DUST
Your Rss Feed belongs to you!

Chema Alonso
chema@informatica64.com
Juan Garrido «Silverhack»
jgarrido@informatica64.com

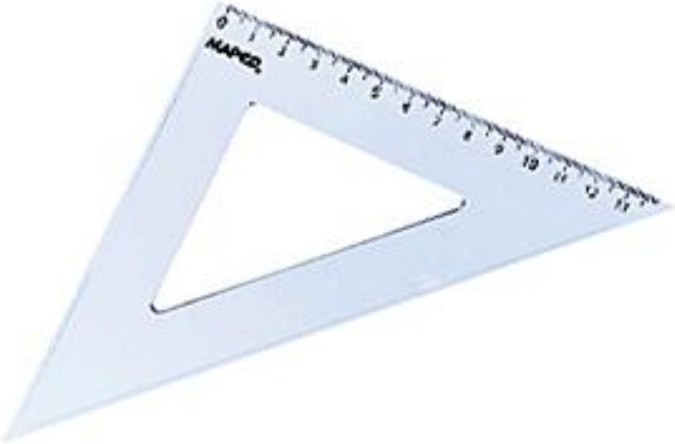
Informática 64

Once upon a time….

Informática 64

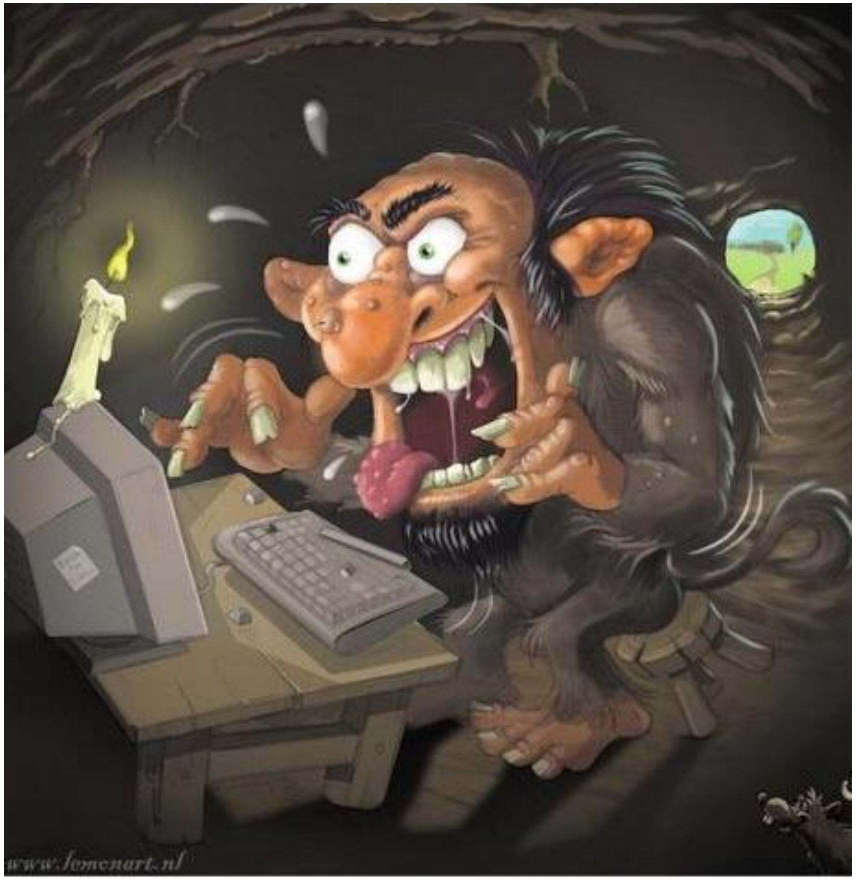
… and we believed it

- Internet is a space of freedom
- All opinions are allowed
- Freedon for news
- Nobody controls Internet
- Neutrality
- Anonimaty
- No Rules
- ….



We lived in the age of Aquarius

Our biggest problem: Trolls



..and we managed as cultured people

Si envian mensajes en HTML, hay tabla.
Si hacen Top-Posting, hay tabla.
Si envian SPAM, hay tabla.
Si envian un Off-Topic sin "OT:", hay tabla.
Si escriben en mayusculas, hay tabla.
Si escriben a lo h4x0r, hay tabla.
Si escriben con 'q' o 'k', hay tabla.
Si se desubican, hay tabla.
Si el subject no es descriptivo, hay tabla.
Si envian attachments, hay tabla.
Si escriben mas de 80 chars por linea, hay tabla.
Si usan un enconding raro, hay tabla.
Y si preguntan por esto, hay tabla.

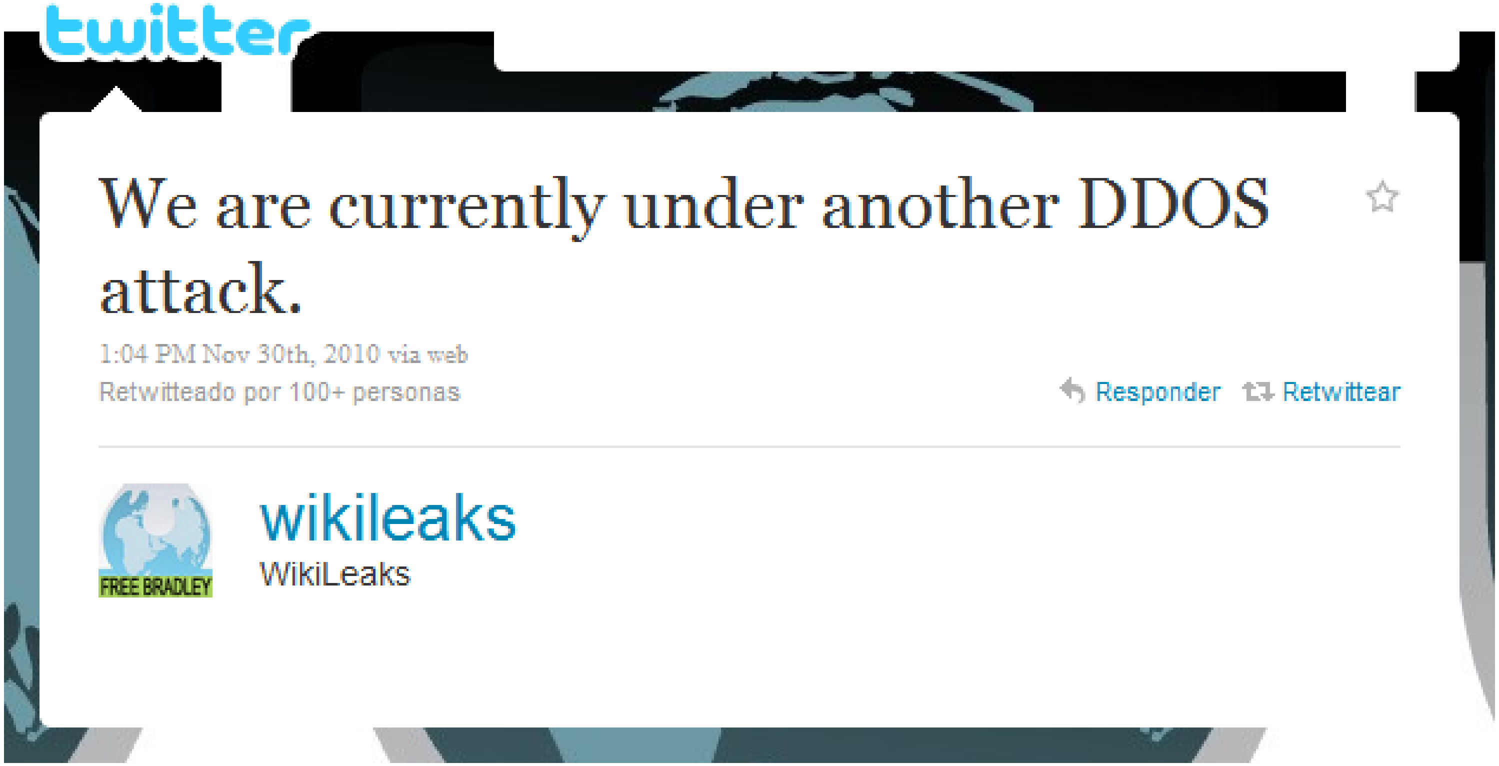
But them….

CENSORED
WIKILEAKS

…and we leaved out Matrix

Informática 64

We don´t like you!



We are currently under another DDOS attack.

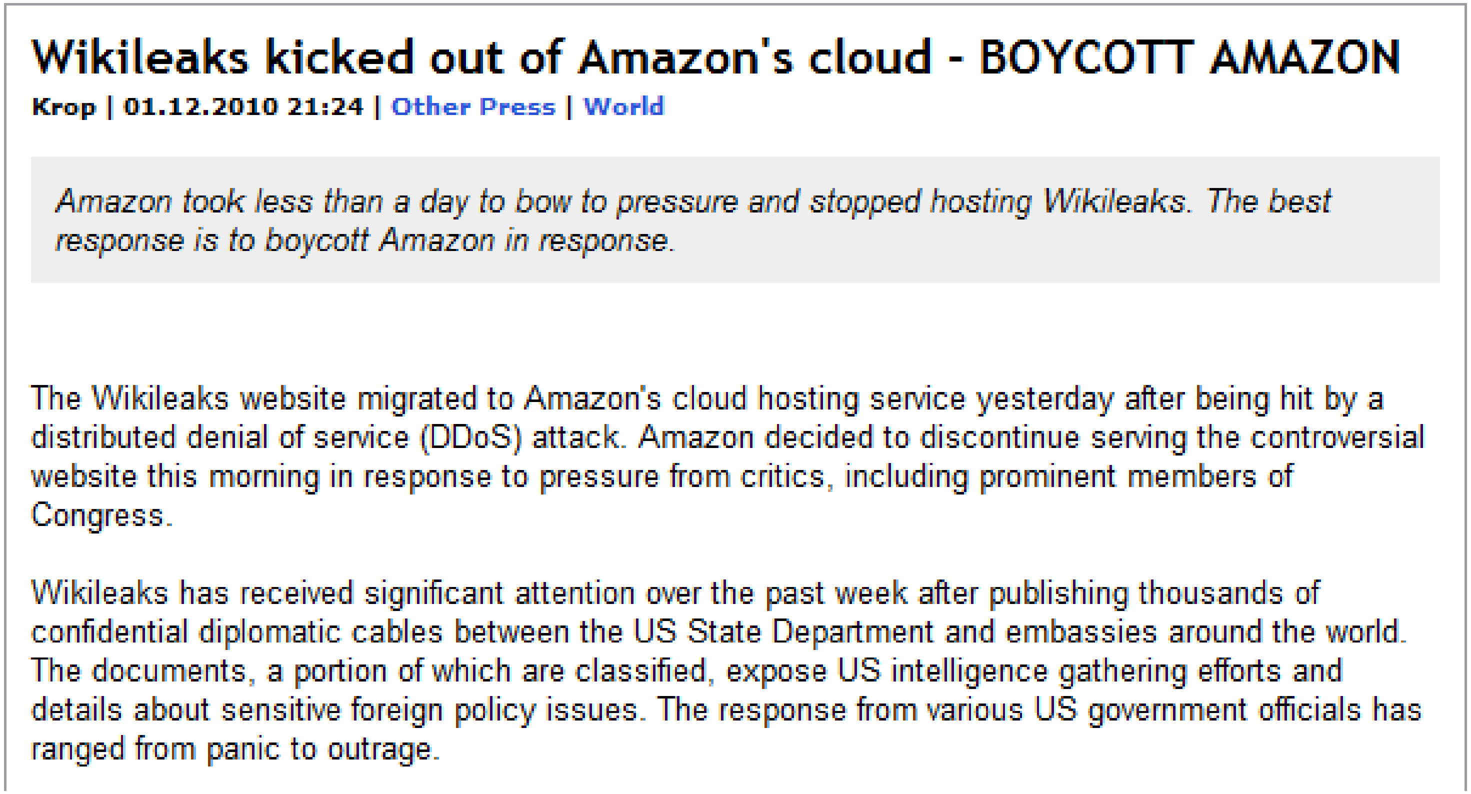
1:04 PM Nov 30th, 2010 via web

Retwitteado por 100+ personas

wikileaks

WikiLeaks

We don´t like you!



Wikileaks kicked out of Amazon's cloud - BOYCOTT AMAZON

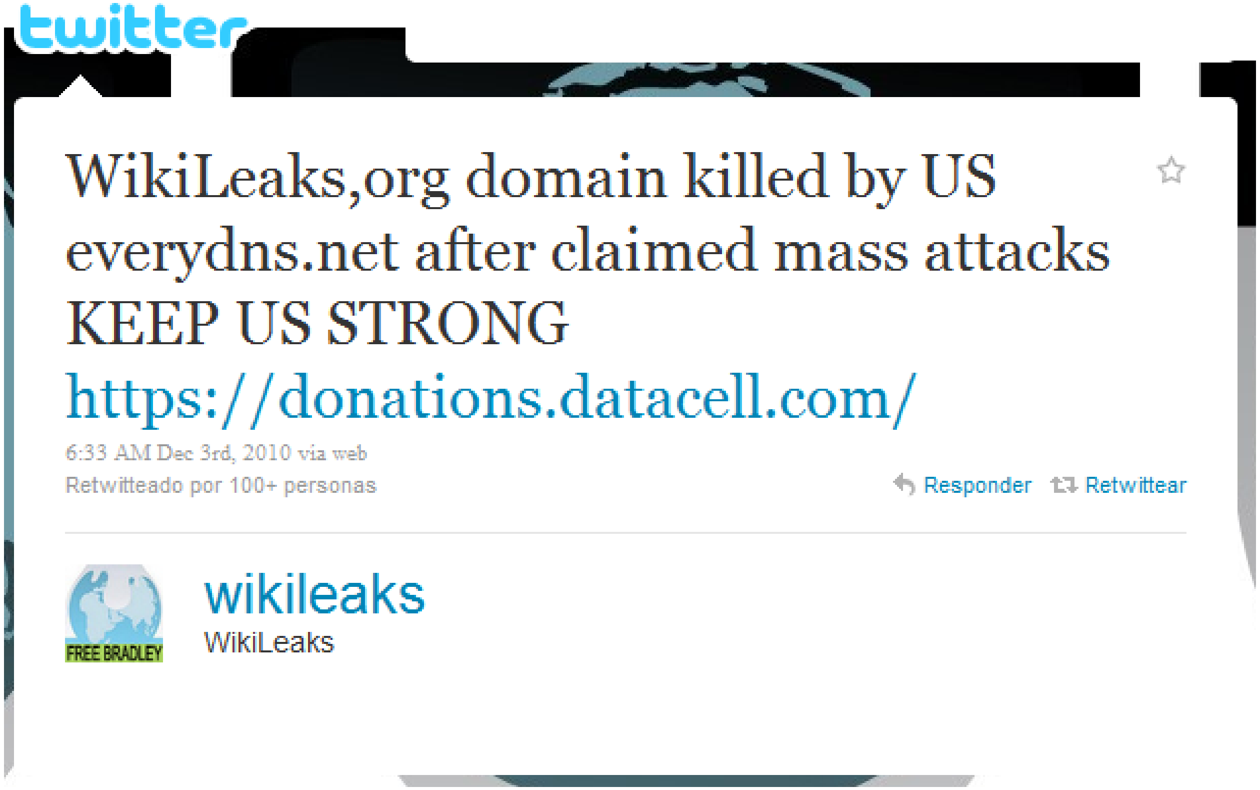
Krop | 01.12.2010 21:24 | Other Press | World

Amazon took less than a day to bow to pressure and stopped hosting Wikileaks. The best response is to boycott Amazon in response.

The Wikileaks website migrated to Amazon's cloud hosting service yesterday after being hit by a distributed denial of service (DDoS) attack. Amazon decided to discontinue serving the controversial website this morning in response to pressure from critics, including prominent members of Congress.

Wikileaks has received significant attention over the past week after publishing thousands of confidential diplomatic cables between the US State Department and embassies around the world. The documents, a portion of which are classified, expose US intelligence gathering efforts and details about sensitive foreign policy issues. The response from various US government officials has ranged from panic to outrage.

We don´t like you!



WikiLeaks,org domain killed by US everydns.net after claimed mass attacks KEEP US STRONG https://donations.datacell.com/

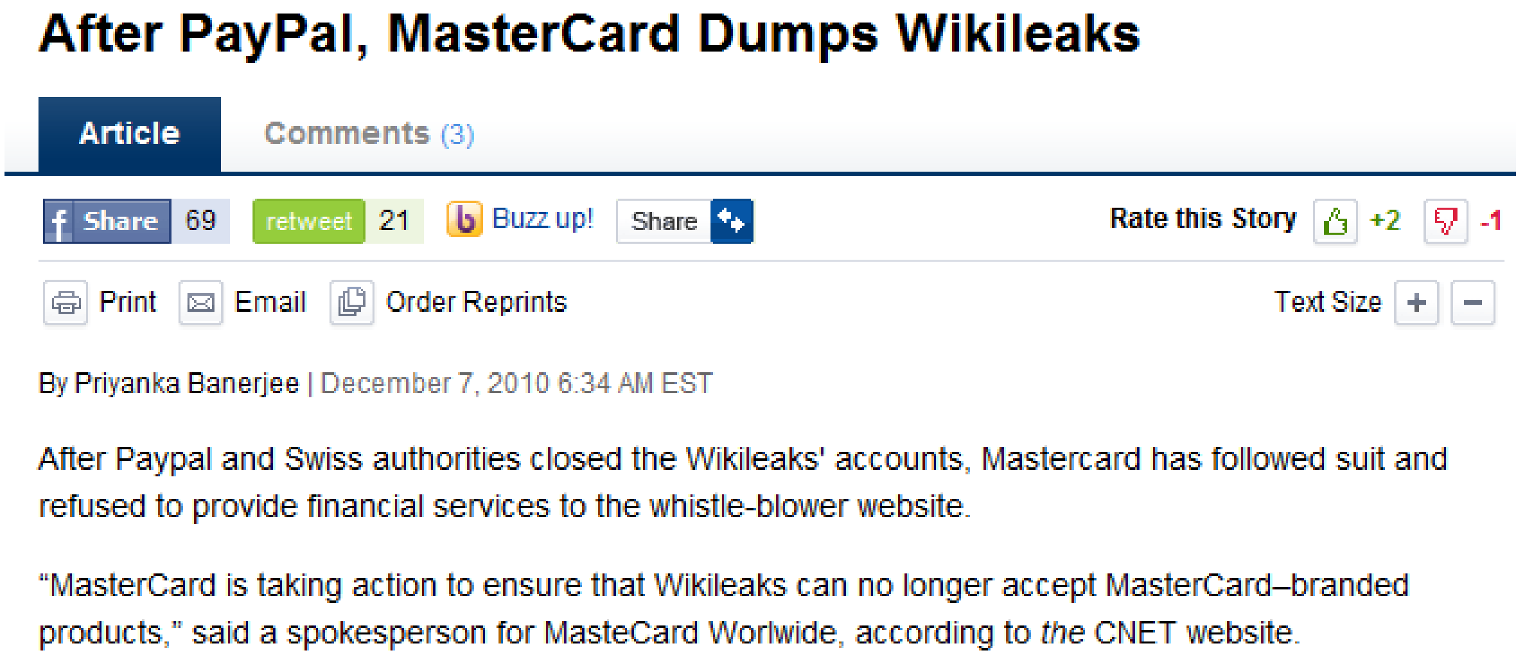
6:33 AM Dec 3rd, 2010 via web

Retwitteado por 100+ personas

wikileaks
WikiLeaks

Informática 64

We don´t like you!



After PayPal, MasterCard Dumps Wikileaks

By Priyanka Banerjee | December 7, 2010 6:34 AM EST

After Paypal and Swiss authorities closed the Wikileaks' accounts, Mastercard has followed suit and refused to provide financial services to the whistle-blower website.

“MasterCard is taking action to ensure that Wikileaks can no longer accept MasterCard–branded products,” said a spokesperson for MasteCard Worlwide, according to *the* CNET website.

4nOym0us

HBGary Ownage

- Backdoors:
  - Task B y 12 monkeys
- Fake FaceBook profiles
- Viral propaganda on Intenet

Internet has weaknesses

- Network connections
  - Great Wall Firewall in China
  - BGP Attack in Egypt
- DNS systems
  - Wikileaks.org
  - Rojadirecta.org
- Laws,
  - Every Country
  - International Laws

Spain: Our politicians…

Informática 64

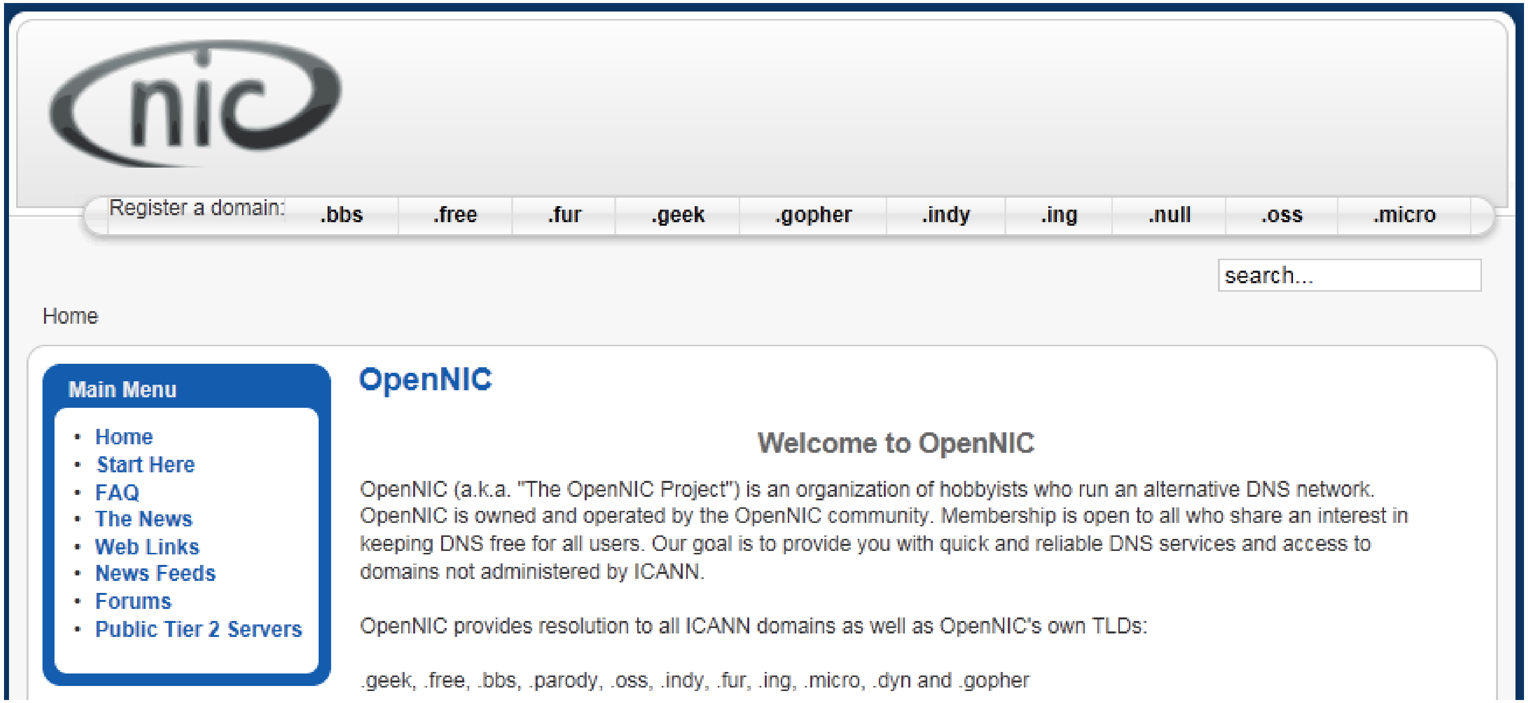
Aren´t you somehow …..?

Informática 64

How to shout you off ?

- GOAL: To disconnect your audience.
- HOW?
  - Taking the root off
    - (owning the system)
  - Making it unavailable
    - D.O.S.
  - Making it unlocalizable
    - Closing the domain name
    - Blocking service accounts
      - Facebook
      - Twitter
      - Google…
    - Infosec war (Banning from web searchers)
  - Throwing on it the law

Some fixes: OpenNIC



OpenNIC

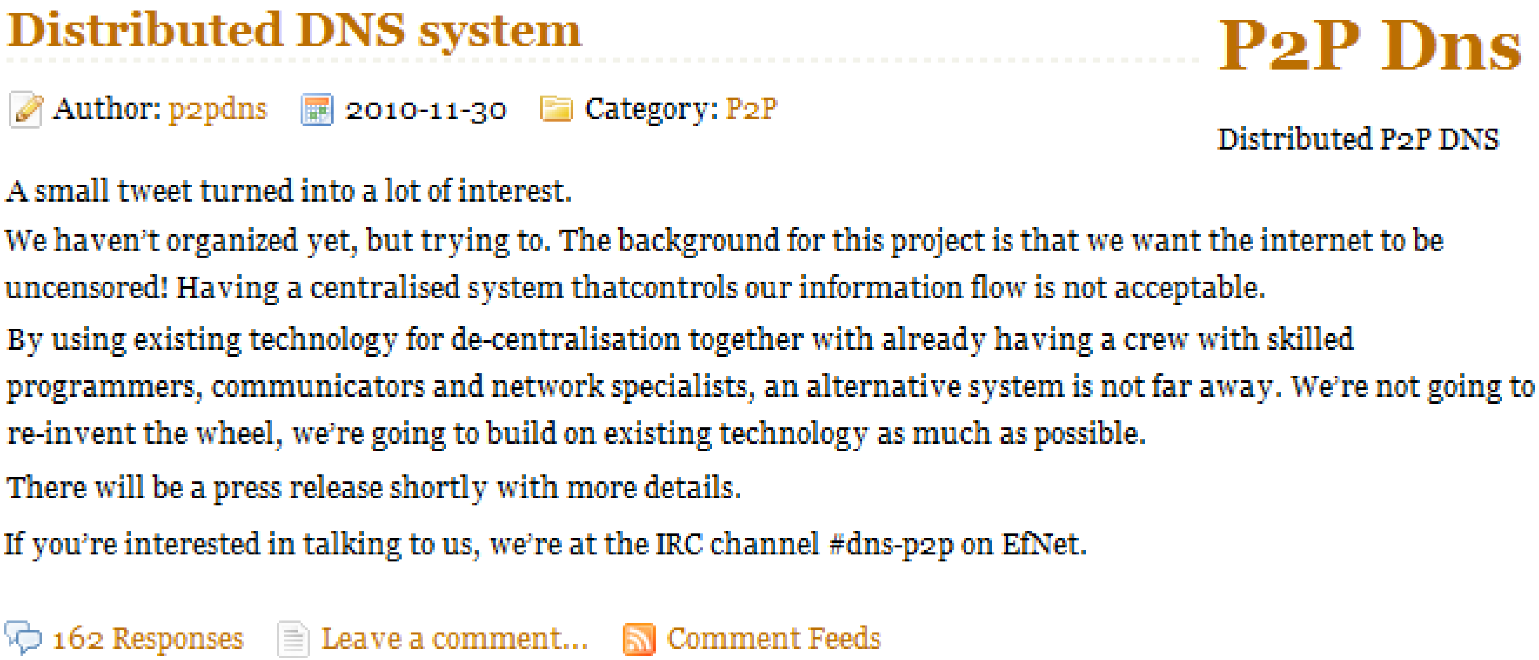
Welcome to OpenNIC

OpenNIC (a.k.a. "The OpenNIC Project") is an organization of hobbyists who run an alternative DNS network. OpenNIC is owned and operated by the OpenNIC community. Membership is open to all who share an interest in keeping DNS free for all users. Our goal is to provide you with quick and reliable DNS services and access to domains not administered by ICANN.

OpenNIC provides resolution to all ICANN domains as well as OpenNIC's own TLDs:

.geek, .free, .bbs, .parody, .oss, .indy, .fur, .ing, .micro, .dyn and .gopher

Some Fixes: P2P DNS



Distributed DNS system

Author: p2pdns   2010-11-30   Category: P2P

A small tweet turned into a lot of interest.

We haven't organized yet, but trying to. The background for this project is that we want the internet to be uncensored! Having a centralised system thatcontrols our information flow is not acceptable.

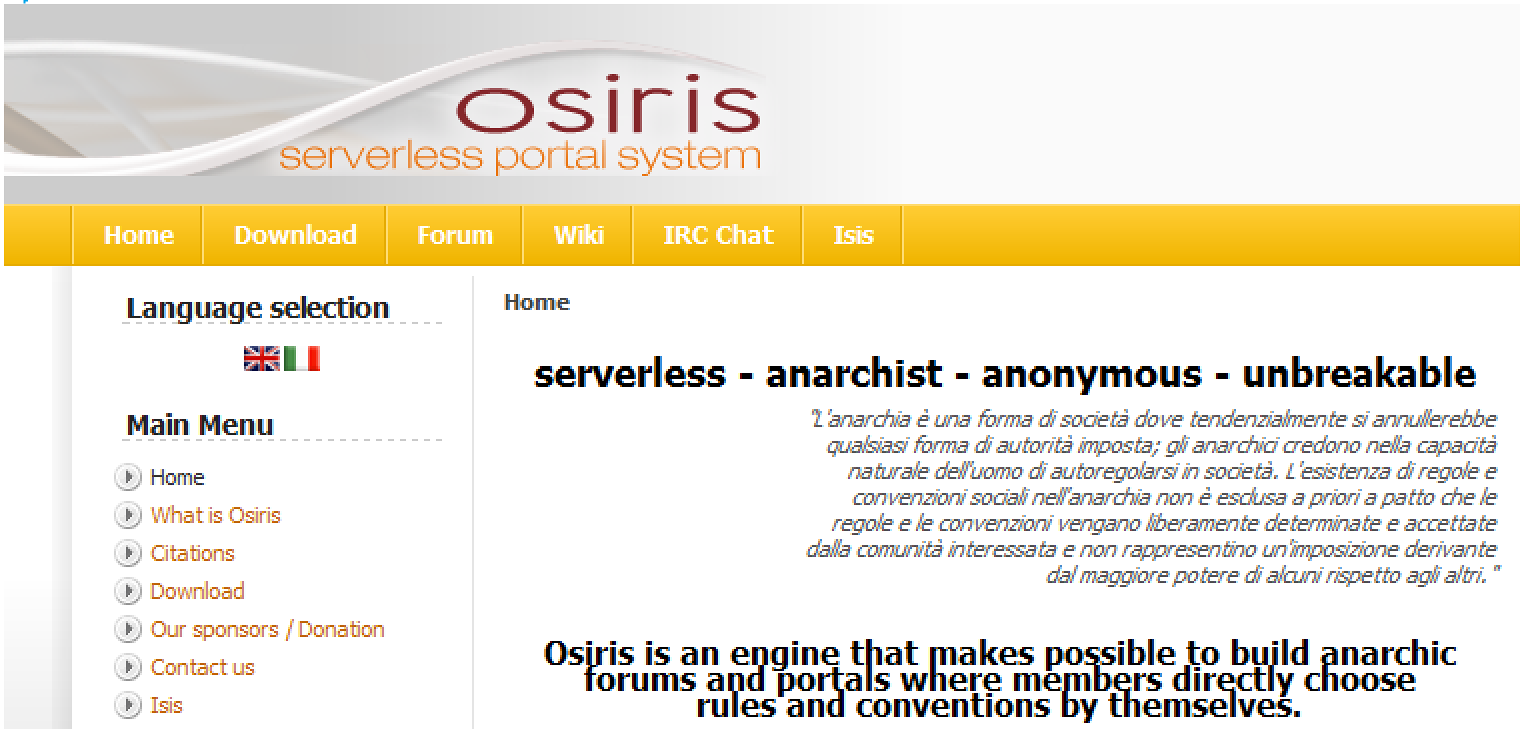
By using existing technology for de-centralisation together with already having a crew with skilled programmers, communicators and network specialists, an alternative system is not far away. We're not going to re-invent the wheel, we're going to build on existing technology as much as possible.

There will be a press release shortly with more details.

If you're interested in talking to us, we're at the IRC channel #dns-p2p on EfNet.

162 Responses   Leave a comment...   Comment Feeds

Workarrounds: OSIRIS CMS

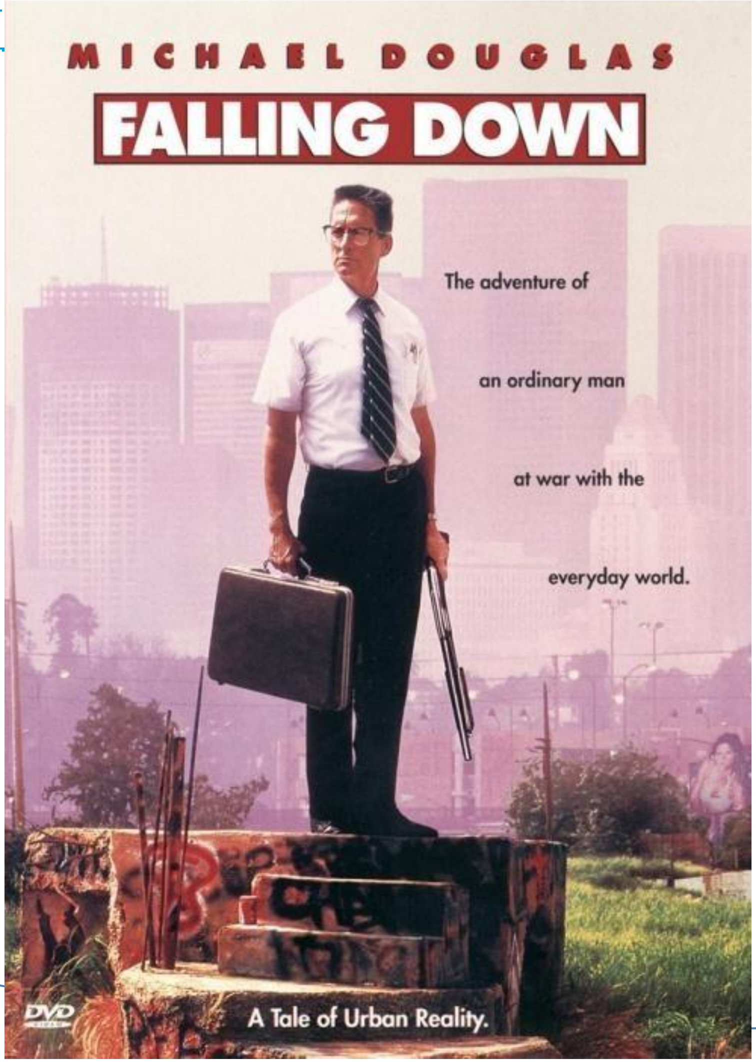


serverless - anarchist - anonymous - unbreakable

"L'anarchia è una forma di società dove tendenzialmente si annullerebbe qualsiasi forma di autorità imposta; gli anarchici credono nella capacità naturale dell'uomo di autoregolarsi in società. L'esistenza di regole e convenzioni sociali nell'anarchia non è esclusa a priori a patto che le regole e le convenzioni vengano liberamente determinate e accettate dalla comunità interessata e non rappresentino un'imposizione derivante dal maggiore potere di alcuni rispetto agli altri."

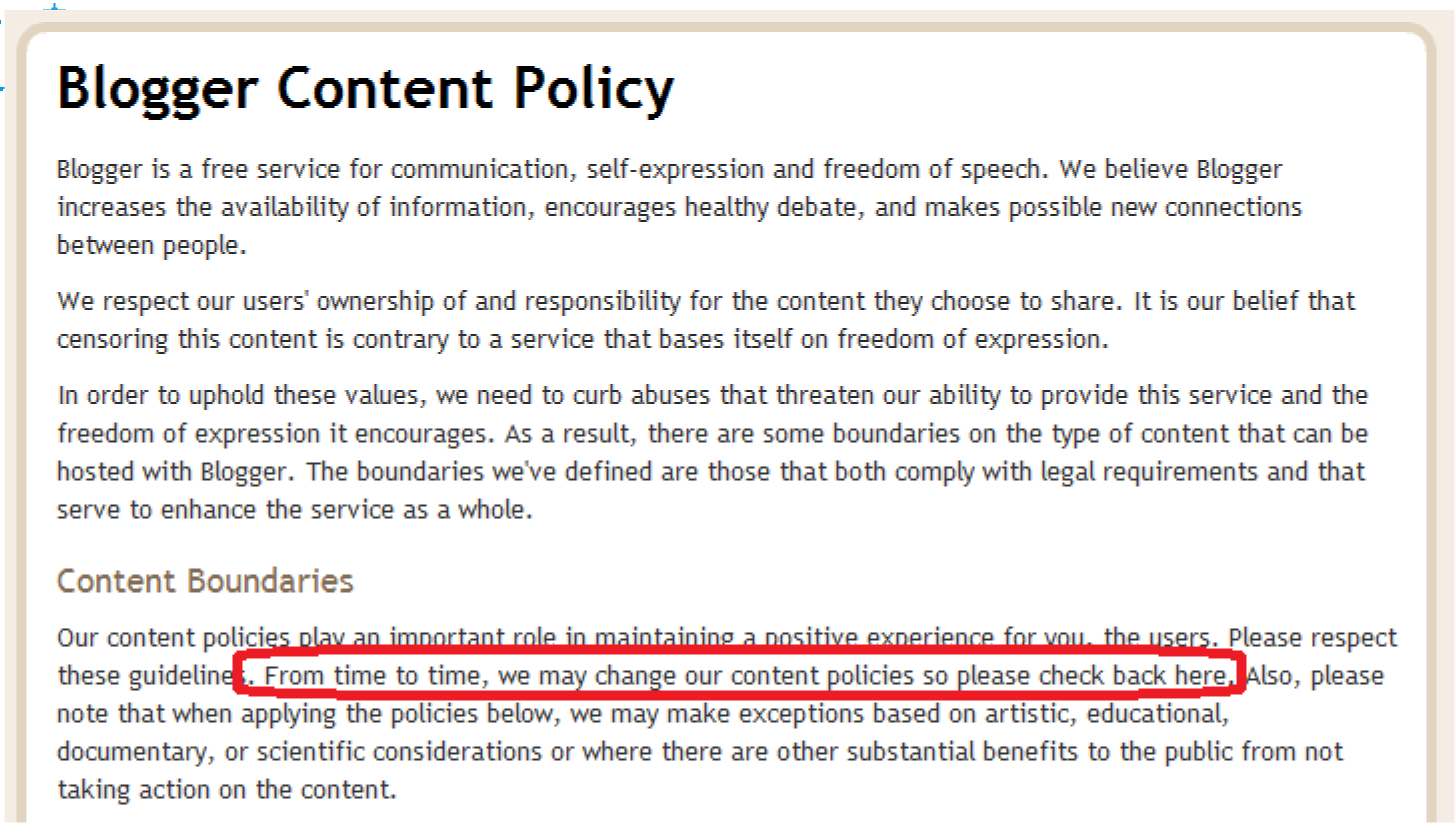
Osiris is an engine that makes possible to build anarchic forums and portals where members directly choose rules and conventions by themselves.

But, what happend if you…



Informática 64

Watch out what you say...



Blogger Content Policy

Blogger is a free service for communication, self-expression and freedom of speech. We believe Blogger increases the availability of information, encourages healthy debate, and makes possible new connections between people.

We respect our users' ownership of and responsibility for the content they choose to share. It is our belief that censoring this content is contrary to a service that bases itself on freedom of expression.

In order to uphold these values, we need to curb abuses that threaten our ability to provide this service and the freedom of expression it encourages. As a result, there are some boundaries on the type of content that can be hosted with Blogger. The boundaries we've defined are those that both comply with legal requirements and that serve to enhance the service as a whole.

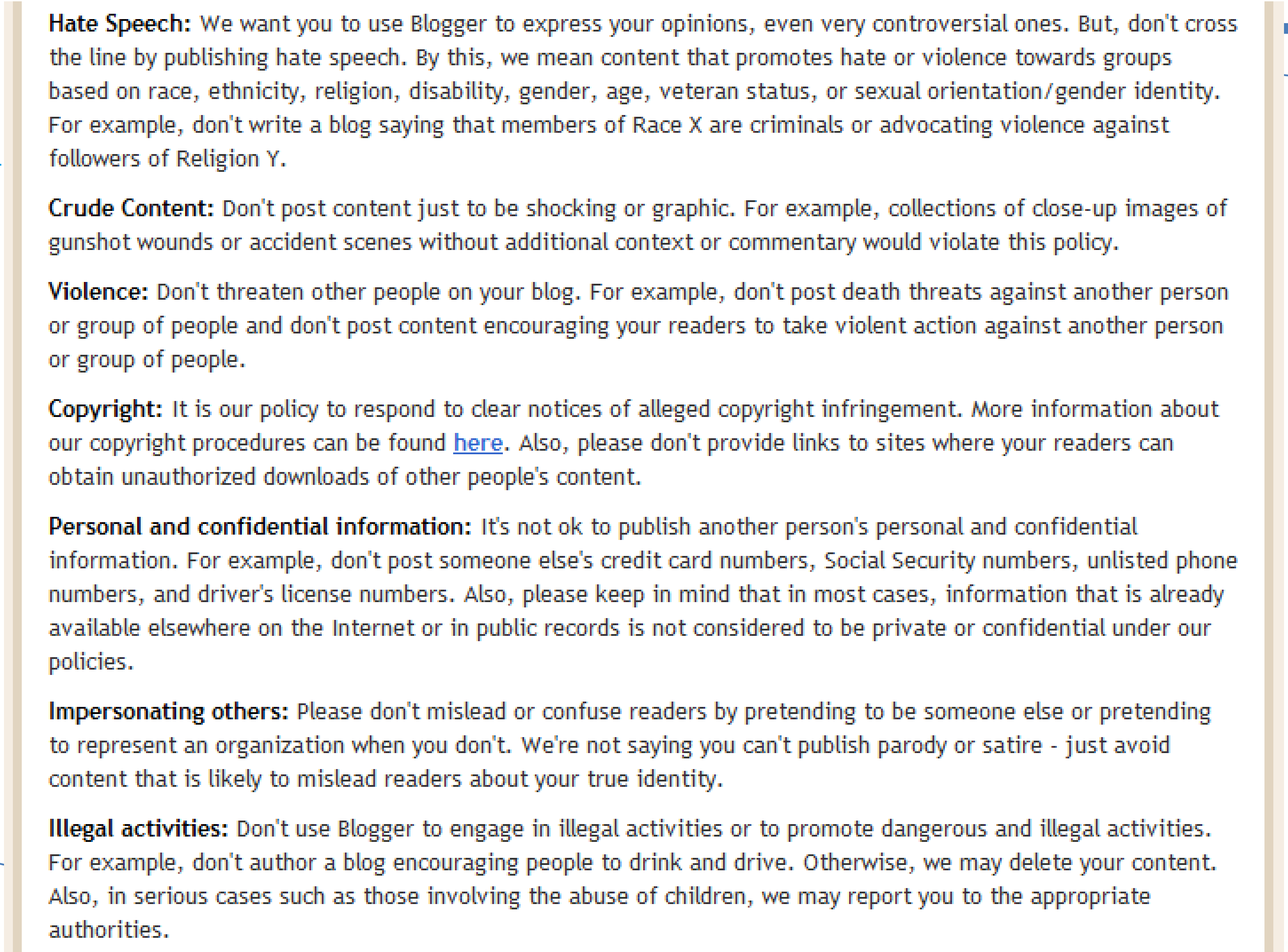
Content Boundaries

Our content policies play an important role in maintaining a positive experience for you, the users. Please respect these guidelines. From time to time, we may change our content policies so please check back here. Also, please note that when applying the policies below, we may make exceptions based on artistic, educational, documentary, or scientific considerations or where there are other substantial benefits to the public from not taking action on the content.

If you have nothing to hide therefore you have nothing to fear

… until we change the policy

Watch out what you say...



Hate Speech: We want you to use Blogger to express your opinions, even very controversial ones. But, don't cross the line by publishing hate speech. By this, we mean content that promotes hate or violence towards groups based on race, ethnicity, religion, disability, gender, age, veteran status, or sexual orientation/gender identity. For example, don't write a blog saying that members of Race X are criminals or advocating violence against followers of Religion Y.

Crude Content: Don't post content just to be shocking or graphic. For example, collections of close-up images of gunshot wounds or accident scenes without additional context or commentary would violate this policy.

Violence: Don't threaten other people on your blog. For example, don't post death threats against another person or group of people and don't post content encouraging your readers to take violent action against another person or group of people.

Copyright: It is our policy to respond to clear notices of alleged copyright infringement. More information about our copyright procedures can be found here. Also, please don't provide links to sites where your readers can obtain unauthorized downloads of other people's content.

Personal and confidential information: It's not ok to publish another person's personal and confidential information. For example, don't post someone else's credit card numbers, Social Security numbers, unlisted phone numbers, and driver's license numbers. Also, please keep in mind that in most cases, information that is already available elsewhere on the Internet or in public records is not considered to be private or confidential under our policies.

Impersonating others: Please don't mislead or confuse readers by pretending to be someone else or pretending to represent an organization when you don't. We're not saying you can't publish parody or satire - just avoid content that is likely to mislead readers about your true identity.

Illegal activities: Don't use Blogger to engage in illegal activities or to promote dangerous and illegal activities. For example, don't author a blog encouraging people to drink and drive. Otherwise, we may delete your content. Also, in serious cases such as those involving the abuse of children, we may report you to the appropriate authorities.

Your RSS is under survilliance

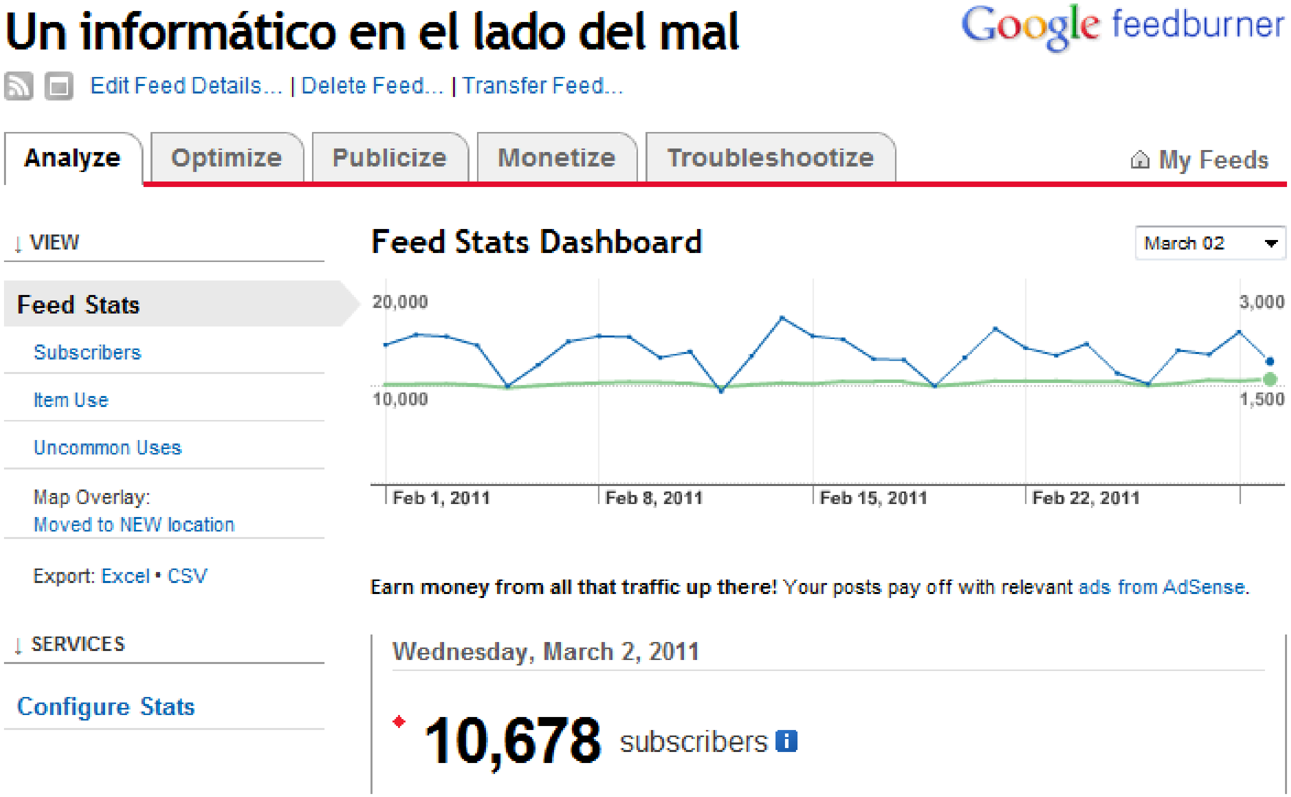
Enjoy but… I am reading your RSS

Informática 64

From blogger to reader

- Domain name
  - Browsing the web
- RSS Suscriptions
  - Readers connected to the XML Feed
- Author?
  - Blogger system account
  - Domain name
  - Http RSS Feed

FeedBurner



Un informático en el lado del mal

Earn money from all that traffic up there! Your posts pay off with relevant ads from AdSense.

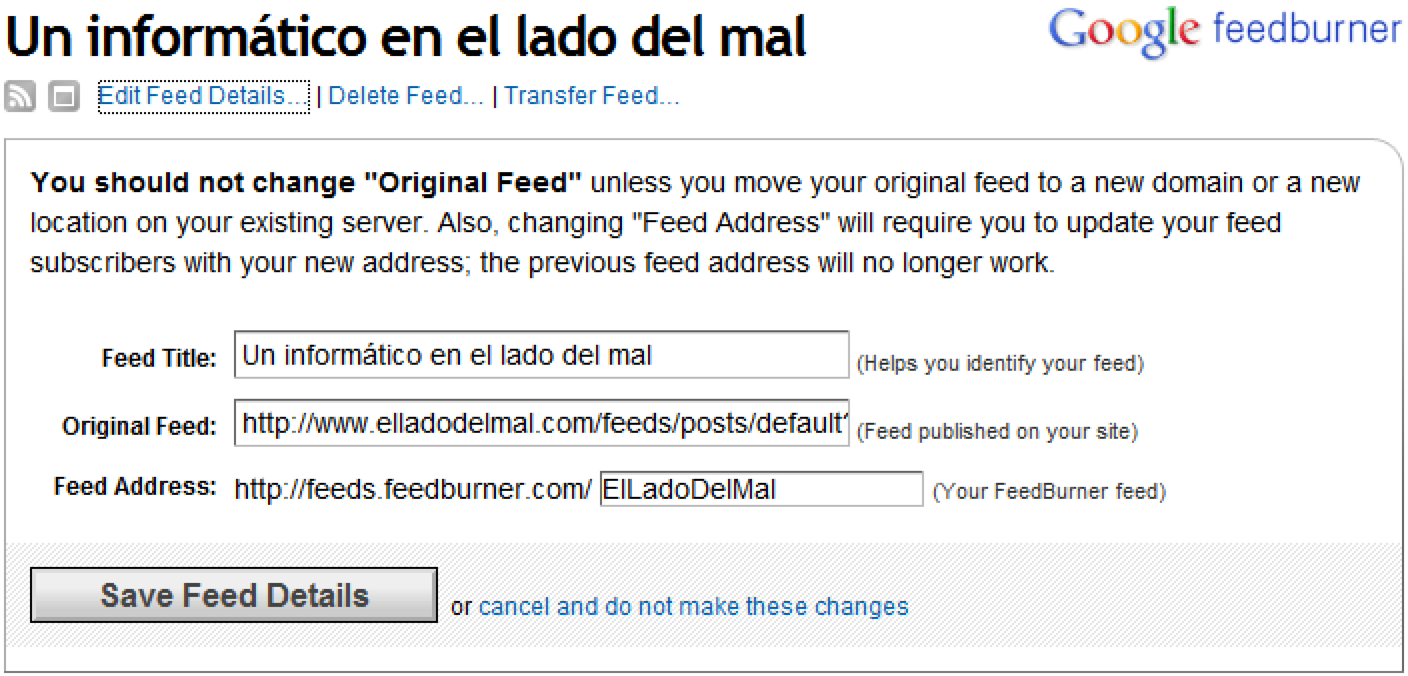
Wednesday, March 2, 2011

10,678 subscribers

Informática 64

It they close your blog?

- If blog is taken down you can change the feed, but if you got the feed with them..



Un informático en el lado del mal

You should not change "Original Feed" unless you move your original feed to a new domain or a new location on your existing server. Also, changing "Feed Address" will require you to update your feed subscribers with your new address; the previous feed address will no longer work.

Feed Title:	Un informático en el lado del mal	(Helps you identify your feed)
Original Feed:	http://www.elladodelmal.com/feeds/posts/default'	(Feed published on your site)
Feed Address:	http://feeds.feedburner.com/ ElLadoDelMal	(Your FeedBurner feed)

Informática 64

Silence… Calm…

Informática 64

DUST: Redundant Feeds by Http & P2P

- RSS Feed PGP-signed by P2P.
- RSS Feeds reader from a source
  - Http (multiple-ones)
  - P2P (multiple-Public PGP Keys)
- Republish of content
  - RSS Feed
  - Just posts or comments

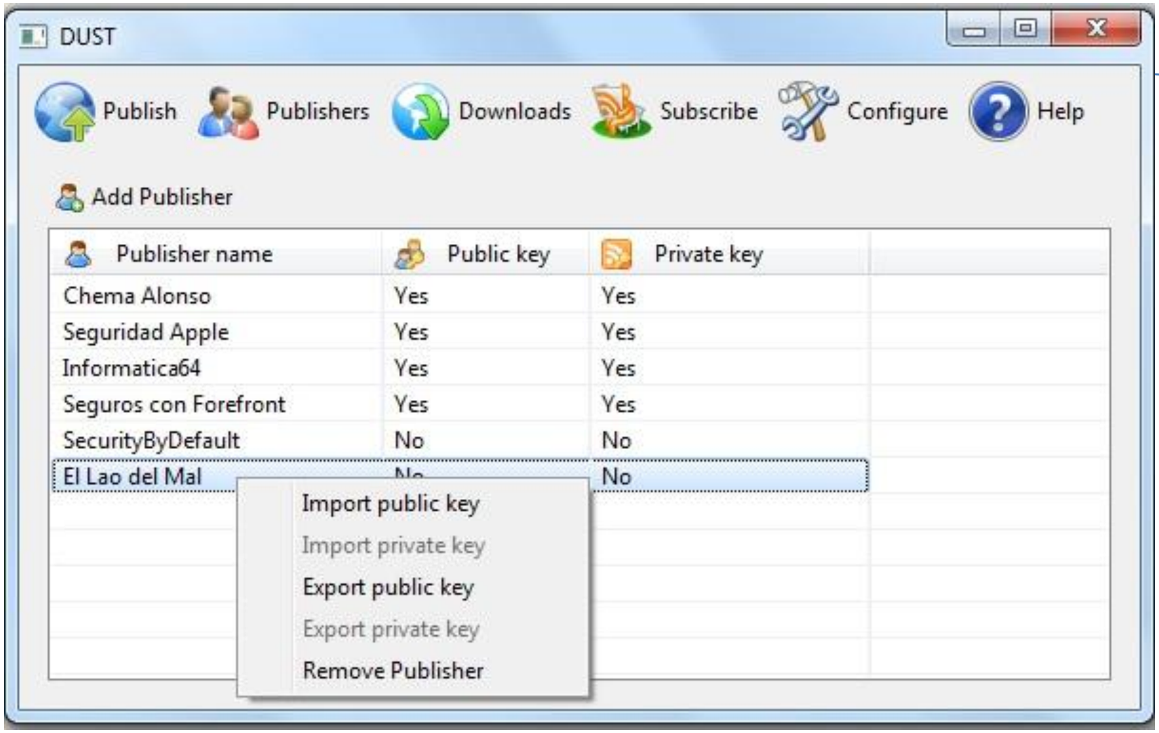
DUST: Redundant Feeds by Http & P2P

- RSS Feeds are PGP-signed
  - From the web
    - To create another communication channel.
    - From Internal severs:
      - your own computer blog system Local files
    - Any XML RSS Feed in disk.
    - Any sent-by-email RSS feed.

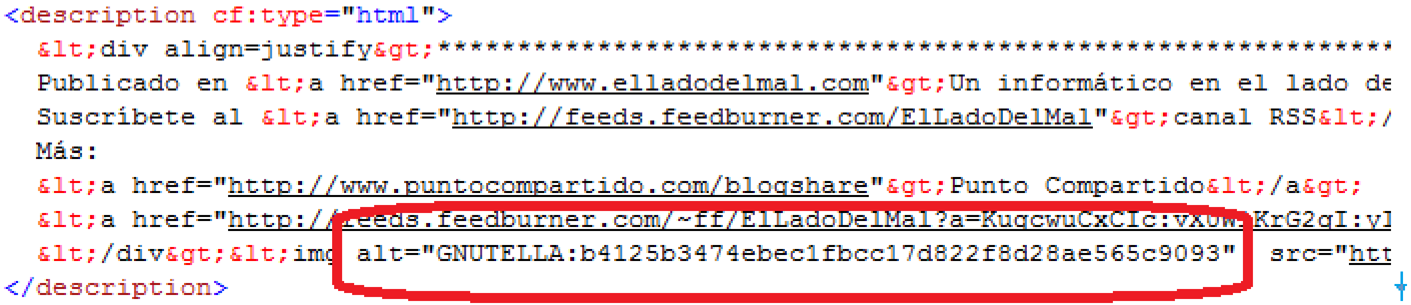
(Not a public IP addres to be DOSed nor a domain name to be closed)

Informática 64

DUST: Redundant Feeds by Http & P2P

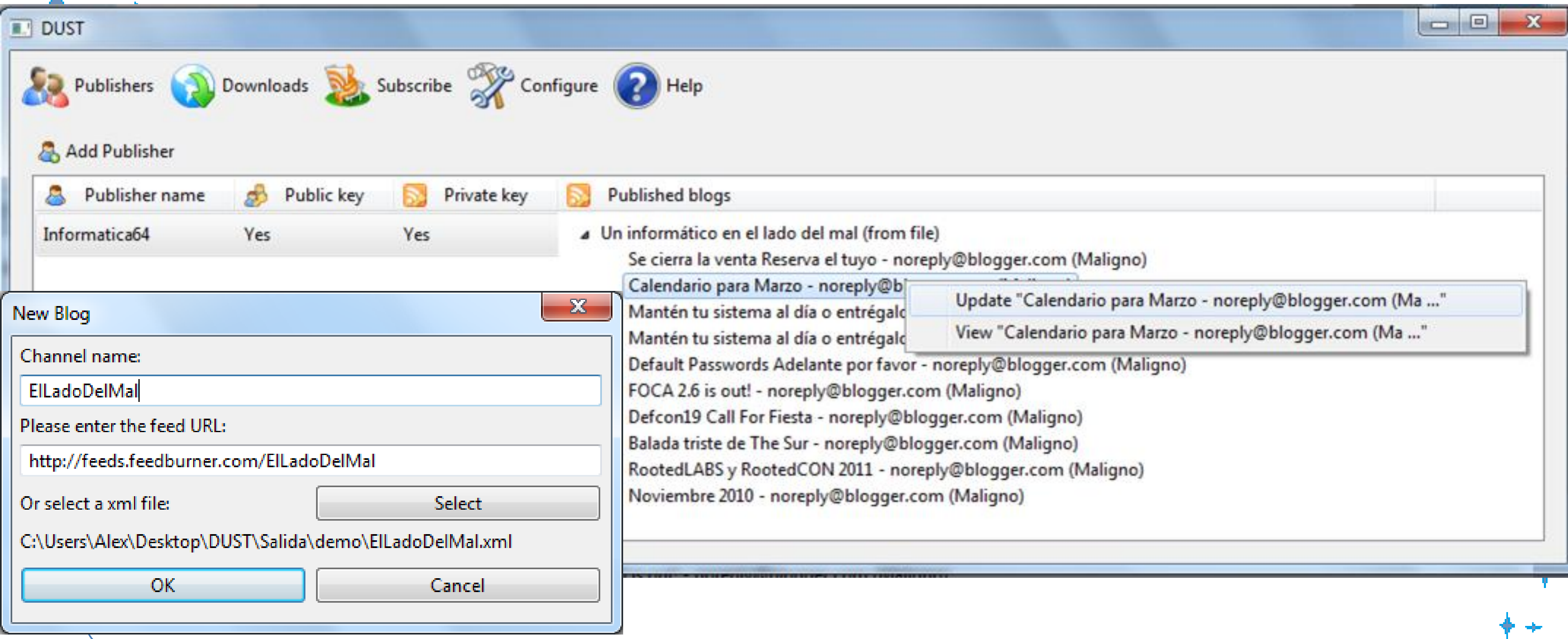


Publisher name	Public key	Private key
Chema Alonso	Yes	Yes
Seguridad Apple	Yes	Yes
Informatica64	Yes	Yes
Seguros con Forefront	Yes	Yes
SecurityByDefault	No	No
El Lao del Mal	No	No



```
<description cf:type="html">
  &lt;div align=justify&gt;************************************************************
  Publicado en &lt;a href="http://www.elladodelmal.com"&gt;Un informático en el lado de
  Suscríbete al &lt;a href="http://feeds.feedburner.com/ElLadoDelMal"&gt;canal RSS&lt;/
  Más:
  &lt;a href="http://www.puntocompartido.com/blogshare"&gt;Punto Compartido&lt;/a&gt;
  &lt;a href="http://feeds.feedburner.com/~ff/ElLadoDelMal?a=KugcwuCxCIc:vx0w-KrG2qI:yI
  &lt;/div&gt;&lt;img alt="GNUTELLA:b4125b3474ebec1fbcc17d822f8d28ae565c9093"  src="htt
</description>
```

DUST: Redundant Feeds by Http & P2P



Publisher name	Public key	Private key
Informatica64	Yes	Yes

Published blogs

- Un informático en el lado del mal (from file)
  - Se cierra la venta Reserva el tuyo - noreply@blogger.com (Maligno)
  - Calendario para Marzo - noreply@b
  - Mantén tu sistema al día o entrégal
  - Mantén tu sistema al día o entrégal
  - Default Passwords Adelante por favor - noreply@blogger.com (Maligno)
  - FOCA 2.6 is out! - noreply@blogger.com (Maligno)
  - Defcon19 Call For Fiesta - noreply@blogger.com (Maligno)
  - Balada triste de The Sur - noreply@blogger.com (Maligno)
  - RootedLABS y RootedCON 2011 - noreply@blogger.com (Maligno)
  - Noviembre 2010 - noreply@blogger.com (Maligno)

Update "Calendario para Marzo - noreply@blogger.com (Ma ..."

View "Calendario para Marzo - noreply@blogger.com (Ma ..."

Channel name: ElLadoDelMal

Please enter the feed URL: http://feeds.feedburner.com/ElLadoDelMal

Or select a xml file:

C:\Users\Alex\Desktop\DUST\Salida\demo\ElLadoDelMal.xml

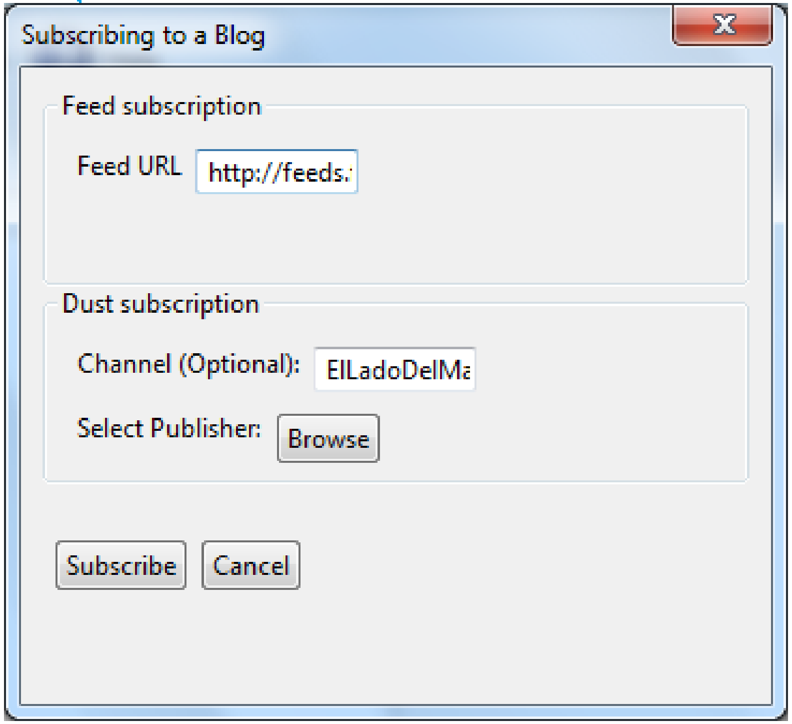
DUST: Redundant Feeds by Http & P2P

- Feed is distributed by P2P networks
  - POC: Right now only in GNUTella (serveless)
- Different methods
  - Feed RSS with linked pgp-signed files
  - Feed RSS with embbeded files
  - Only posts with embbeded dfiles

DUST: Redundant Feeds by Http & P2P

- Anyone can re-publish the RSS Feed
- Anyone can re-publish posts
- Anyone can follow a chanel of a PGP Key
- Everybody shares downladed feeds
- Anyone can re-sign the information
    - Multiple files (File Pollution)

DUST: Subscripción a Feeds RSS



Subscribing to a Blog

Feed subscription

Feed URL: http://feeds.

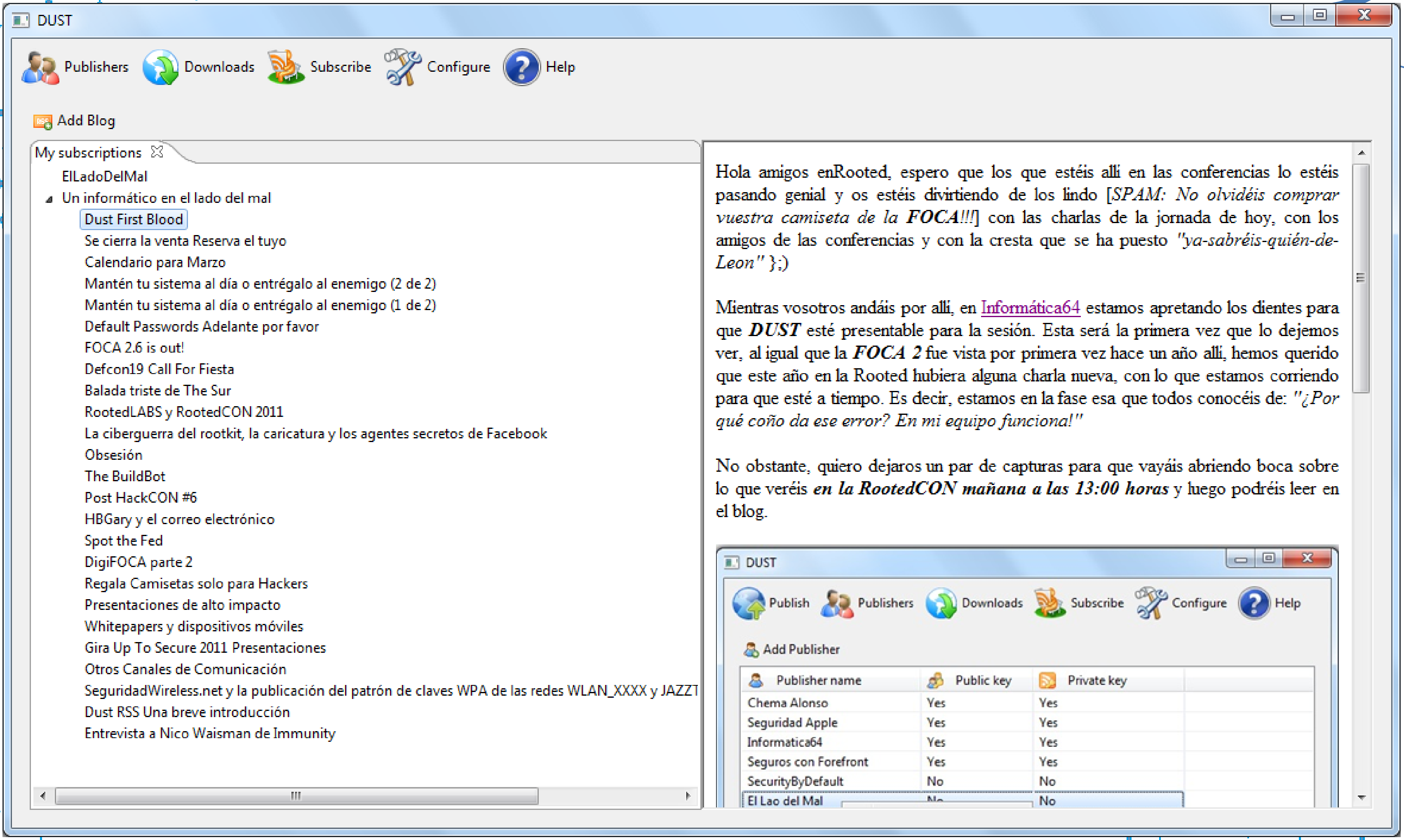
Dust subscription

Channel (Optional): ElLadoDelMa

Select Publisher:

- HTTP Suscription
- DUST Suscription
  - A clave PGP
  - A clave y Canal

DUST: RSS Feeds Reader



ElLadoDelMal
- Un informático en el lado del mal
  - Dust First Blood
  - Se cierra la venta Reserva el tuyo
  - Calendario para Marzo
  - Mantén tu sistema al día o entrégalo al enemigo (2 de 2)
  - Mantén tu sistema al día o entrégalo al enemigo (1 de 2)
  - Default Passwords Adelante por favor
  - FOCA 2.6 is out!
  - Defcon19 Call For Fiesta
  - Balada triste de The Sur
  - RootedLABS y RootedCON 2011
  - La ciberguerra del rootkit, la caricatura y los agentes secretos de Facebook
  - Obsesión
  - The BuildBot
  - Post HackCON #6
  - HBGary y el correo electrónico
  - Spot the Fed
  - DigiFOCA parte 2
  - Regala Camisetas solo para Hackers
  - Presentaciones de alto impacto
  - Whitepapers y dispositivos móviles
  - Gira Up To Secure 2011 Presentaciones
  - Otros Canales de Comunicación
  - SeguridadWireless.net y la publicación del patrón de claves WPA de las redes WLAN_XXXX y JAZZT
  - Dust RSS Una breve introducción
  - Entrevista a Nico Waisman de Immunity

Hola amigos enRooted, espero que los que estéis allí en las conferencias lo estéis pasando genial y os estéis divirtiendo de los lindo [*SPAM: No olvidéis comprar vuestra camiseta de la **FOCA**!!!*] con las charlas de la jornada de hoy, con los amigos de las conferencias y con la cresta que se ha puesto *"ya-sabréis-quién-de-Leon"* };)

Mientras vosotros andáis por allí, en Informática64 estamos apretando los dientes para que ***DUST*** esté presentable para la sesión. Esta será la primera vez que lo dejemos ver, al igual que la ***FOCA 2*** fue vista por primera vez hace un año allí, hemos querido que este año en la Rooted hubiera alguna charla nueva, con lo que estamos corriendo para que esté a tiempo. Es decir, estamos en la fase esa que todos conocéis de: *"¿Por qué coño da ese error? En mi equipo funciona!"*

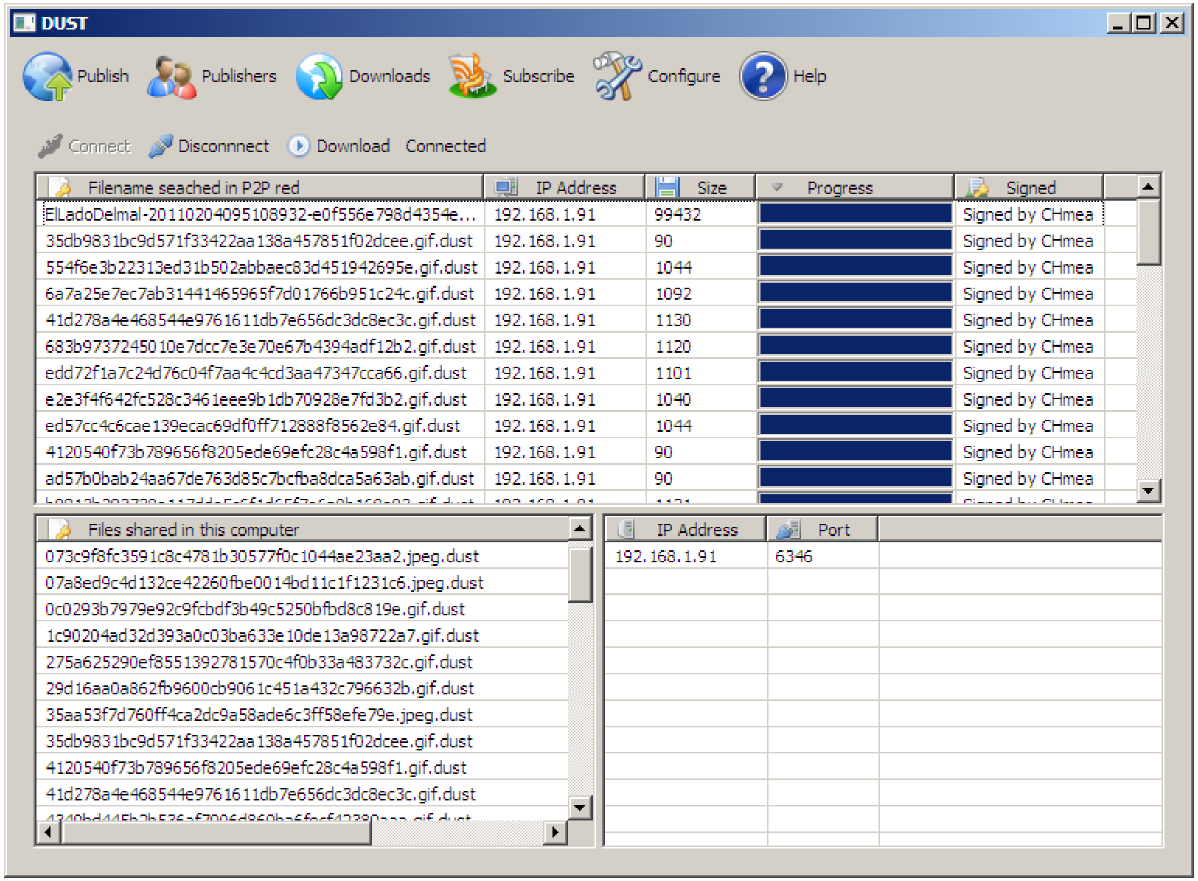
No obstante, quiero dejaros un par de capturas para que vayáis abriendo boca sobre lo que veréis ***en la RootedCON mañana a las 13:00 horas*** y luego podréis leer en el blog.

Publisher name	Public key	Private key
Chema Alonso	Yes	Yes
Seguridad Apple	Yes	Yes
Informatica64	Yes	Yes
Seguros con Forefront	Yes	Yes
SecurityByDefault	No	No
El Lao del Mal	No	No

DUST

- Automaticly detect redundant sources y the XML file of the RSS Feed:
  - HTTP -> New URL to download copies.
  - DUST -> New P2P/PGP channel
- Automaticly import sources from Google Reader
  - Easy to migrate

DUST: Meanwhile …under the hood



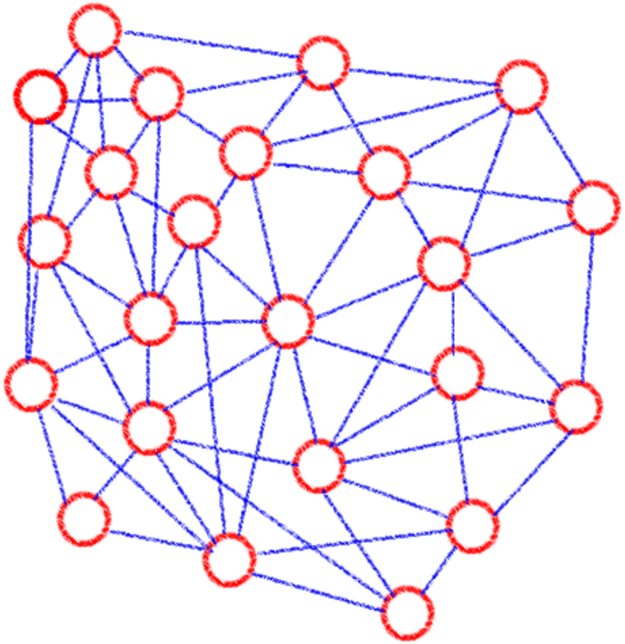
Filename seached in P2P red	IP Address	Size	Progress	Signed
ElLadoDelmal-20110204095108932-e0f556e798d4354e...	192.168.1.91	99432	█	Signed by CHmea
35db9831bc9d571f33422aa138a457851f02dcee.gif.dust	192.168.1.91	90	█	Signed by CHmea
554f6e3b22313ed31b502abbaec83d451942695e.gif.dust	192.168.1.91	1044	█	Signed by CHmea
6a7a25e7ec7ab31441465965f7d01766b951c24c.gif.dust	192.168.1.91	1092	█	Signed by CHmea
41d278a4e468544e9761611db7e656dc3dc8ec3c.gif.dust	192.168.1.91	1130	█	Signed by CHmea
683b97372450 10e7dcc7e3e70e67b4394adf12b2.gif.dust	192.168.1.91	1120	█	Signed by CHmea
edd72f1a7c24d76c04f7aa4c4cd3aa47347cca66.gif.dust	192.168.1.91	1101	█	Signed by CHmea
e2e3f4f642fc528c3461eee9b1db70928e7fd3b2.gif.dust	192.168.1.91	1040	█	Signed by CHmea
ed57cc4c6cae139ecac69df0ff712888f8562e84.gif.dust	192.168.1.91	1044	█	Signed by CHmea
4120540f73b789656f8205ede69efc28c4a598f1.gif.dust	192.168.1.91	90	█	Signed by CHmea
ad57b0bab24aa67de763d85c7bcfba8dca5a63ab.gif.dust	192.168.1.91	90	█	Signed by CHmea

Files shared in this computer
073c9f8fc3591c8c4781b30577f0c1044ae23aa2.jpeg.dust
07a8ed9c4d132ce42260fbe0014bd11c1f1231c6.jpeg.dust
0c0293b7979e92c9fcbdf3b49c5250bfbd8c819e.gif.dust
1c90204ad32d393a0c03ba633e10de13a98722a7.gif.dust
275a625290ef8551392781570c4f0b33a483732c.gif.dust
29d16aa0a862fb9600cb9061c451a432c796632b.gif.dust
35aa53f7d760ff4ca2dc9a58ade6c3ff58efe79e.jpeg.dust
35db9831bc9d571f33422aa138a457851f02dcee.gif.dust
4120540f73b789656f8205ede69efc28c4a598f1.gif.dust
41d278a4e468544e9761611db7e656dc3dc8ec3c.gif.dust

IP Address	Port
192.168.1.91	6346

DUST: under the hood

- P2P connections
- Seraching using GNUTella
  - SHA1(Public PGP)
  - Channels/PGP
    - Size limits
    - PGP checks
    - If rogue node then jump!
- XML files are server vía Http
- Port configuration
- Shares all downaladed feeds



Informática 64

Demo

DUST is in beta, but needs users

- Let´s do something cool for social-media-victims…

fuckbook

Boobble™

The Adult Search Engine

DUST: Services

- Send us your PGP-signed RSS feed and we republish it on P2P network
- Read a feed, and share it vía DUST
- Dust is in Java, help us to improve it.
- Open Source
- Let´s contol our channels…

Gracias!

- Chema Alonso
- Alejandro Martín
- David Luengo
- Ignacio Briones
- Alejandro «para» Nolla