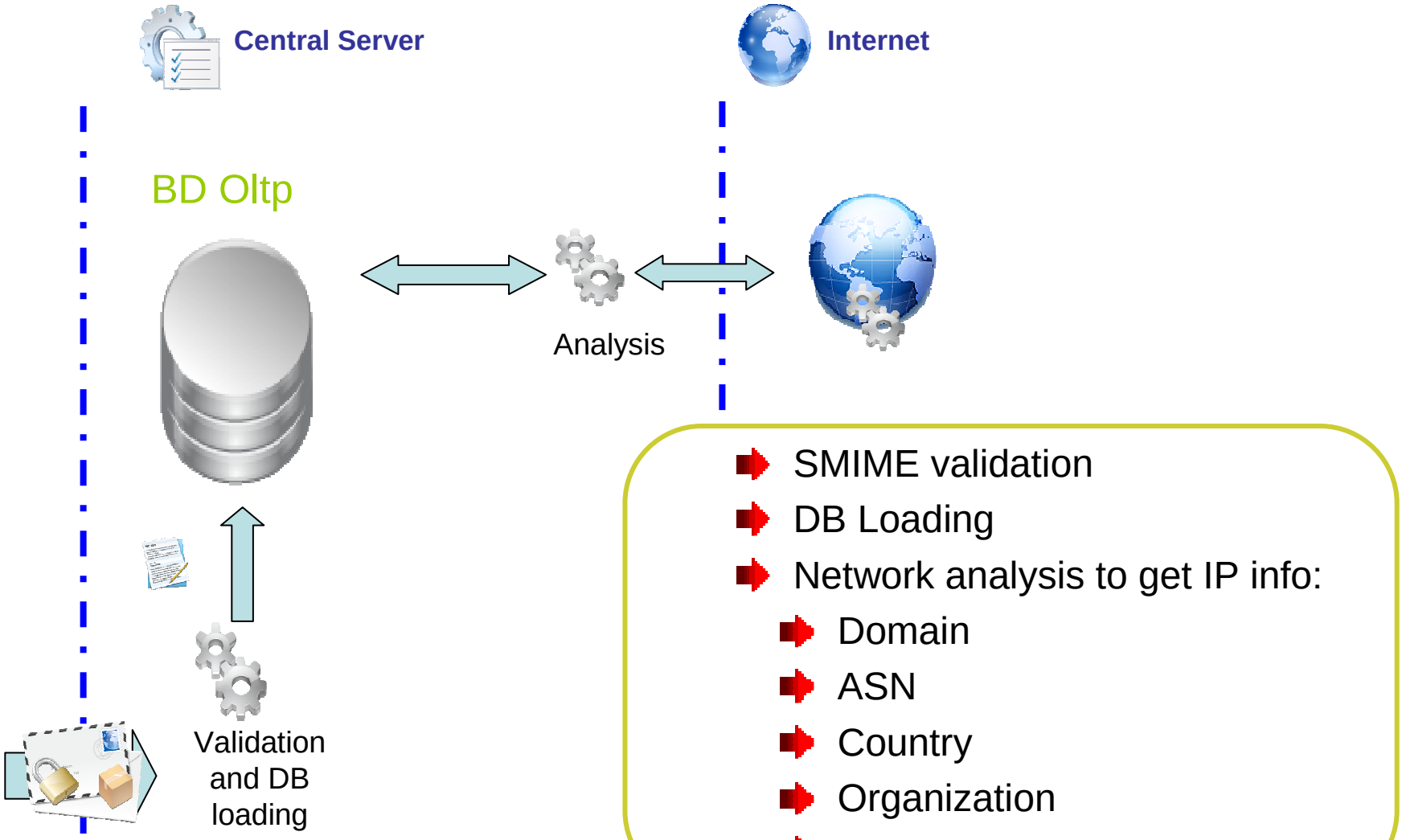
Sensor script

SMIME Delivery



- INTECO-CERT CA certificate used to:
  - Generate one cert per organization
  - Sign every report on SMIME delivery
  - Verify digital signature on the central server reception

Central Server



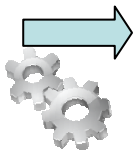
- SMIME validation
- DB Loading
- Network analysis to get IP info:
  - Domain
  - ASN
  - Country
  - Organization
  - …

Central Server

Central Server

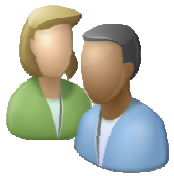
Internet

BD Oltp



BD Olap

Web Portal



- Analytical Environment to
  - Totalize data
  - Aggregate data
- Speed up web queries
- Minimize web response time

Web Components

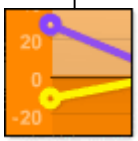
- Powerful CMS (specially 1.5)
- Free (as in freedom) software
- Big supporting community

Spam Statistics Custom Component

- Fast development (using Joomla API)
- Modular for new interface addition (web service?)
- Easily extensible (thanks to OOP)

xajax:

- Fast AJAX development.
- Easy to integrate if server code is modular.
- ☹ Not fully customizable.
- ☹ Not accessible.



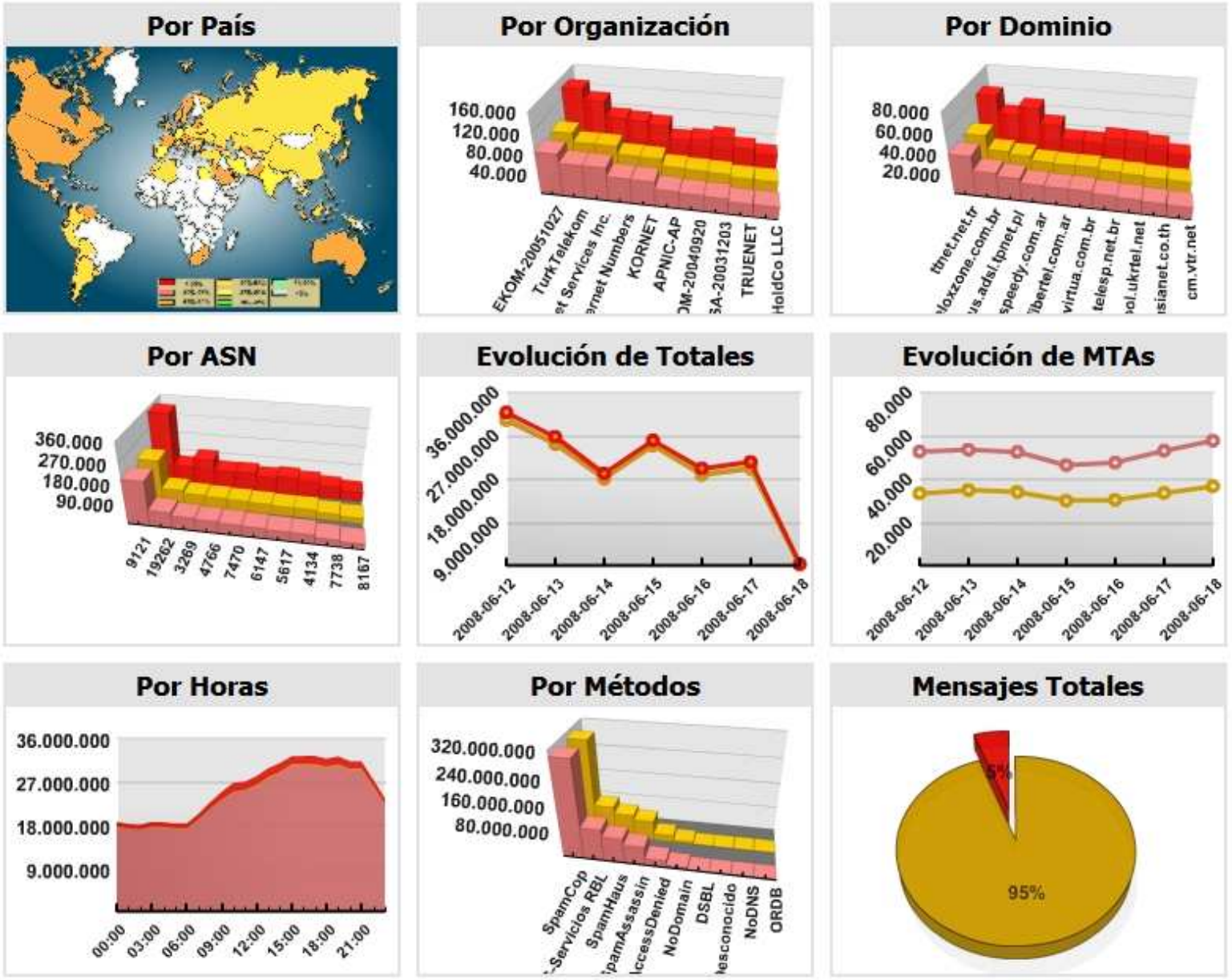
PHP/SWF Charts

PHP/SWF:

- Eye-catching flash charts
- Totally customizable.
- PHP API for easy configuration.
- Not free, but cheap.

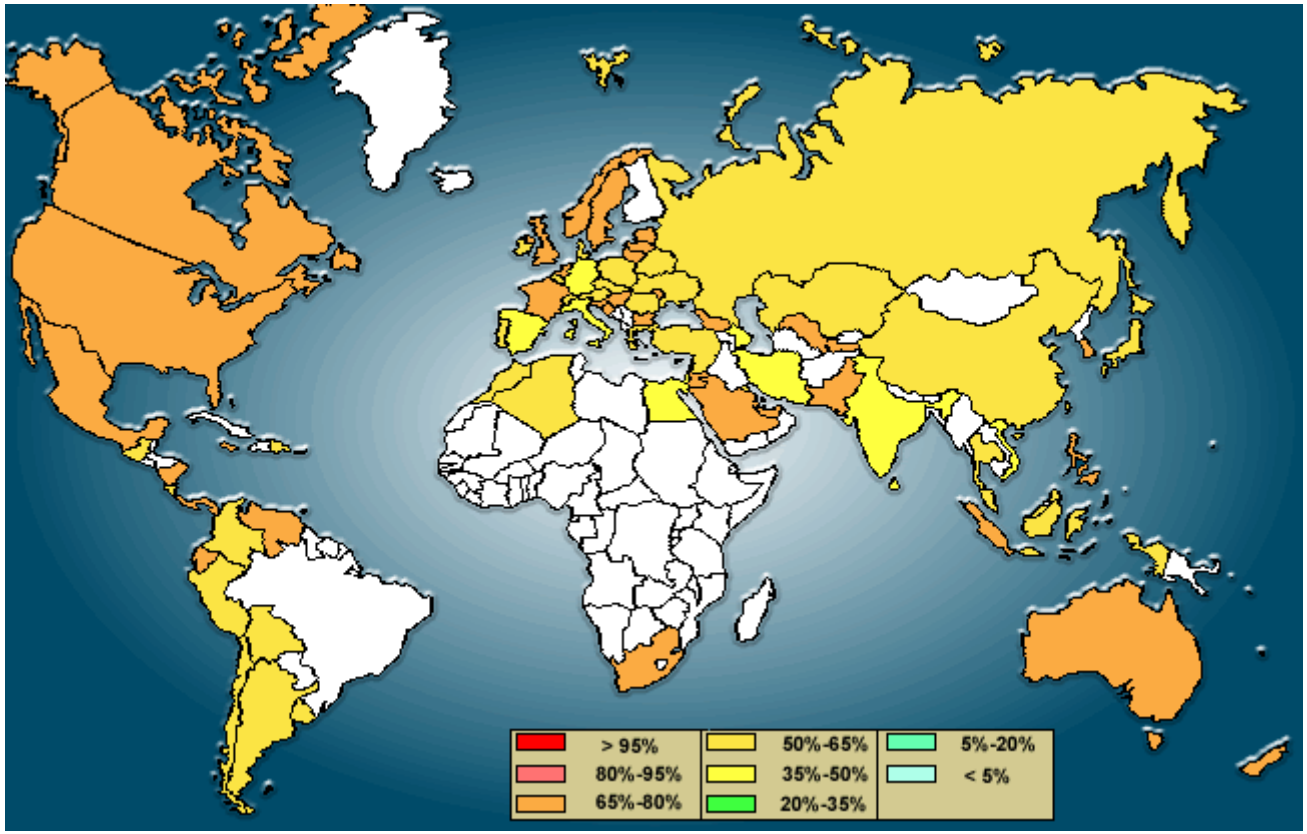
Web Site: https://ersi.inteco.es

INTECO
Instituto Nacional de Tecnologías de la Comunicación

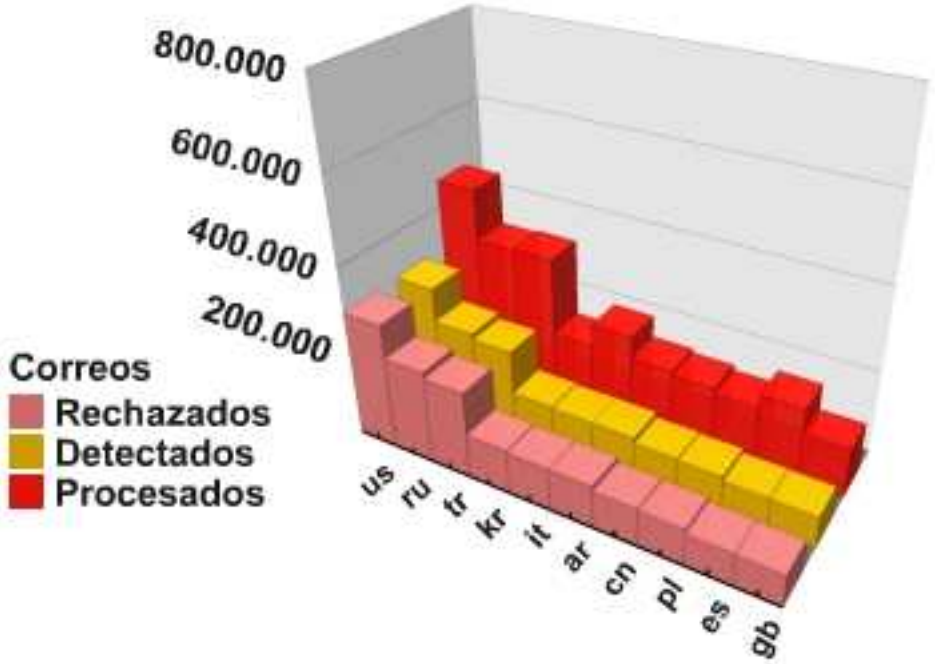


World map: SPAM by COUNTRY

INTECO
Instituto Nacional
de Tecnologías
de la Comunicación



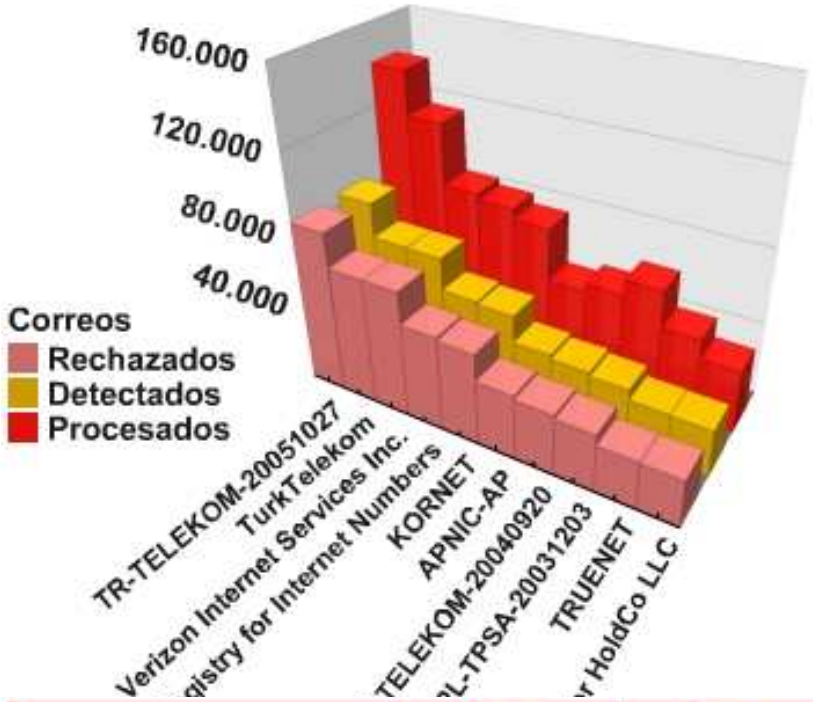
Interactive bar chart: SPAM by COUNTRY



Total de Mensajes Procesados	4.056.400
Total de Spam Detectado	2.401.292
Porcentaje de Spam Detectado	59,2 %
Total de Spam Rechazado	2.401.292
Porcentaje de Spam Rechazado	59,2 %

Código	País	Correos Procesados	Spam Detectado	% Spam Detectado	Spam Rechazado	% Spam Rechazado
us	Estados Unidos de América	460.668	299.020	64,9 %	299.020	64,9 %
ru	Rusia	340.332	219.888	64,6 %	219.888	64,6 %
tr	Turquía	344.723	206.688	60,0 %	206.688	60,0 %
kr	Corea del Sur	162.292	105.668	65,1 %	105.668	65,1 %
it	Italia	214.926	102.372	47,6 %	102.372	47,6 %
ar	Argentina	163.450	101.726	62,2 %	101.726	62,2 %
cn	República Popular China	154.770	90.236	58,3 %	90.236	58,3 %
pl	Polonia	143.525	87.146	60,7 %	87.146	60,7 %
es	España	175.760	77.020	43,8 %	77.020	43,8 %
gb	Reino Unido (en desuso)	114.427	75.775	66,2 %	75.775	66,2 %

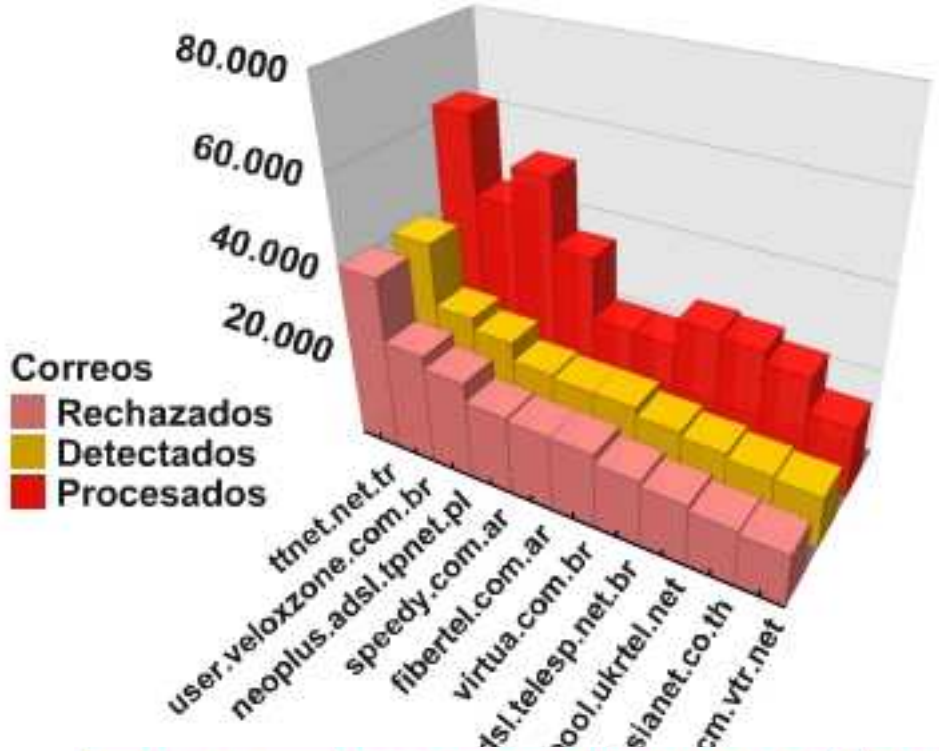
Interactive bar chart: SPAM by ORGANIZATION



Total de Mensajes Procesados	4.060.269
Total de Spam Detectado	2.403.236
Porcentaje de Spam Detectado	59,2 %
Total de Spam Rechazado	2.403.236
Porcentaje de Spam Rechazado	59,2 %

Organización	Correos Procesados	Spam Detectado	% Spam Detectado	Spam Rechazado	% Spam Rechazado
TR-TELEKOM-20051027	140.551	85.808	61,1 %	85.808	61,1 %
TurkTelekom	118.061	67.890	57,5 %	67.890	57,5 %
Verizon Internet Services Inc.	86.487	67.775	78,4 %	67.775	78,4 %
American Registry for Internet Numbers	83.355	50.710	60,8 %	50.710	60,8 %
KORNET	78.218	49.324	63,1 %	49.324	63,1 %
APNIC-AP	50.637	34.980	69,1 %	34.980	69,1 %
TR-TELEKOM-20040920	55.095	33.126	60,1 %	33.126	60,1 %
PL-TPSA-20031203	63.340	31.214	49,3 %	31.214	49,3 %
TRUENET	44.043	25.675	58,3 %	25.675	58,3 %
Road Runner HoldCo LLC	33.901	25.468	75,1 %	25.468	75,1 %

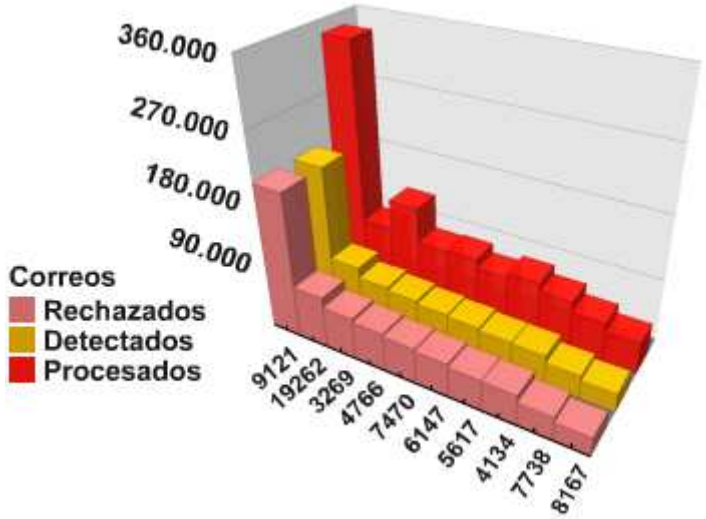
Interactive bar chart: SPAM by DOMAIN



Total de Mensajes Procesados	2.569.862
Total de Spam Detectado	1.524.873
Porcentaje de Spam Detectado	59,3 %
Total de Spam Rechazado	1.524.873
Porcentaje de Spam Rechazado	59,3 %

Dominio	Correos Procesados	Spam Detectado	% Spam Detectado	Spam Rechazado	% Spam Rechazado
ttnet.net.tr	63.120	40.570	64,3 %	40.570	64,3 %
user.veloxzone.com.br	44.677	25.837	57,8 %	25.837	57,8 %
neoplus.adsl.tpnet.pl	53.467	23.003	43,0 %	23.003	43,0 %
speedy.com.ar	37.402	18.515	49,5 %	18.515	49,5 %
fibertel.com.ar	22.979	17.780	77,4 %	17.780	77,4 %
virtua.com.br	22.779	17.768	78,0 %	17.768	78,0 %
dsl.telesp.net.br	28.745	15.608	54,3 %	15.608	54,3 %
pool.ukrtel.net	27.864	14.400	51,7 %	14.400	51,7 %
revip2.asianet.co.th	24.990	13.125	52,5 %	13.125	52,5 %
cm.vtr.net	16.702	12.360	74,0 %	12.360	74,0 %

Interactive bar chart: SPAM by ASN

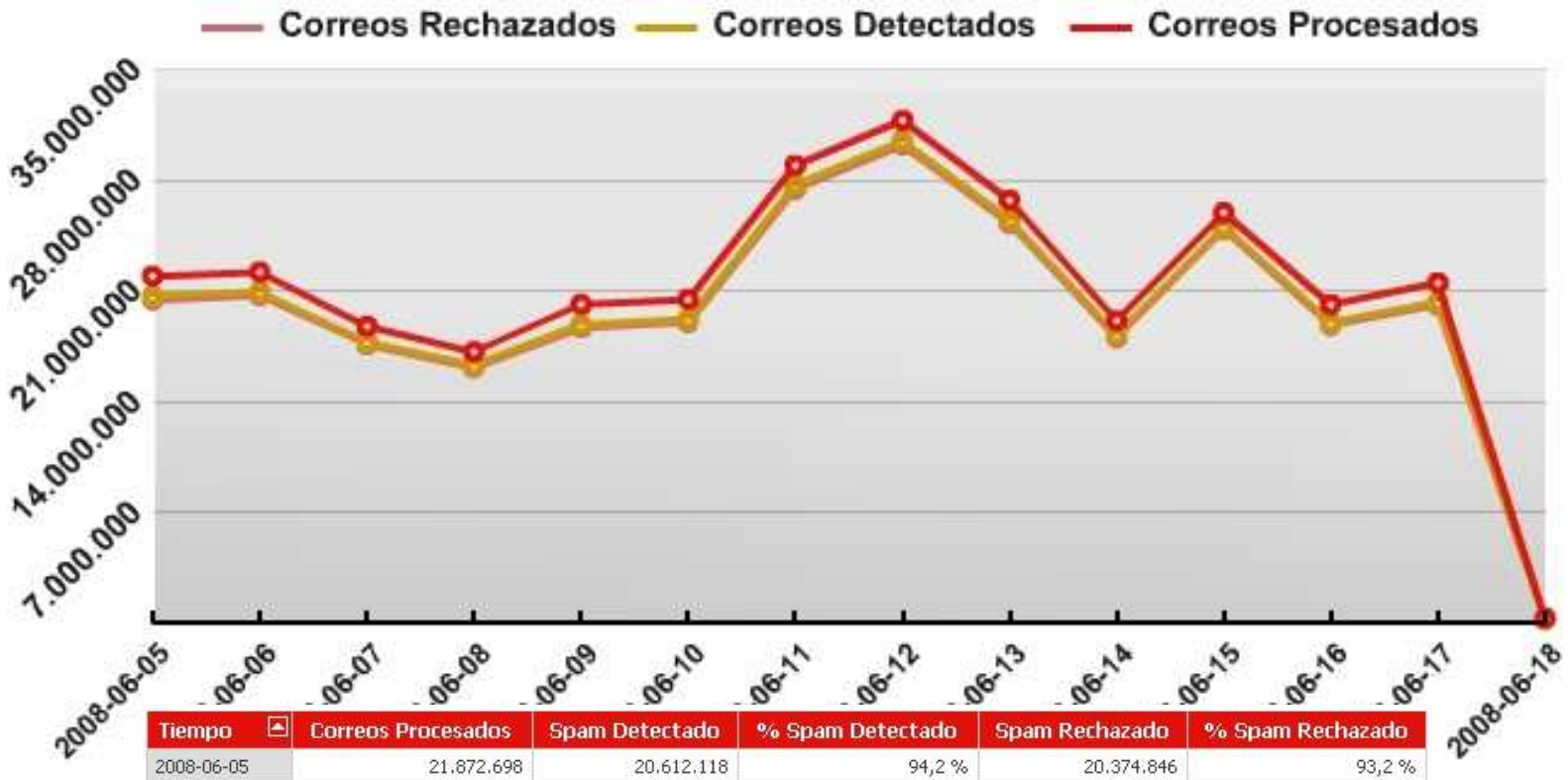


Total de Mensajes Procesados	4.356.601
Total de Spam Detectado	2.571.799
Porcentaje de Spam Detectado	59,0 %
Total de Spam Rechazado	2.571.799
Porcentaje de Spam Rechazado	59,0 %

Número	Descripción	Correos Procesados	Spam Detectado	% Spam Detectado	Spam Rechazado	% Spam Rechazado
9.121	TTNET TTnet Autonomous System	342.430	204.836	59,8 %	204.836	59,8 %
19.262	VZGNI-TRANSIT - Verizon Internet Services Inc.	93.915	73.627	78,4 %	73.627	78,4 %
3.269	ASN-IBSNAZ TELECOM ITALIA	136.122	59.641	43,8 %	59.641	43,8 %
4.766	KIXS-AS-KR Korea Telecom	86.385	55.136	63,8 %	55.136	63,8 %
7.470	ASIAINFO-AS-AP ASIA INFONET Co.,Ltd.	88.543	50.722	57,3 %	50.722	57,3 %
6.147	Telefonica del Peru S.A.A.	75.402	47.855	63,5 %	47.855	63,5 %
5.617	TPNET Polish Telecom_s commercial IP network	83.836	43.908	52,4 %	43.908	52,4 %
4.134	CHINANET-BACKBONE No.31,Jin-rong Street	71.717	42.910	59,8 %	42.910	59,8 %
7.738	Telecomunicacoes da Bahia S.A.	56.485	32.724	57,9 %	32.724	57,9 %
8.167	TELESC - Telecomunicacoes de Santa Catarina SA	44.040	26.269	59,6 %	26.269	59,6 %

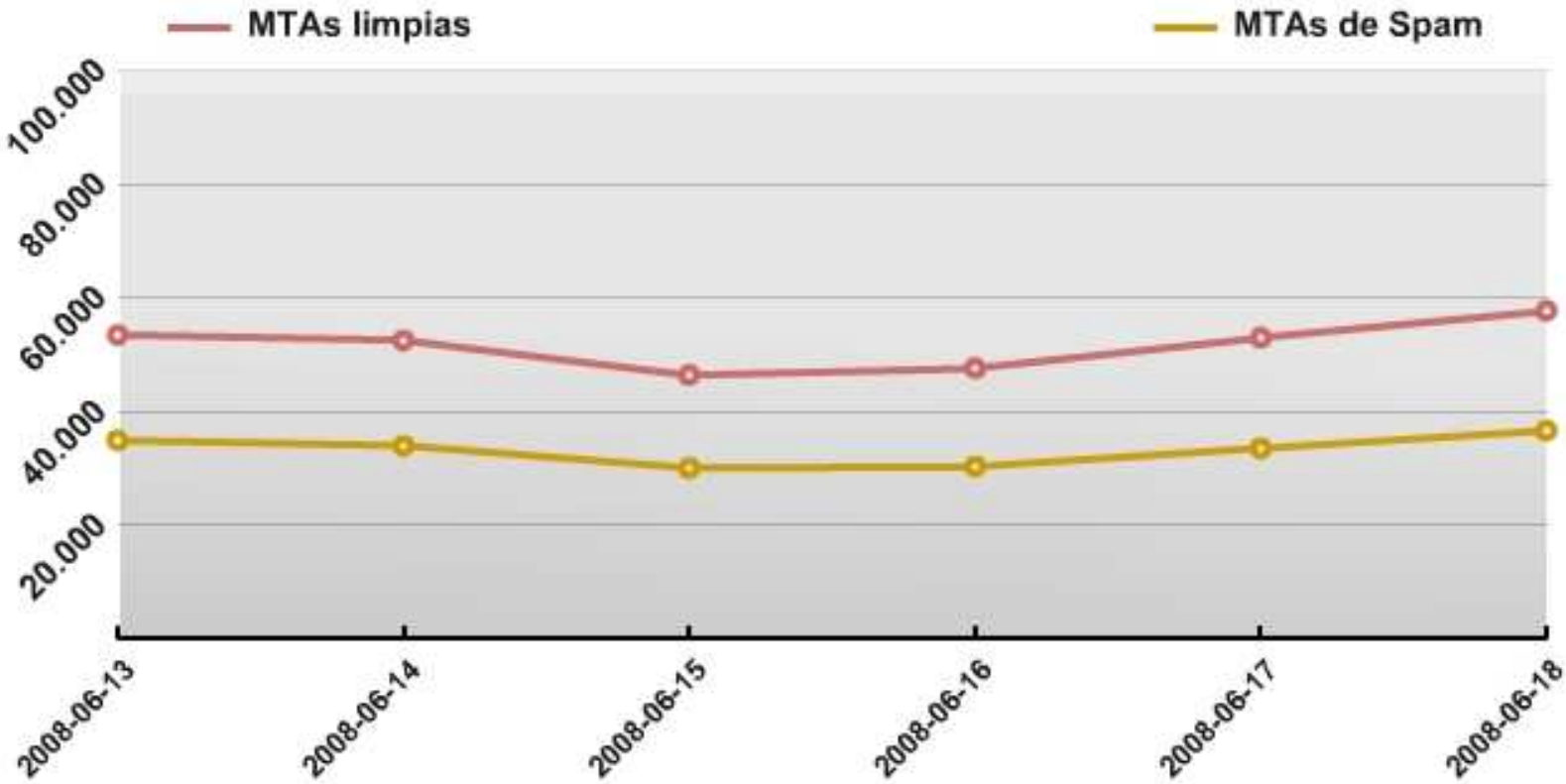
Line chart: TOTAL EVOLUTION of the SPAM

INTECO
Instituto Nacional
de Tecnologías
de la Comunicación



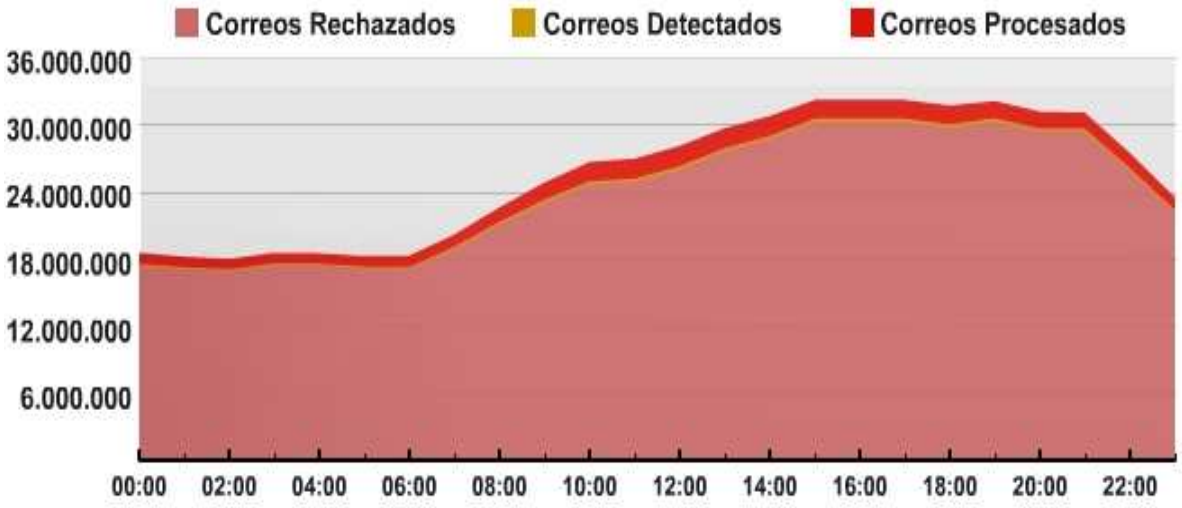
Tiempo	Correos Procesados	Spam Detectado	% Spam Detectado	Spam Rechazado	% Spam Rechazado
2008-06-05	21.872.698	20.612.118	94,2 %	20.374.846	93,2 %
2008-06-06	22.126.606	20.885.555	94,4 %	20.645.890	93,3 %
2008-06-07	18.709.085	17.718.849	94,7 %	17.560.832	93,9 %
2008-06-08	17.100.806	16.249.918	95,0 %	16.112.502	94,2 %
2008-06-09	20.094.968	18.833.842	93,7 %	18.632.126	92,7 %
2008-06-10	20.402.728	19.159.310	93,9 %	18.959.098	92,9 %
2008-06-11	28.858.352	27.629.027	95,7 %	27.364.198	94,8 %
2008-06-12	31.703.525	30.411.735	95,9 %	30.156.846	95,1 %
2008-06-13	26.676.115	25.443.859	95,4 %	25.203.802	94,5 %
2008-06-14	19.075.525	18.202.263	95,4 %	18.000.330	94,4 %
2008-06-15	25.889.555	25.008.162	96,6 %	24.843.303	96,0 %
2008-06-16	20.084.606	18.940.011	94,3 %	18.777.397	93,5 %
2008-06-17	21.450.145	20.253.202	94,4 %	20.059.274	93,5 %
2008-06-18	300.111	172.816	57,6 %	172.816	57,6 %

Interactive line chart: MTA EVOLUTION



Tiempo	Correos Procesados	Spam Detectado	% Spam Detectado	Spam Rechazado	% Spam Rechazado	MTAs	MTAs Spam	% MTAs Spam
2008-06-13	254.492	158.805	62,4 %	158.805	62,4 %	53.280	34.767	65,3 %
2008-06-14	256.860	154.671	60,2 %	154.671	60,2 %	52.322	33.809	64,6 %
2008-06-15	230.297	141.261	61,3 %	141.261	61,3 %	46.223	29.887	64,7 %
2008-06-16	219.677	125.764	57,2 %	125.764	57,2 %	47.423	30.173	63,6 %
2008-06-17	270.394	150.751	55,8 %	150.751	55,8 %	52.806	33.362	63,2 %
2008-06-18	300.111	172.816	57,6 %	172.816	57,6 %	57.513	36.491	63,4 %

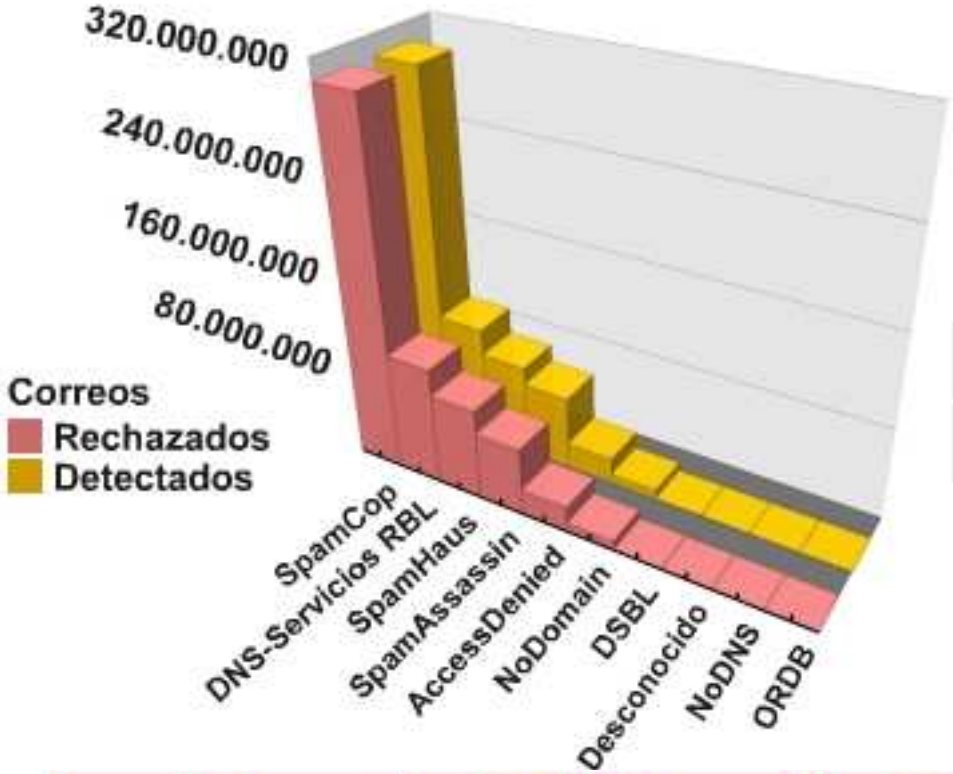
Interactive area chart: SPAM by HOUR



Total de Mensajes Procesados	611.426.468
Total de Spam Detectado	578.134.126
Porcentaje de Spam Detectado	94,6 %
Total de Spam Rechazado	572.773.123
Porcentaje de Spam Rechazado	93,7 %

Hora	Correos Procesados	Spam Detectado	% Spam Detectado	Spam Rechazado	% Spam Rechazado
00:00	18.538.374	17.553.409	94,7 %	17.385.318	93,8 %
01:00	18.170.868	17.247.018	94,9 %	17.097.284	94,1 %
02:00	17.988.682	17.031.481	94,7 %	16.888.380	93,9 %
03:00	18.529.396	17.617.825	95,1 %	17.467.691	94,3 %
04:00	18.497.268	17.549.696	94,9 %	17.397.518	94,1 %
05:00	18.243.861	17.314.285	94,9 %	17.178.513	94,2 %
06:00	18.269.149	17.248.008	94,4 %	17.101.794	93,6 %
07:00	20.160.680	19.064.669	94,6 %	18.895.489	93,7 %
08:00	22.609.767	21.293.329	94,2 %	21.089.033	93,3 %
09:00	24.803.888	23.265.370	93,8 %	23.022.454	92,8 %
10:00	26.626.462	24.903.879	93,5 %	24.657.292	92,6 %
11:00	26.931.348	25.167.275	93,4 %	24.922.480	92,5 %
12:00	28.090.338	26.251.706	93,5 %	25.957.100	92,4 %
13:00	29.689.510	27.874.704	93,9 %	27.615.997	93,0 %

Interactive bar chart: SPAM by METHOD



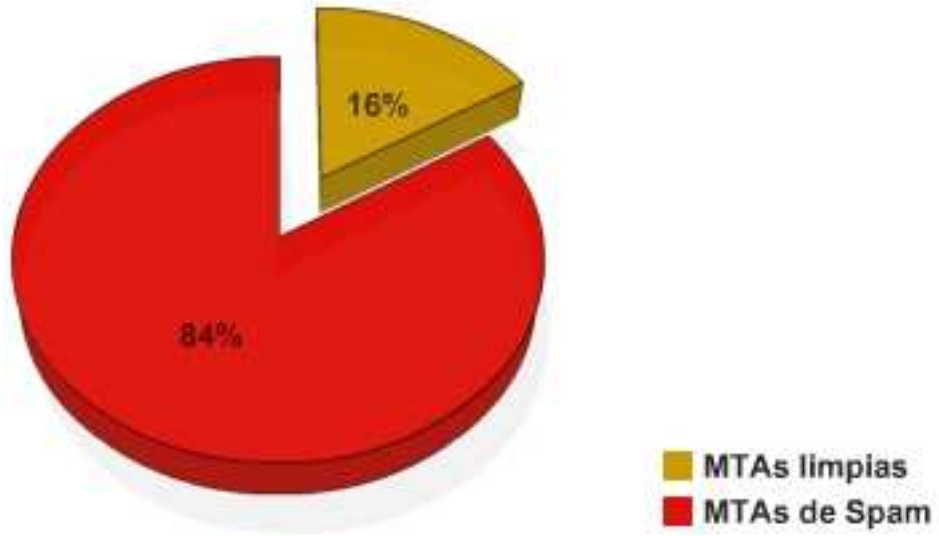
Total de Spam Detectado	578.152.134
Total de Spam Rechazado	572.790.513

Método	Spam Detectado	Spam Rechazado	Número de Sensores
SpamCop	303.998.635	303.998.635	14
DNS-Servicios RBL	101.021.293	101.021.293	11
SpamHaus	78.718.713	78.718.713	11
SpamAssassin	63.941.694	58.580.073	11
AccessDenied	22.078.833	22.078.833	11
NoDomain	7.799.976	7.799.976	11
DSBL	422.250	422.250	11
Desconocido	167.646	167.646	11
NoDNS	3.093	3.093	3

Interactive pie chart: SPAM TOTALS

Total de Mensajes Procesados	611.426.106
Total de Spam Detectado	578.152.134
Porcentaje de Spam Detectado	94,6 %
Total de Spam Rechazado	572.790.513
Porcentaje de Spam Rechazado	99,1 %

Interactive pie chart: MTA TOTALS



Total de MTAs	2.798.339
Total de MTAs de Spam	2.351.856
Porcentaje de MTAs de Spam	84,0 %

Problems found

INTECO
Instituto Nacional de Tecnologías de la Comunicación

- Client side
  - Tailored for each organization
    - Email infrastructure changes.
    - Anti-SPAM products changes
    - Anti-SPAM versions changes
    - Anti-SPAM Filter changes
- Server side
  - Huge amount of input data. Sampling.
  - IP information changes. Ip resolution very often.
  - Whois services response differences (RIPE, ARIN, APNIC..)

Questions?

INTECO
Instituto Nacional de Tecnologías de la Comunicación

- More info:
  - https://ersi.inteco.es
  - Sensors Support. soporte.sensores@inteco.es

- Juan Díez. juan.diez@inteco.es
- Luis Fernández. luis.fernandez@inteco.es

Instituto Nacional
de Tecnologías
de la Comunicación

www.inteco.es