Ataques de amplificación y protección de servicios esenciales

Lic. Einar Lanfranco
Lic. Nicolás Macia

Sobre CERTUNLP

La Universidad Nacional de La Plata es sede y miembro fundador del NAP Cabase La Plata

CERTUNLP es un CSIRT académico que funciona en el ámbito de la UNLP

- ASN: 5692
- Net Block IPv4: 163.10.0.0/16
- Net Block IPv6: 2800:340::/32
- Domain: .unlp.edu.ar

… pero, ¿Qué es un CSIRT?

CERTUNLP
Equipo de Respuesta a Incidentes de Seguridad

CSIRT

Un CSIRT o “Equipo de respuesta de incidentes de Seguridad Informática” **gestiona, coordina y da soporte en la respuesta a incidentes de seguridad** que afectan a su comunidad.

¿CERT = CSIRT?

CERT = Computer Emergency Response Team

CSIRT = Computer Security Incident Response Team

Ambos términos se solían utilizar indistintamente.

Actualmente se tiende a usar el término CSIRT.

CERT UNLP

Equipo de Respuesta a Incidentes de Seguridad

Agenda

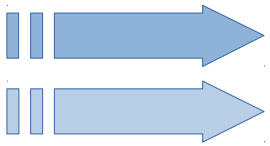
- Ataques de amplificación
- BCP 38: para filtros antispoofing
- La experiencia del CERTUNLP y NAP LPL
- BCP 134: SPAM y la experiencia de Brasil

CERTUNLP
Equipo de Respuesta a Incidentes de Seguridad

Ataques de Amplificación

- Se aprovechan de protocolos que, ante un requerimiento de un tamaño “x”, retornan una respuesta mucho mayor que “x”.
- El grado de amplificación depende del protocolo utilizado.
- Generalmente se utilizan servicios UDP ya que:
  - No se necesita establecer una conexión.
  - Es más simple “mentir” sobre el origen IP.
- Se usan en ataques de DDOS (Denegación de Servicio Distribuido)
- Afectan: en mayor medida, la red de la víctima del ataque y, en menor medida, a las redes intermedias entre, el servicio vulnerable y la víctima.

Factores de Amplificación



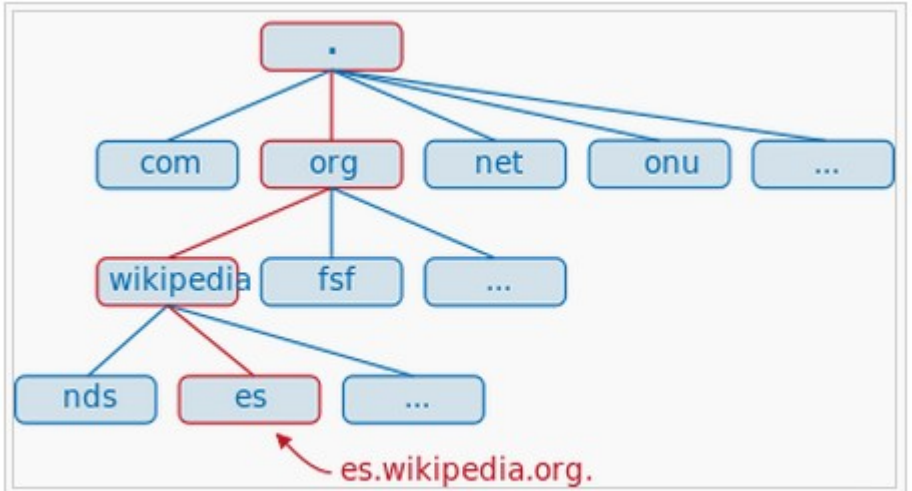
Protocol	Bandwidth Amplification Factor	Vulnerable Command
DNS	28 to 54	see: TA13-088A [4]
NTP	556.9	see: TA14-013A [5]
SNMPv2	6.3	GetBulk request
NetBIOS	3.8	Name resolution
SSDP	30.8	SEARCH request
CharGEN	358.8	Character generation request
QOTD	140.3	Quote request
BitTorrent	3.8	File search
Kad	16.3	Peer list exchange
Quake Network Protocol	63.9	Server info exchange
Steam Protocol	5.5	Server info exchange
Multicast DNS (mDNS)	2 to 10	Unicast query
RIPv1	131.24	Malformed request
Portmap (RPCbind)	7 to 28	Malformed request

Fuente: https://www.us-cert.gov/ncas/alerts/TA14-017A

CERT UNLP
Equipo de Respuesta a Incidentes de Seguridad

DNS

- Servicio esencial para el funcionamiento de Internet.
  - Mediante el DNS, se maneja la resolución de nombres FQDN a IP
- Originalmente corría sobre UDP, aunque ahora está previsto el uso de TCP en determinadas situaciones.
- El sistema de DNS mantiene la información en forma distribuida.



Árbol DNS

Tipos de servidores de DNS

El esquema de DNS plantea distintos tipos de servidores. De éstos, los que seguramente tengamos oportunidad de administrar:

- DNS resolver:

  Servidor de DNS que utilizarán mis usuarios para resolver los FQDN utilizados:

  - www.google.com
  - www.facebook.com

  Debería atender requerimientos solamente de nuestros usuarios

  - Si alguien en Internet quiere preguntarme por www.google.com ,

    → **QUE USE SU DNS SERVER!!!**

- DNS Zone server:

  Es donde se configuran las IP que tienen los hosts y servidores de mi zona DNS (suponiendo que mi zona fuese .mizona.com):

  - www.mizona.com

  Debe estar abierto a consultas de todo el mundo

  - Si alguien en Internet quiere saber la IP de www.mizona.com debo responder con la IP de dicho servidor.

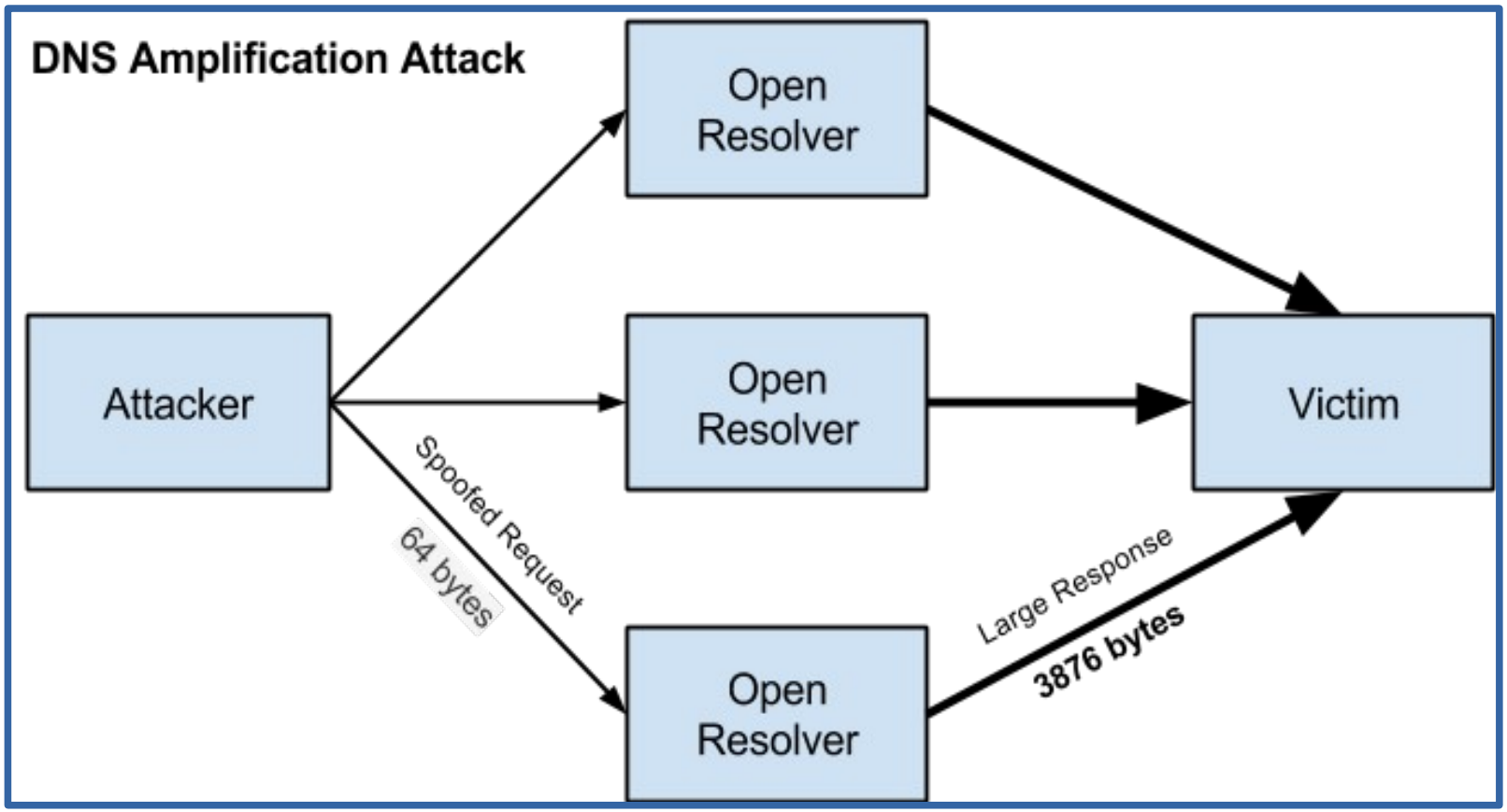
DNS Resolvers abiertos

- Es común que el Resolver DNS no se configure para aceptar **solamente** consultas de nuestras redes.
- Un resolver abierto permite que cualquier IP le haga consultas DNS, posibilitando entre otros problemas, ataques de amplificación.

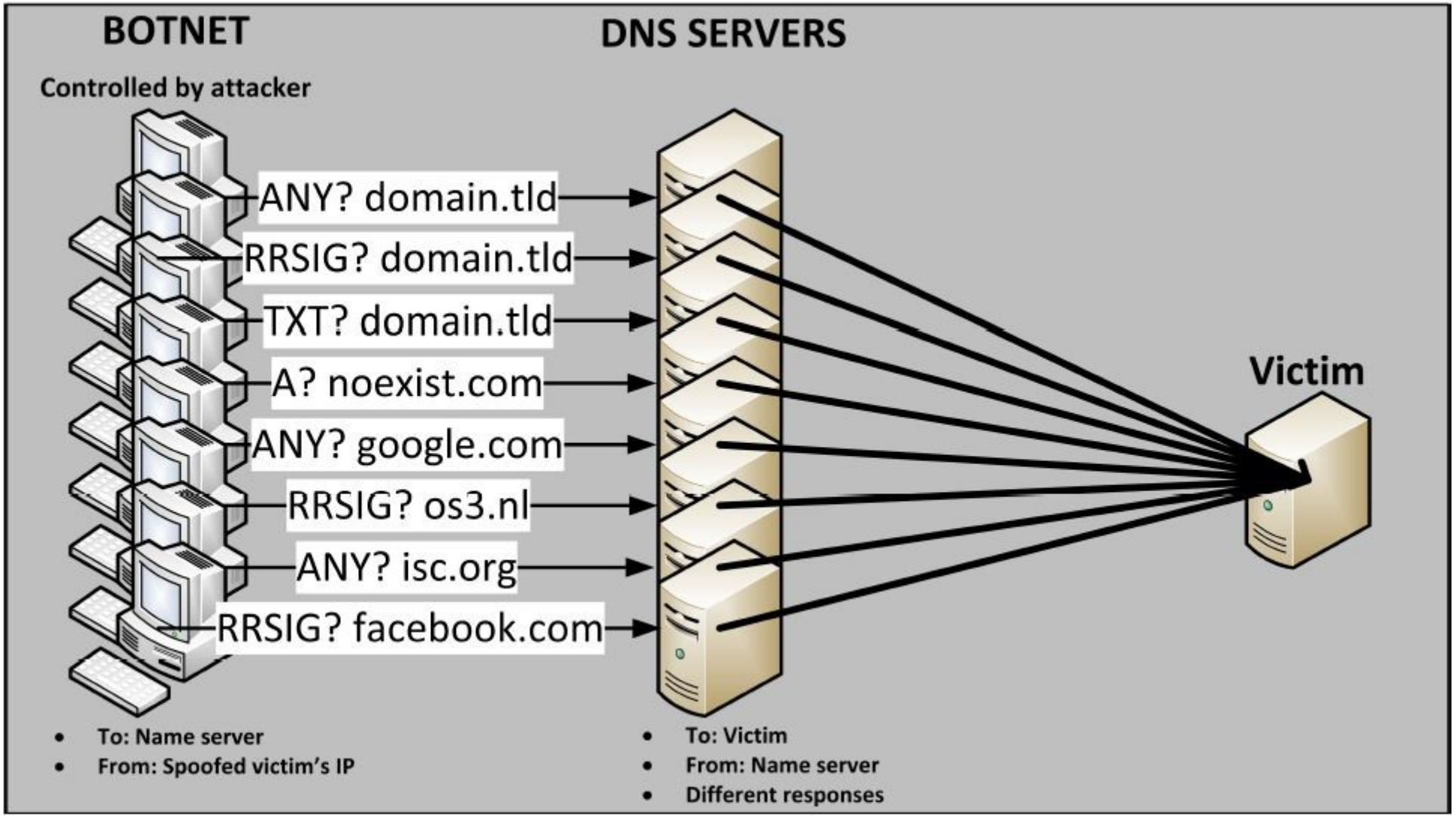
```
dig +dnssec any lacnic.net  @8.8.4.4
```

```
;; Query time: 95 msec
;; SERVER: 8.8.4.4#53(8.8.4.4)
;; WHEN: Mon Nov 02 18:30:05 ART 2015
;; MSG SIZE  rcvd: 3656
```

Ataque de amplificación usando resolvers abiertos



Ataque de amplificación usando resolvers abiertos (cont)



Demo Simple

Usando:

- Dig
- Wireshark
- Un Servidor DNS que admita consultas recursivas
  - Uso de registros DNSsec
- Veamos un video

Soluciones en DNS

Evitar que terceros manipulen nuestros servidores DNS:

- En los DNS Resolvers:
  - No aceptar consultas recursivas sin restricciones

Bind9

Add the following to the global options [8]:

```
options {
      allow-query-cache { none; };
      recursion no;
};
```

In the global options, include the following [10]:

```
acl corpnets { 192.168.1.0/24; 192.168.2.0/24; };
options {
  allow-query { any; };
  allow-recursion { corpnets; };
};
```

- Sobre los servidores de zona:
  - Limitar el número de consultas en un lapso de tiempo (RRL)

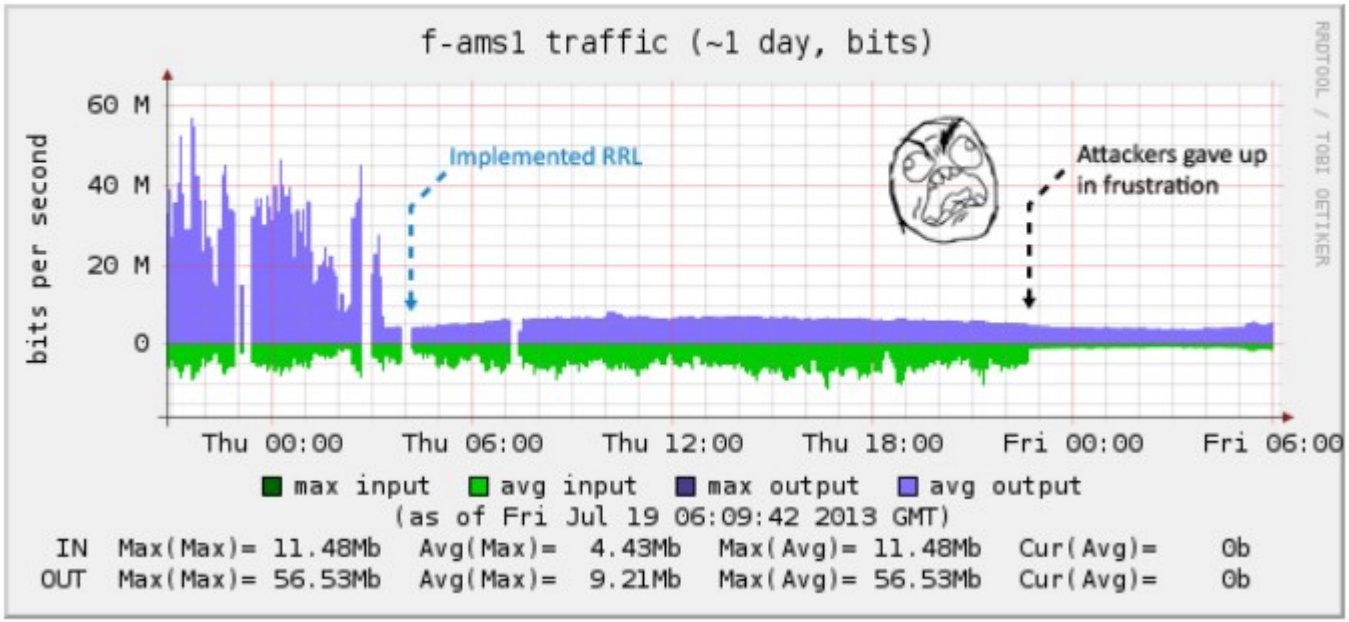
```
rate-limit {
    responses-per-second 5;
    window 5;
};
```

Fuente: https://www.us-cert.gov/ncas/alerts/TA13-088A

Experiencia RRL

Fuente: https://conference.apnic.net/data/37/apricot-2014-rrl_1393309768.pdf

ISC F-Root



Enabling RRL

- RRL is available in ISC's BIND 9.9.4 Software
  - **Download:** https://www.isc.org/downloads/
  - **RRL support must be enabled with –enable-rrl prior to compiling**
  - **Documentation:** https://kb.isc.org/article/AA-01000

```
options {
    directory "/var/named";
    rate-limit {
        responses-per-second 5;
#       log-only yes;
    };
};
```

Otros protocolos susceptibles a ataque de amplificación

Protocol	Bandwidth Amplification Factor	Vulnerable Command
DNS	28 to 54	see: TA13-088A [4]
NTP	556.9	see: TA14-013A [5]
SNMPv2	6.3	GetBulk request
NetBIOS	3.8	Name resolution
SSDP	30.8	SEARCH request
CharGEN	358.8	Character generation request
QOTD	140.3	Quote request
BitTorrent	3.8	File search
Kad	16.3	Peer list exchange
Quake Network Protocol	63.9	Server info exchange
Steam Protocol	5.5	Server info exchange
Multicast DNS (mDNS)	2 to 10	Unicast query
RIPv1	131.24	Malformed request
Portmap (RPCbind)	7 to 28	Malformed request

Fuente: https://www.us-cert.gov/ncas/alerts/TA14-017A

CERT UNLP
Equipo de Respuesta a Incidentes de Seguridad

NTP

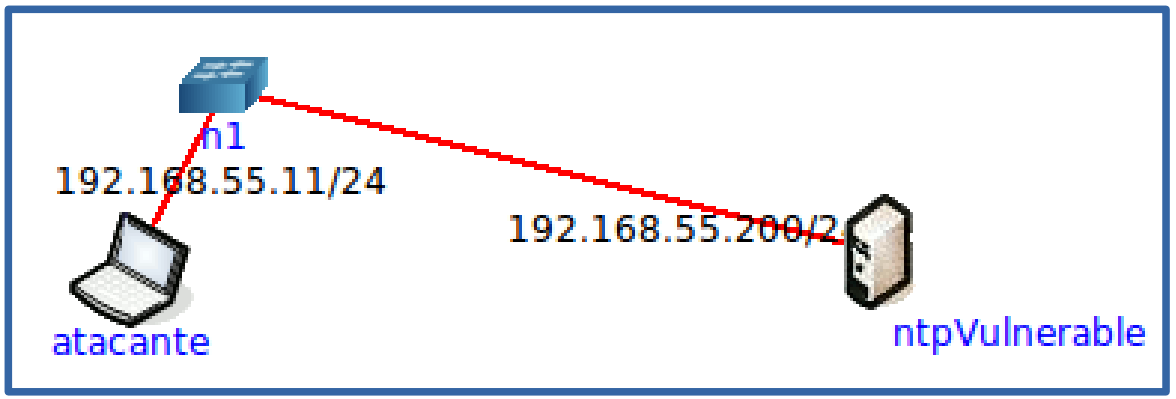
- Maneja el sincronismo de relojes en Internet.
- Corre sobre UDP.
- Es uno de los protocolos con mayor factor de amplificación!!!

Detección y verificación de servidores NTP públicos

- Detección de servidores:
  - Shodan
  - Veamos un VIDEO
- Verificación de amplificación:
  - ntpdc -n -c monlist x.x.x.x
  - Wireshark
  - Veamos un VIDEO

Demo ataque amplificación en laboratorio

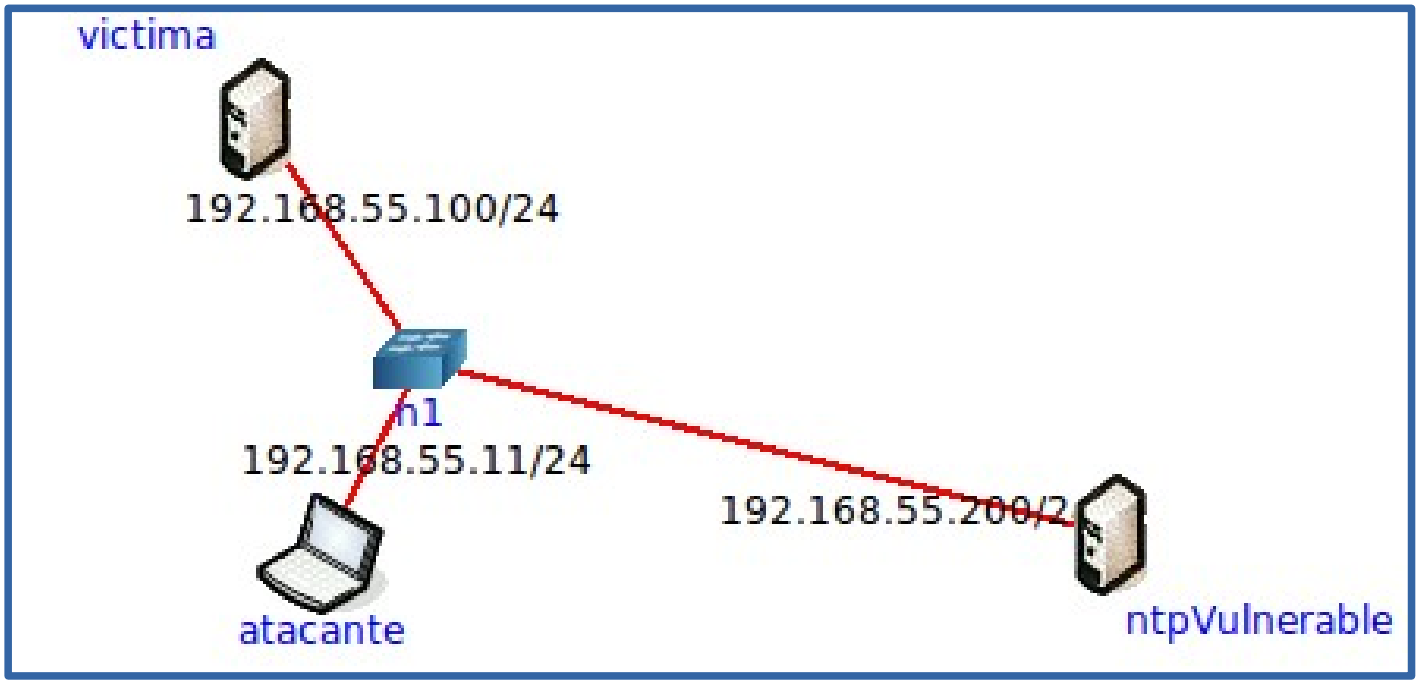
- Verificación de amplificación:
  - ntpdc -n -c monlist x.x.x.x
  - ntpdate -p 1 -d <vulnerable ntp IP>
  - ntpdc -n -c monlist x.x.x.x
  - Wireshark
  - Veamos un VIDEO



- Envenenando el servidor
  - ntpdate -p 1 -d <vulnerable ntp IP>
  - wireshark
  - bittwiste -I original.pcap -O spoofed.pcap -T ip -s <spoofed IP>
  - bittwist spoofed.pcap -I 1 -i eth0
  - Veamos un VIDEO

Demo ataque amplificación en laboratorio (cont)

- Ataque a un tercero
  - bittwiste -I original.pcap -O spoofed.pcap -T ip -s <víctima>
  - bittwist spoofed.pcap -l 800000 -i eth0
  - Iptraf



  - Veamos un VIDEO

Soluciones en NTP

En el pasado, los problemas descubiertos en NTP que se prestaban a ataques de amplificación, requerían:

- Actualización de software
- Configuraciones adecuadas

Recommended Course of Action

As all versions of ntpd prior to 4.2.7 are vulnerable by default, the simplest recommended course of action is to upgrade all versions of ntpd that are publically accessible to at least 4.2.7. However, in cases where it is not possible to upgrade the version of the service, it is possible to disable the monitor functionality in earlier versions of the software.

To disable “monlist” functionality on a public-facing NTP server that cannot be updated to 4.2.7, add the “noquery” directive to the “restrict default” line in the system’s ntp.conf, as shown below:

```
restrict default kod nomodify notrap nopeer noquery

restrict -6 default kod nomodify notrap nopeer noquery
```

Fuente: https://www.us-cert.gov/ncas/alerts/TA14-013A

¿Qué otras cosas podemos hacer?

Todos podemos ayudar evitando ser parte del problema:

- Aplicando filtros antispoofing para evitar que nuestros servicios se usen en ataques de amplificación contra terceros.

- Estando atentos a nuevos problemas en servicios o protocolos que usamos para poder aplicar recomendaciones dadas en cada caso.

Filtros antispoofing

- Basado en la “Best Current Practice” **BCP 38: Network Ingress Filtering**

  https://tools.ietf.org/html/bcp38

  http://www.bcp38.info

- La idea es aplicar filtros que eviten que se inicien comunicaciones desde una IP origen falsa:
  - El ISP puede aplicar los filtros en forma entrante en el punto de conexión del cliente.
  - Alternativamente, el administrador de red puede aplicar filtros salientes en su punto de conexión a Internet.

Mantenerse informado

- Para enterarnos de problemas de seguridad en servicios que se prestan (incluidos ataques de amplificación)
  - **Es útil estar suscripto a listas de correo.**
  - Hay muchas listas, con distintos volúmenes y nivel de especialización.
  - Para empezar, la lista de Hispasec es una muy buena opción. http://www.hispasec.com/
    - En español, dirigida a un público genérico

Experiencia en el NAP LPL

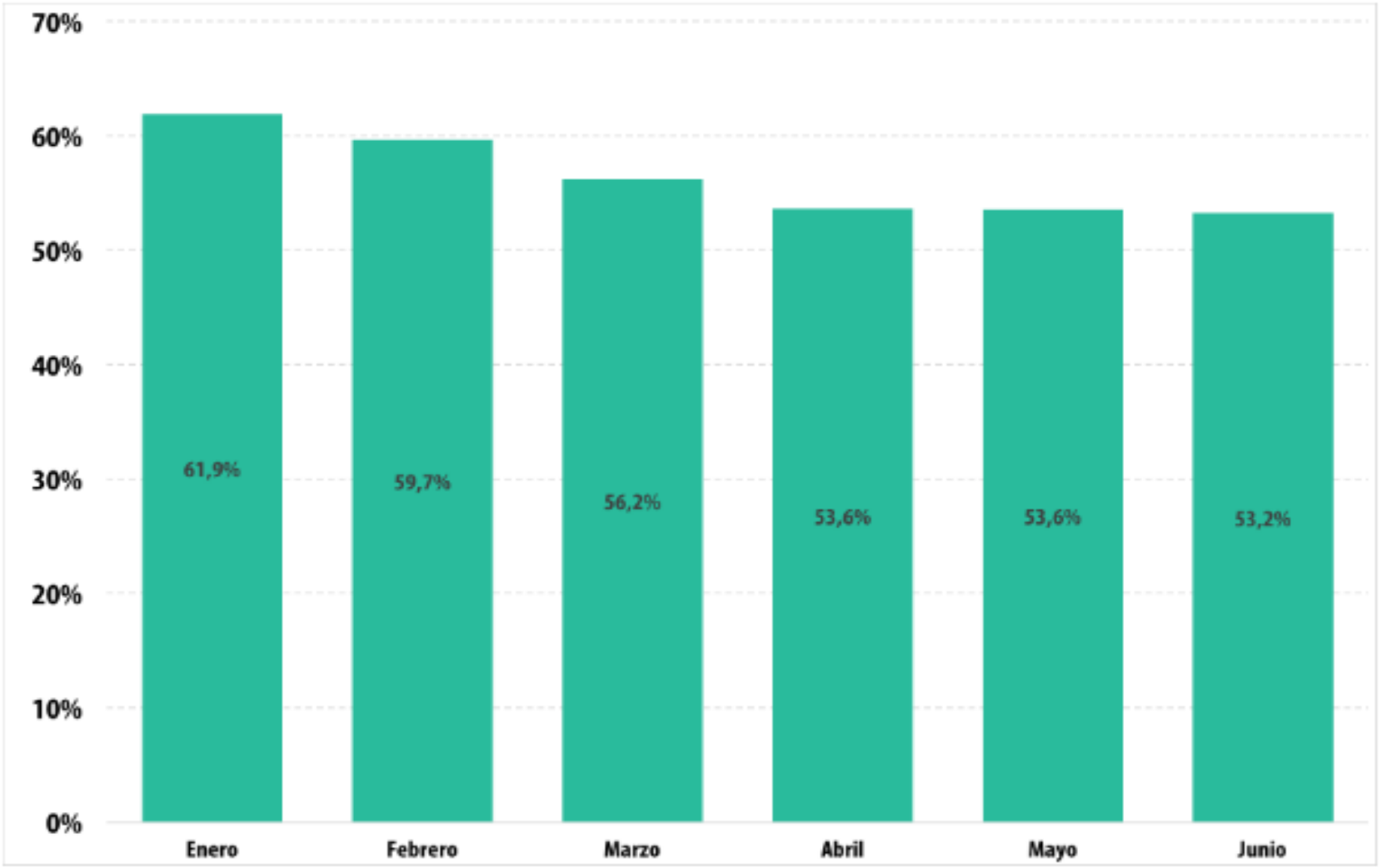
- En Diciembre del año 2014, CERTUNLP realizó una serie de pruebas buscando determinados problemas de seguridad en las redes de los miembros del NAP LPL
  - Entre los problemas buscados, se relevaron algunos relacionados a posibles ataques de amplificación.
  - Entre los hallazgos, se encontraron:
    - 29 casos de problemas de Resolvers DNS abiertos
    - 7 casos de problemas de NTP servers vulnerables

Actualmente estamos trabajando para probar e incorporar más pruebas de seguridad al sistema de detección

CERTUNLP
Equipo de Respuesta a Incidentes de Seguridad

SPAM

Según Kaspersky:



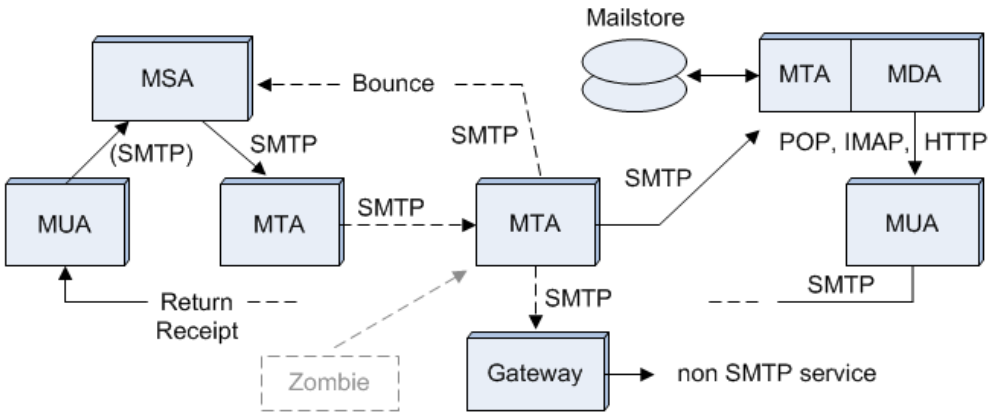
Porcentaje de spam en el tráfico postal en enero-junio de 2015

ERT UNLP
Respuesta a Incidentes de Seguridad

Otras acciones que podemos promover

- Como operadores de red, tenemos la posibilidad de combatir el SPAM residencial
- La “Best Current Practice” **BCP 134: Email Submission Operations: Access and Accountability Requirements**

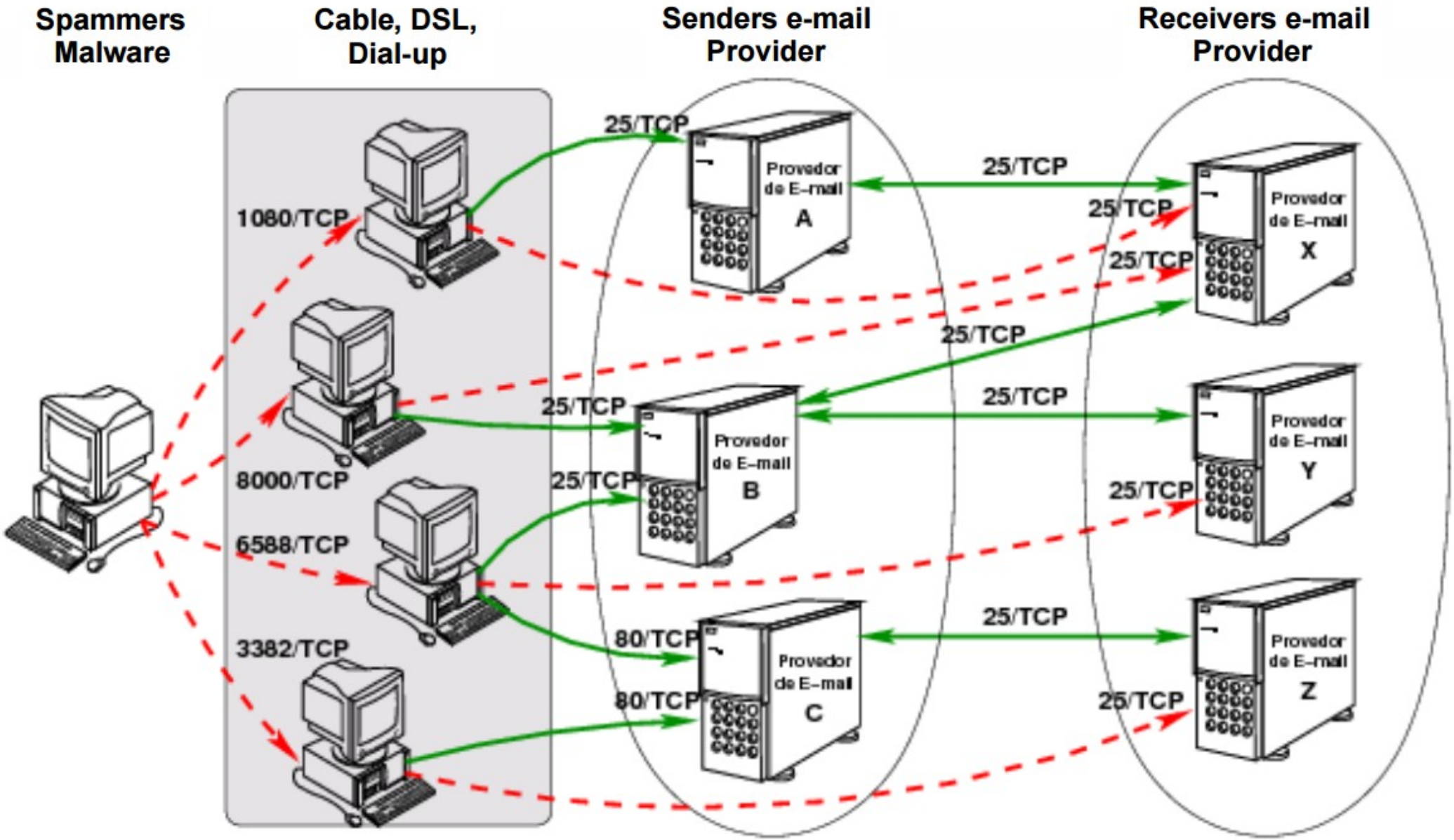
https://tools.ietf.org/html/bcp134



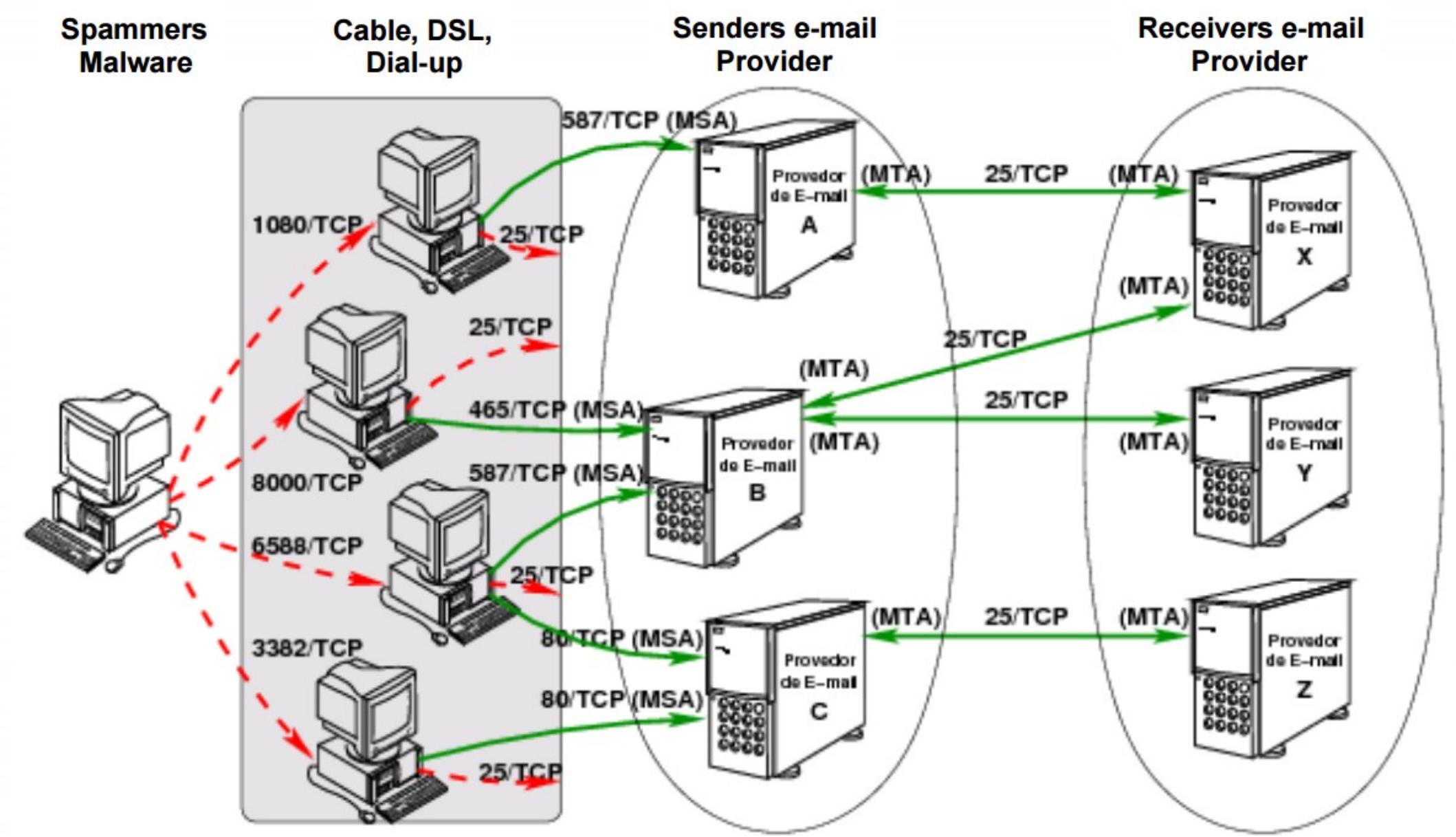
- Mail User Agents (MUAs)
- Mail Submission Agents (MSAs)
- Mail Transfer Agents (MTAs)
- Mail Delivery Agents (MDAs)

CERT UNLP
Equipo de Respuesta a Incidentes de Seguridad

Cuál es el problema?



En qué consiste el gerenciamiento?



Una buena experiencia para replicar

- En el año 2009 Brasil era el país con más número de IPs listadas en CBL (14,53%)

  http://www.abuseat.org/nas.html

- Después de una fuerte campaña basada en la BCP 134 llamada **Gerência de Porta 25** lograron mitigar el problema.
- Para el año 2013, figuraban fuera del listado CBL.

Sobre la campaña

http://www.antispam.br/

CERT UNLP
Equipo de Respuesta a Incidentes de Seguridad

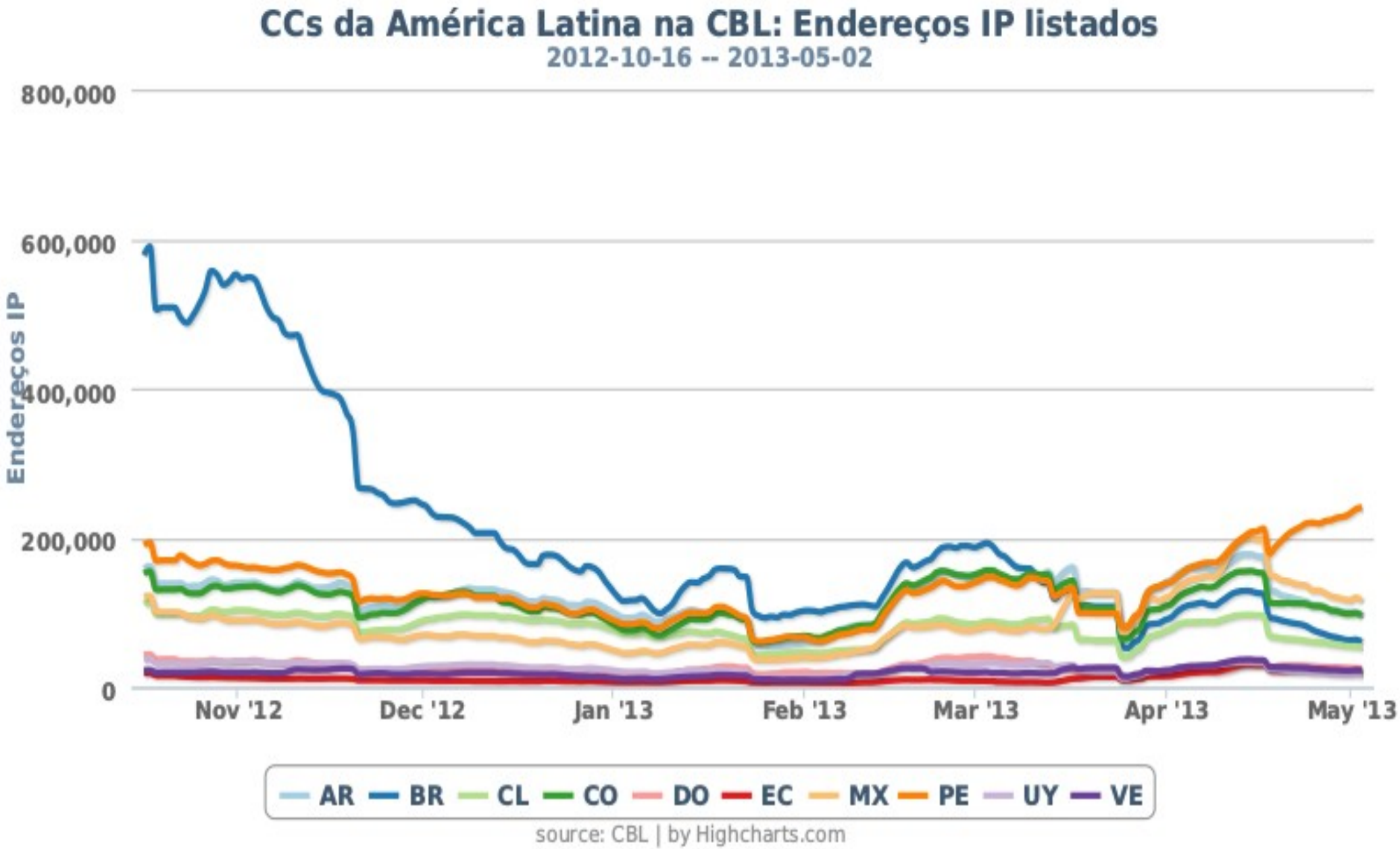
Sobre la campaña

CERT UNLP
Equipo de Respuesta a Incidentes de Seguridad

From CBL 1st in 2009 to 25th in 2013

The deadline for the implementation was March 2013

Comparison of the top LAC Countries in CBL



Gerenciamiento del puerto 25

La situación de Argentina según http://www.abuseat.org/nas.html

The top 20 worst countries (

Rank	By Infections			By Spam Volume	
	Country	Infections	%of CBL	Country	%of traffic
1	India	1309662	11.8%	Vietnam	18.1%
2	China	1083768	9.8%	United States	12.9%
3	Vietnam	968592	8.76%	South Korea	8.91%
4	Russian Federation	613055	5.54%	Russian Federation	5.89%
5	Iran	571700	5.17%	India	3.9%
6	Indonesia	503928	4.56%	China	3.2%
7	Brazil	387157	3.5%	Brazil	3.17%
8	Pakistan	315750	2.85%	Argentina	3.17%
9	Mexico	296608	2.68%	Ukraine	3%
10	United States	276457	2.5%	Iran	2.53%
11	Thailand	242903	2.2%	Indonesia	2.33%
12	Italy	238842	2.16%	Colombia	2.21%
13	Argentina	218588	1.98%	Chile	2.02%
14	Japan	197154	1.78%	Peru	1.55%
15	Peru	175447	1.59%	Turkey	1.44%
16	Germany	174149	1.57%	Kazakhstan	1.35%
17	Turkey	166188	1.5%	Spain	1.16%
18	Poland	158943	1.44%	Taiwan	1.15%
19	Ukraine	152437	1.38%	United Kingdom	1.13%
20	Taiwan	136110	1.23%	Mexico	1.1%

CERT UNLP
Equipo de Respuesta a Incidentes de Seguridad

Gracias!!

Contactos:

nmacia@cert.unlp.edu.ar

elanfranco@cert.unlp.edu.ar