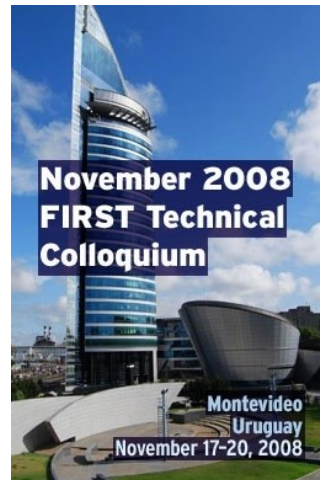


Nuevas Amenazas: *Fast Flux Service Networks*



Carlos Marcelo Martínez
FIRST TC
Montevideo, Uruguay
Noviembre de 2008

Plan de la Presentación

- Amenazas en el Web
- (Brevísima) Introducción al DNS
- (Brevísima) Introducción a las Botnets
- *Fast Flux Service Networks*
- Conclusiones
- Referencias

Amenazas en la Web

Security - eWeek

eWEEK.COM

SUBSCRIBE TO eWEEK RSS

HOME NEWS REVIEWS DATA STORAGE SECURITY DESKTOPS/NO

Security News | Security Reviews | Security Blogs | IT Infrastructure | G

Home ▶ Security ▶ Web Threats Keep Users Away

LATEST STORIES

- The New Washington Tech Agenda
- Standards Come to Anti-malware Testing
- Pirates of the Caribbean: The Cyber-crime Ed...
- SpringSource Gains Momentum in Enterprise Ja...
- How to Improve Sales Forecasting



Shell Security - Seguridad informática

NOTICIAS DIARIAS DE SEGURIDAD INFORMÁTICA, FOROS, VULNERABILIDADES, ANTI-MALWARE, DOCUMENTACIÓN, AUDITORÍAS, C

Alerta de un phishing que simula una devolución fiscal de la Agencia Tributaria

Febrero 01, 07 by admin

Estos días hemos recibido diversos emails que contienen un **ataque de phishing que utiliza de forma dinámica las imágenes e incluso las noticias de la página oficial de la Agencia Tributaria para apropiarse ilegalmente de claves de tarjetas bancarias y datos personales.**

El asunto del correo trampa "Devolución Fiscal"
Su contenido simula la devolución fiscal de 90 Euros.

Security

Web Threats Keep Users Away

By Matt Hines
2005-10-26

Article V...
Article R...

New re:
users a
online l
identity
Web-or



Hardware Software Music & Media Comms Security Management Sci

Crime | Enterprise Security | Anti-Virus | Spam | ID | Spyware

[The Register](#) » [Security](#) » [Spam](#) »

The illicit trade in compromised PCs

New re: Zombie army

WebW: By [John Leyden](#) → [More by this author](#)

cutting Published Friday 30th April 2004 14:43 GMT

shunnir [Find your perfect job - click here from thousands of tech vacancies](#)

out per
rising ti

Information Security 2004 Investigators are piecing together the complex relations virus writers, middlemen and criminal gangs held largely responsible for the growth of months.

Amenazas en la Web (2)

- Algunas amenazas...
 - Envío de correo electrónico no solicitado (*spam*)
 - Ataques de denegación de servicio distribuidos
 - *Phishing*
 - Instalación de “*adware*”
 - “*Sniffing*” de tráfico
 - “*Keylogging*”
 - Guardar las “teclas” pulsadas por el usuario y enviar esa información al “*bot herder*”
 - “*Click Fraud*”
 - Generación de clicks fraudulentos a herramientas de promoción en Internet (Google, Yahoo)
- **En general [el atacante] necesita alguna infraestructura**
 - Páginas de log in; agentes de recolección de datos; envíos de correo masivos



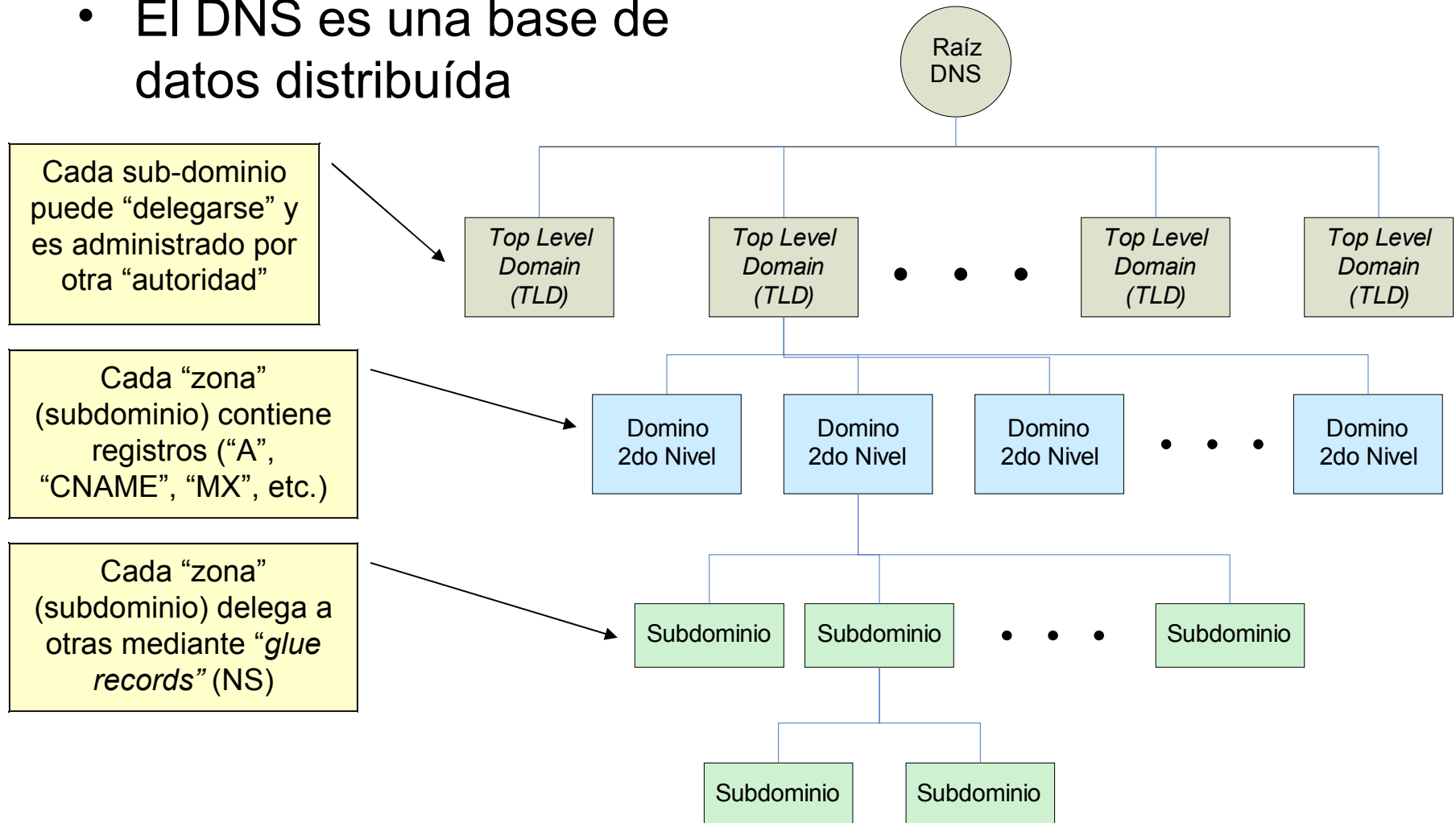
Introducción al DNS

Introducción al DNS

- DNS: Domain Name System
- Propósito básico:
 - Traducir números IP en nombres textuales mas amigables para los usuarios “humanos” de la red
- Propósitos adicionales:
 - Soporte a diferentes servicios a dar sobre la red (directorío de servicios)
 - Ejemplo: Correo electrónico
 - Sub-delegaciones de nombres
 - Zonas, autoridad
 - Resolución reversa
 - Reverso: correspondencia nombre -> número IP

Introducción al DNS

- El DNS es una base de datos distribuida



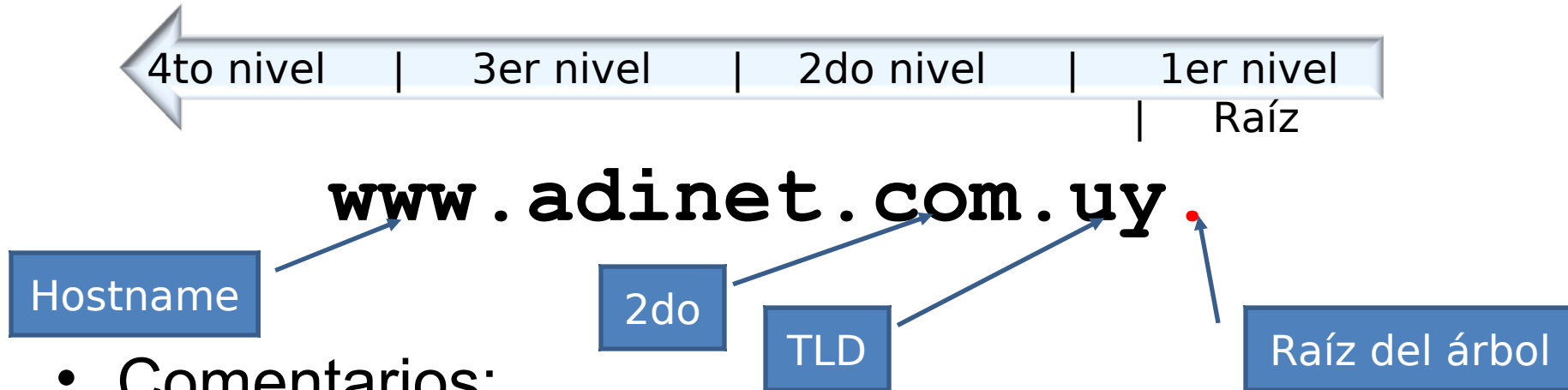
Introducción al DNS

- Base de datos distribuída
 - Operaciones de *lookup*
 - Distribución -> *delegación*
 - Zonas
 - Autoridad
- Estructura de árbol
 - *Si no tengo autoridad, puedo delegar*



Introducción al DNS

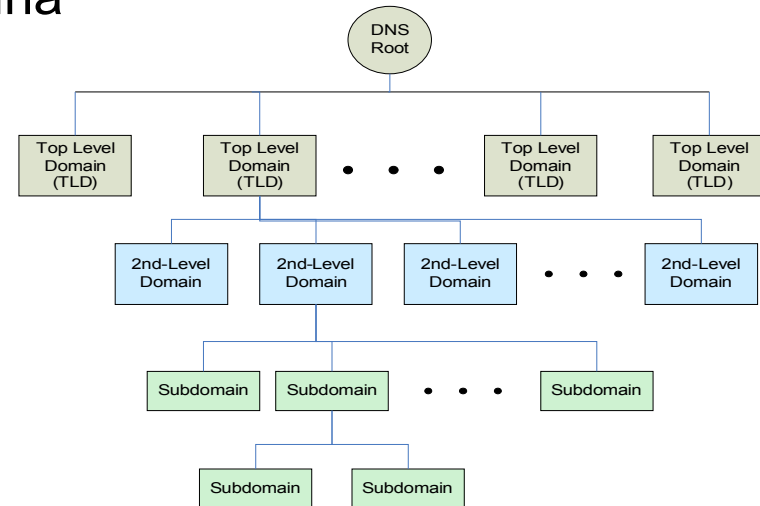
- Estructura de los nombres de dominio:



- Comentarios:
 - Los niveles del árbol reflejan las divisiones administrativas
 - El *root* del árbol esta siempre presente de forma implícita
 - No hay restricciones a la cantidad de niveles
 - Los niveles superiores “**delegan**” hacia los inferiores

Conceptos básicos

- Zonas
 - A cada dominio (*incluyendo también al root*) le corresponde lo que se denomina una *zona* de DNS
 - Cada zona agrupa un conjunto de *resource records*
- Recursión
 - Consultas a otros servidores
- Round-Robin DNS
 - Cuando hay múltiples registros, las respuestas varían el orden de los mismos
 - Balance de carga
- *Time-to-Live*
 - Los resultados de las consultas se almacenan en caché durante un cierto tiempo



Conceptos básicos: *Resource Records*

- RR “A”: *Address*
 - Los registros A establecen las correspondencias entre direcciones IP y nombres de dominio
- RR “NS” : *Name Server*
 - Establece un punto de delegación, donde la autoridad sobre un cierto subdominio es cedida a otro servidor DNS
 - Llamados “*glue records*”
- RR “CNAME”: *Canonical Name*
 - Son el equivalente de los alias o de los links simbólicos.
 - Establecen una correspondencia entre dos nombres
 - En teoría para resolver completamente a la dirección hacen falta dos consultas
 - En la práctica los servidores ya devuelven el “A” correspondiente en la sección *Additional* de la consulta (ya lo vamos a ver)

Conceptos básicos: DNS Round Robin

- Técnica empleada para:

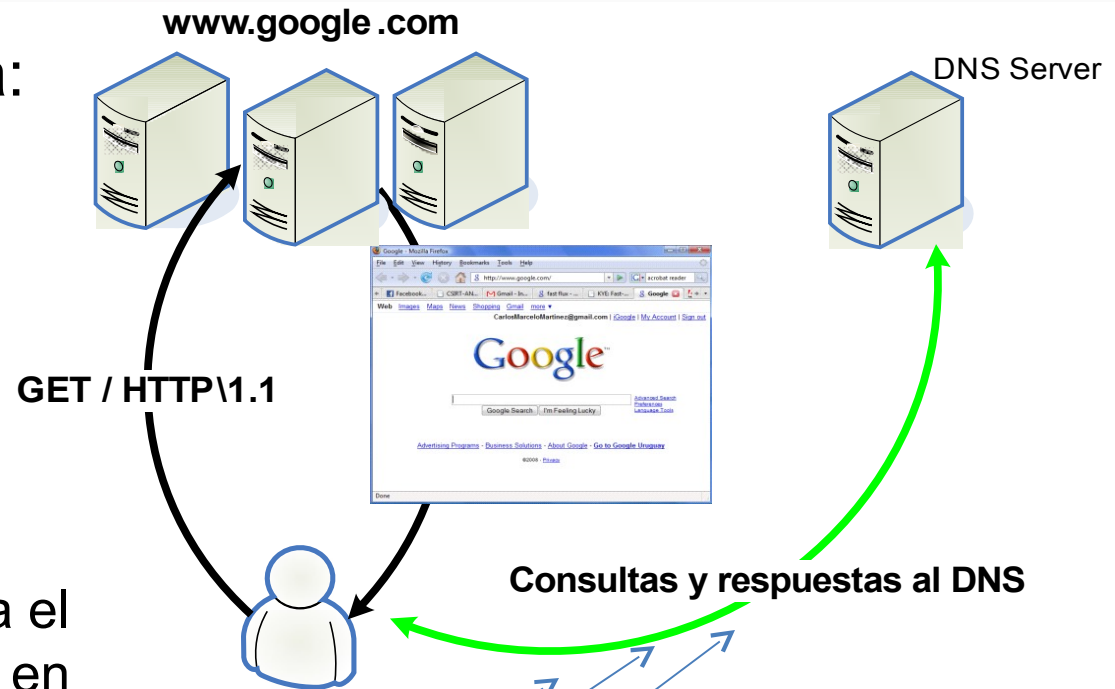
- Balanceo de carga
- Tolerancia a fallas

- Concepto:

- Una consulta por un nombre devuelve varios registros
- El servidor DNS permuta el orden de estos registros en respuestas siguientes

- Problemas:

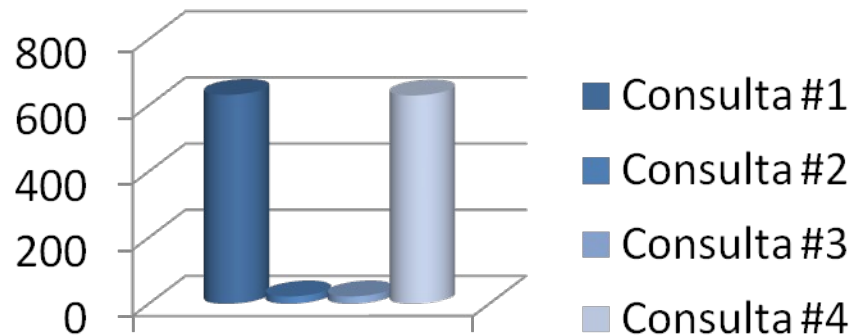
- Falta de *feedback* de servicios a DNS
- Tiempo de reacción limitado por TTL de los registros



www.google.com	IN A	10.11.20.21
www.google.com	IN A	1.2.3.4
www.google.com	IN A	50.55.60.65
www.google.com	IN A	10.11.20.21
www.google.com	IN A	1.2.3.4
www.google.com	IN A	4.5.6.7

Conceptos básicos: *Time-to-Live*

- Cada consulta al DNS es “costosa”
 - Consulta a servidores remotos
 - Consultas recursiva
- Los resultados se almacenan en *caché* local
- ¿Por cuánto tiempo?
Time-to-Live
- Típicamente
 - 86400 segundos (1 día)



IN A www.google.com ?

Conceptos básicos

- Registros (*Resource Records*)
 - La información en la base de datos del DNS de cada zona está estructurada en un conjunto de *resource records*:
 - SOA, A, NS, MX, PTR, TXT, etc.
 - Cada RR representa un ítem de información en la base de datos de DNS que puede ser consultado
- SOA: “*Start of Authority*”
 - Delimita una zona
 - Campos
 - **RETRY:**
 - tiempo a esperar para reintentar una transferencia fallida
 - **EXPIRE:**
 - tiempo a esperar hasta considerar la zona no autoritativa
 - **MINIMUM:**
 - TTL mínimo que se exporta con cualquier RR que se responde sobre esta zona

SOA:
adinet.com.uy

IN A
IN A
IN MX ...



Introducción a las Botnets

Introducción a las Botnets

- **BotNet** : Robot Network
 - Conjunto de sistemas comprometidos, bajo el comando de una entidad central
 - *Bot Herder*
- Una “botnet” está formada por un conjunto de sistemas comprometidos y bajo el control de un operador central
- En cada sistema comprometido hay instalado alguna forma de malware que permite al operador controlarlo

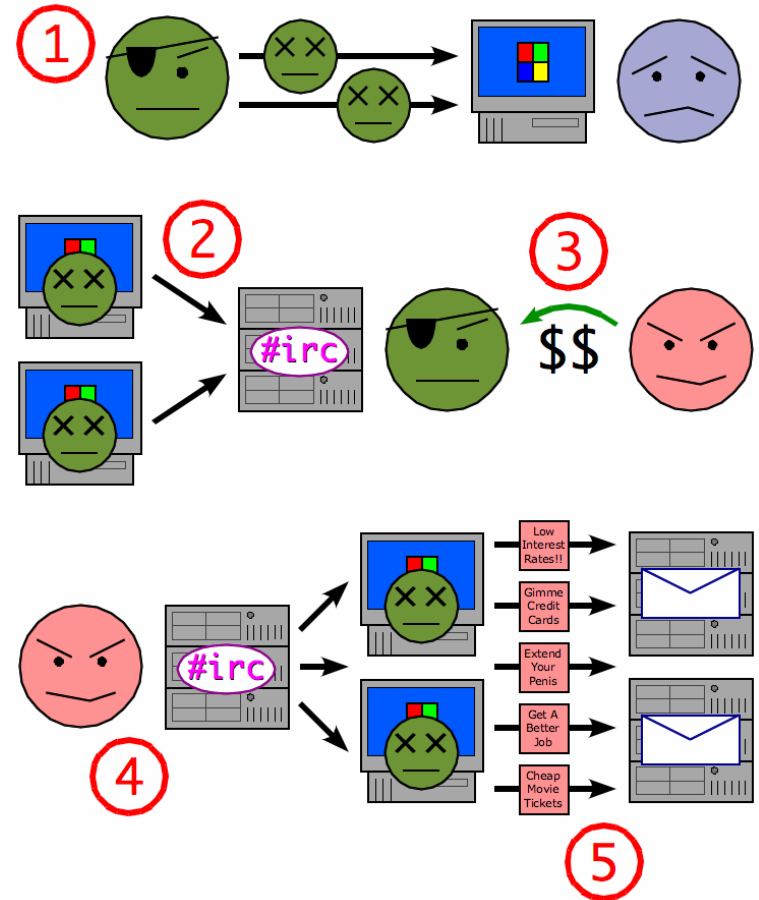
Botnets: Ciclo de Vida

- *Herding*
 - Fase de crecimiento de la botnet
 - Ciclo de infección y agregado de nuevos bots
 - Cada nuevo bot
 - Un PC es infectado o instala algún tipo de troyano
 - Búsqueda de blancos “cercaños” para propagar el bot
 - El bot levanta un canal de comando y control (C&C)
 - IRC
- Equilibrio
 - La red no crece “activamente” pero si hay una permanente “lucha” entre malwares y hay bajas y altas en la misma
- Utilización
 - Ingresa al “mercado” para su uso

Introducción a las Botnets

- Botnets

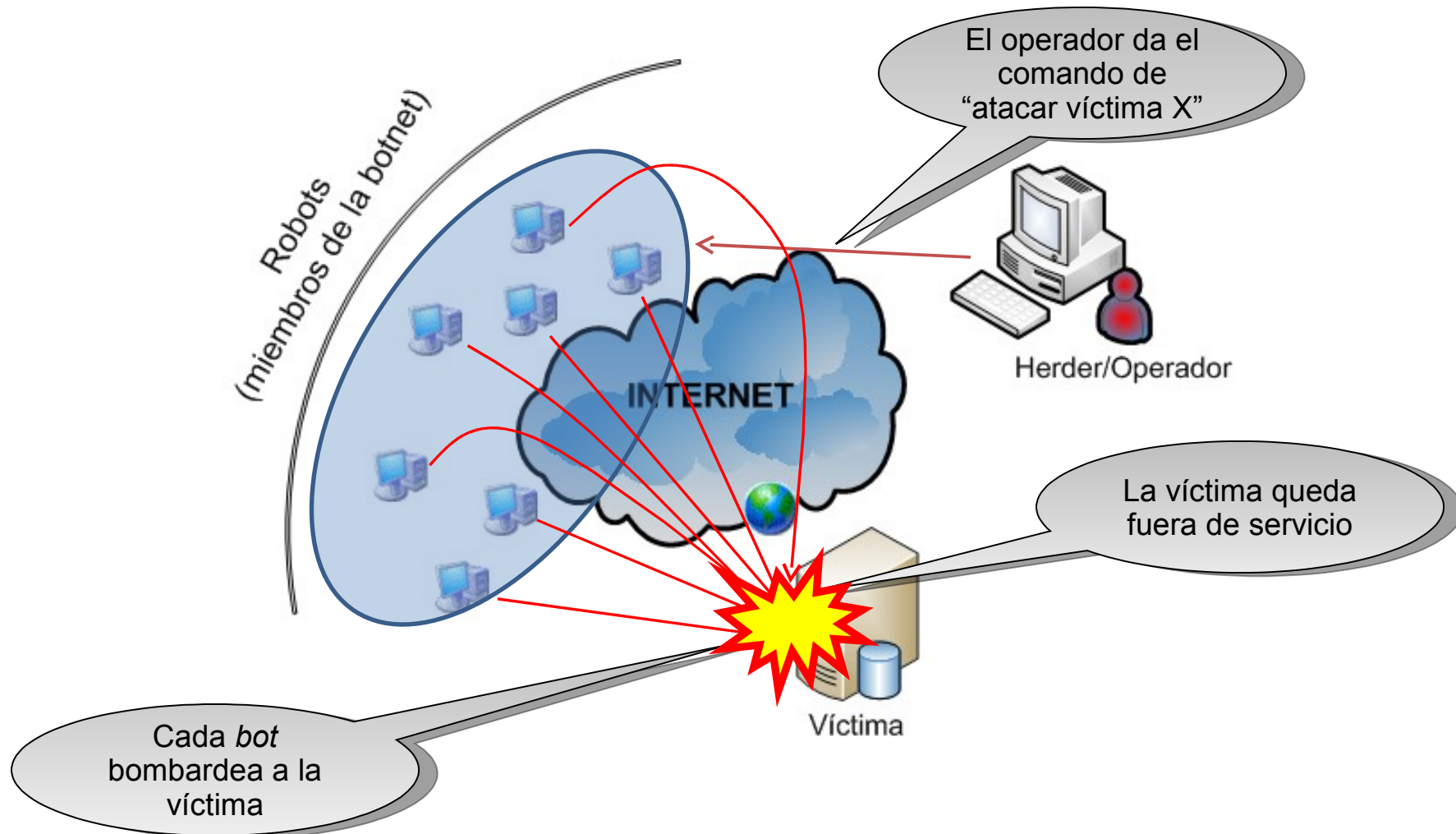
1. El “operador” infecta PC’s de usuarios
2. Los “bots” se conectan a una red IRC u otro canal de comunicaciones
3. Un spammer “compra” acceso a la botnet para enviar sus correos
4. El spammer envia comandos via IRC
5. El spam llega a otros sistemas



Fuente: *Wikimedia Commons*

Botnets para DDoS

- Lanzamiento de una *denegación de servicio distribuida* utilizando una *botnet*






Fast Flux Service Networks

Anatomía de un *Phishing*

Activate your PayPal Account - Thunderbird

File Edit View Go Message Tools Help

Subject: Activate your PayPal Account
From: service@paypal.com <service@paypal.com>
Reply-To: noreply@paypal.com
Date: 19/12/2005 06:11 p.m.



Information Regarding Your account:
Dear PayPal Member!

Attention! Your PayPal account has been violated!

Someone with ip address 80.97.171.22 tried to access your personal account!

Please **click the link below** and enter your account information to confirm that you are not currently away. You have 3 days to confirm account information or your account will be locked.

[Click here to activate your account](#)

Thank you for using PayPal!
The PayPal Team

Protect Your Account Info

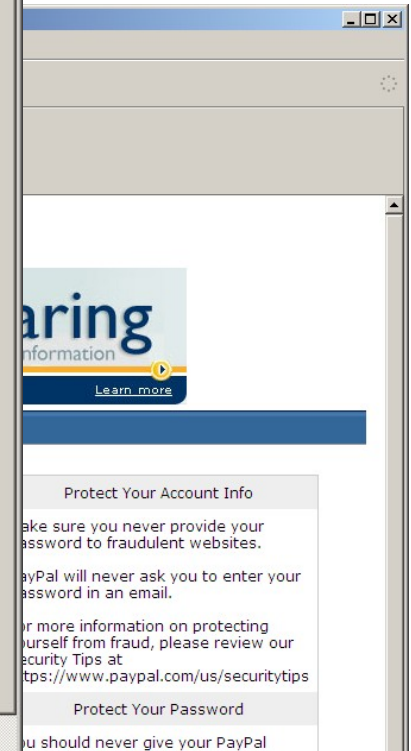
Make sure you never provide your password to fraudulent websites.

PayPal will never ask you to enter your password in an email.

For more information on protecting yourself from fraud, please review our Security Tips at <https://www.paypal.com/us/securitytips>

Protect Your Password

You should never give your PayPal password to anyone.



Shop Without Sharing
Your Financial Information
Learn more

Protect Your Account Info

Make sure you never provide your password to fraudulent websites.

PayPal will never ask you to enter your password in an email.

For more information on protecting yourself from fraud, please review our Security Tips at <https://www.paypal.com/us/securitytips>

Protect Your Password

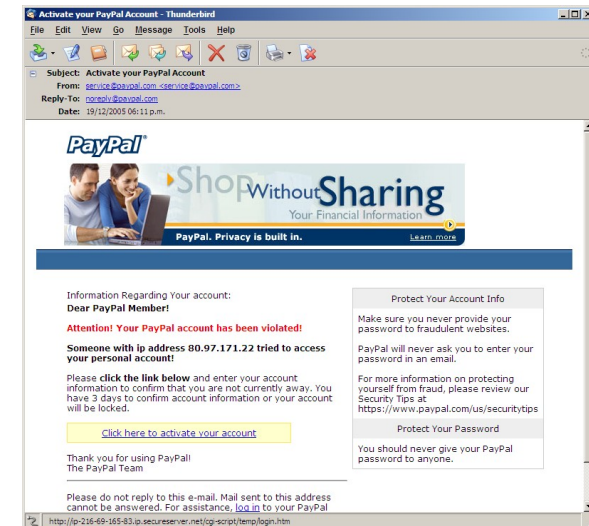
You should never give your PayPal



<http://ip-216-69-165-83.ip.secureserver.net/cgi-script/temp/login.htm>

Anatomía de un *Phishing*

- Para que el *phishing* opere hacen falta:
 - Un sistema comprometido donde alojar las páginas web que simulan al sitio “real”
 - Una forma de direccionar (nombre o IP), para dirigir a los usuarios al mismo
 - En general, las IPs son variables, hacen falta nombres
 - Un agente de recolección de datos
- Rastros:
 - Artefactos en web servers comprometidos



El “Problema”

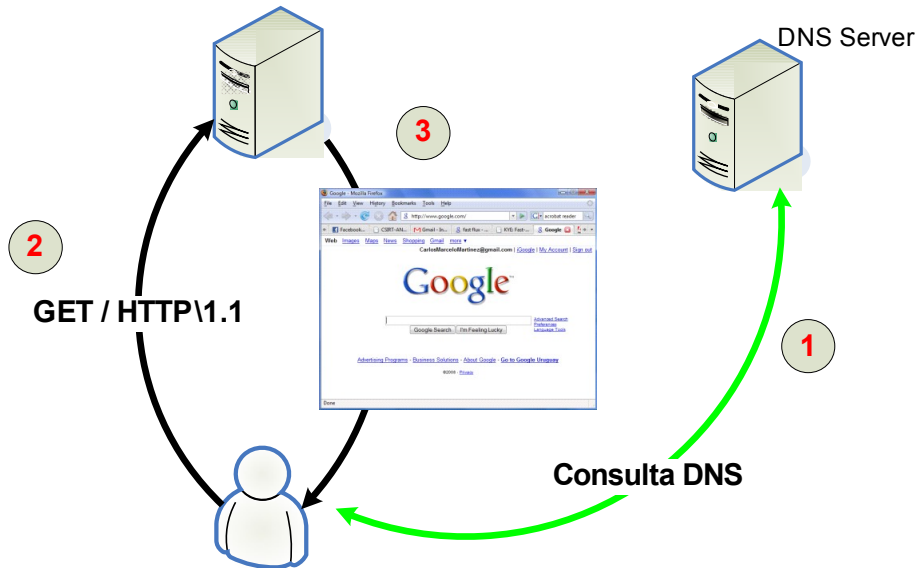
- Bloqueos
 - Un sitio de phishing o similar, “tradicional” es muy sencillo de bloquear una vez detectado
 - Basta con eliminar el sistema comprometido que aloja las páginas fraudulentas
 - La distribución de software en la Botnet también puede ser bloqueada de manera completa si se detecta el sistema central
 - Los administradores de redes en general toman acciones inmediatas contra sitios de phishing y similares bloqueándolos
- Desde el punto de vista del *operador*: ¿*Como dotar de alta disponibilidad a mi botnet?*

La Solución

- Eliminar los puntos únicos de falla
 - Web Server
 - Sistema comprometido donde se aloja el phishing
 - Resolución de nombres
 - a donde se apunta el phishing
- *Fast Flux Service Networks*
- Modos
 - *Single flux*: Servidor web
 - Servidor web distribuido, no ya un único sistema
 - Registros “A” en *round robin*
 - *Double flux*: Resolución de nombres
 - Resolución de nombres distribuída
 - Registros “NS” variables

Anatomía de una *FFSN*

- Acceso web “*normal*”



- Etapas

1. Consulta al DNS por “A” de www.google.com
2. Envía pedido HTTP al servidor web
3. Obtiene la página buscada

Anatomía de una *FFSN*: Tipos

- *Single Flux*
 - Múltiples servidores web
 - Alojados en sistemas comprometidos (botnets)
 - Servidores DNS limitados
 - Alojados en proveedores de DNS “usuales”
 - Deben permitir configurar dinámicamente registros “A” con TTLs pequeños
- *Double Flux*
 - Múltiples servidores web
 - Múltiples servidores DNS
 - Proveedor de DNS debe además permitir la configuración dinámica de registros “NS”

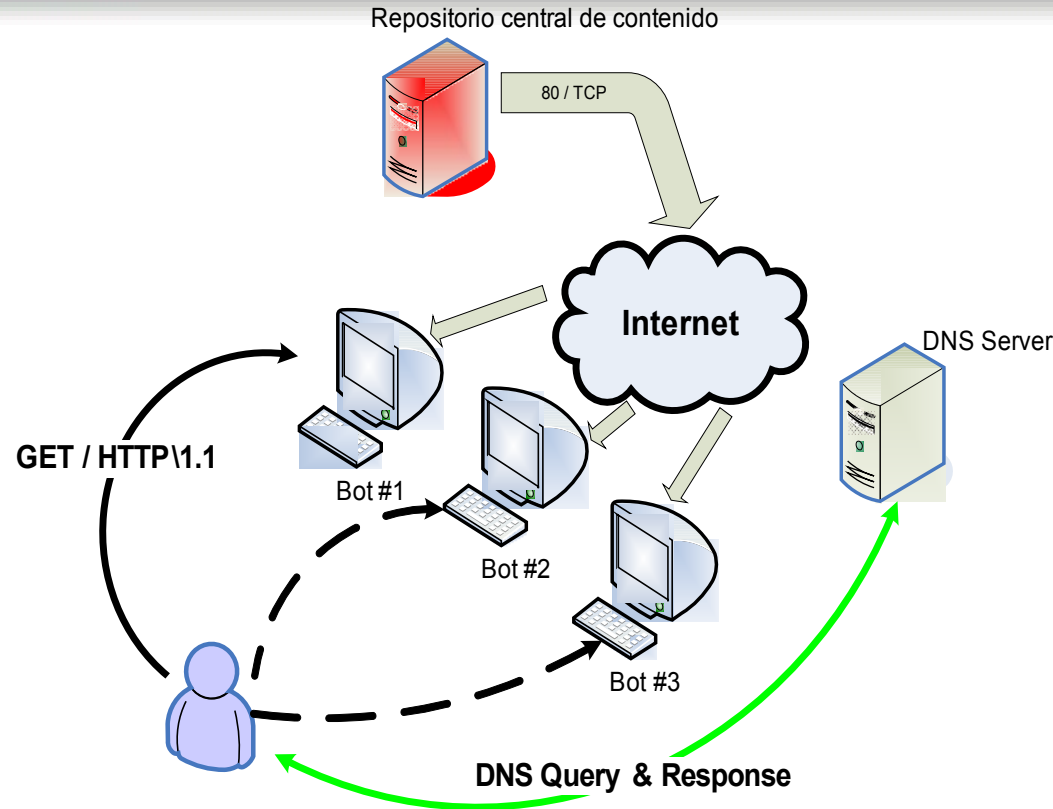
Anatomía de una *FFSN: Single Flux*

- ¿En que se diferencia del caso normal?

- Múltiples registros “A” devueltos por el DNS
- TTLs muy pequeños
- Los “servidores” son en general computadores personales comprometidos
- Registros “A” van cambiando con el tiempo

- Servidores DNS similares al caso “normal”

- Pocos registros
- Asociados a un proveedor

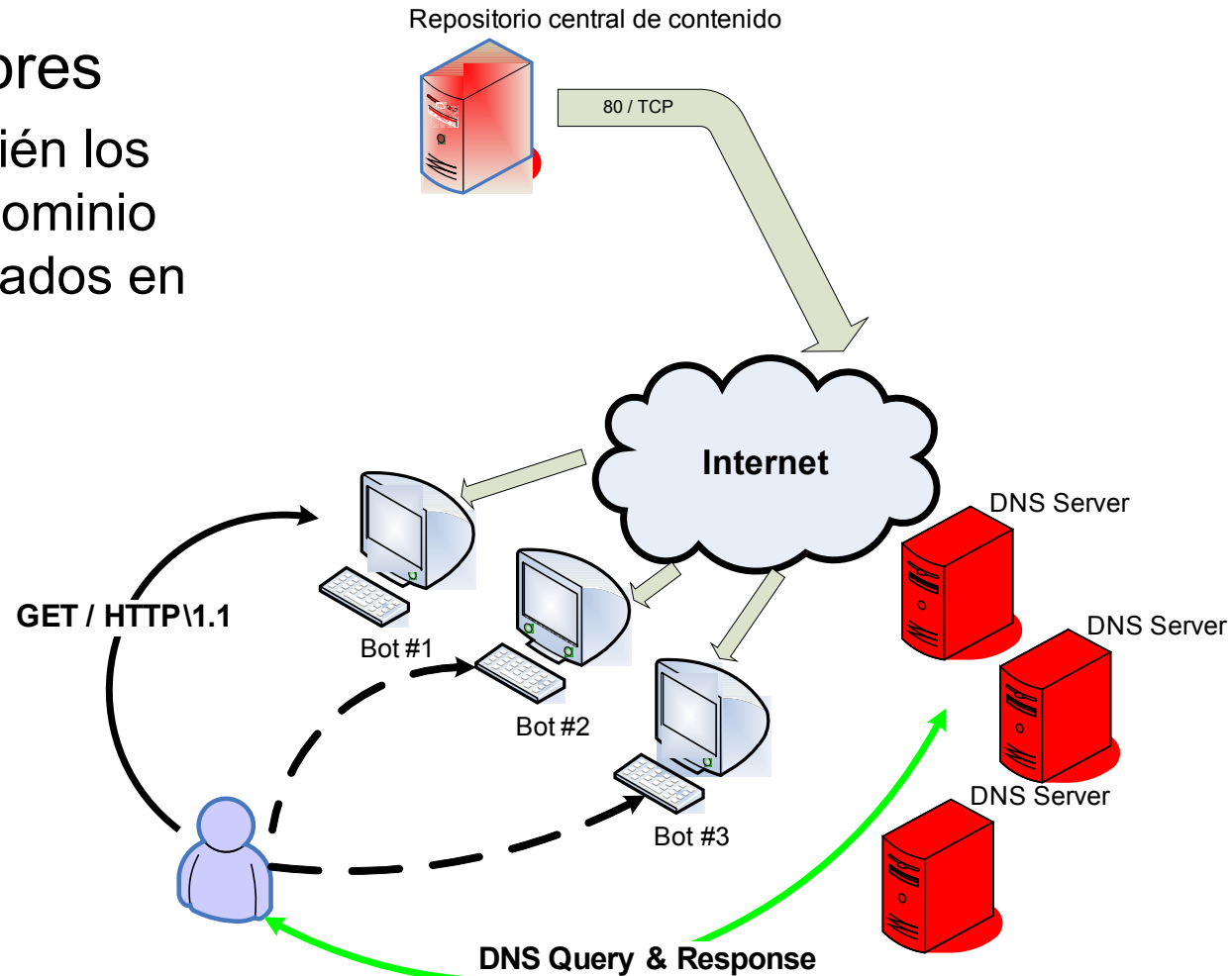


- Observaciones

- Contenido entregado desde un sitio central
 - Facilita gestión

Anatomía de una *FFSN: Double Flux*

- El *double flux* agrega “redundancia” a la resolución de nombres
 - En este caso, también los registros “NS” del dominio asociado están alojados en bots y varían



Detección de *FFSNs*

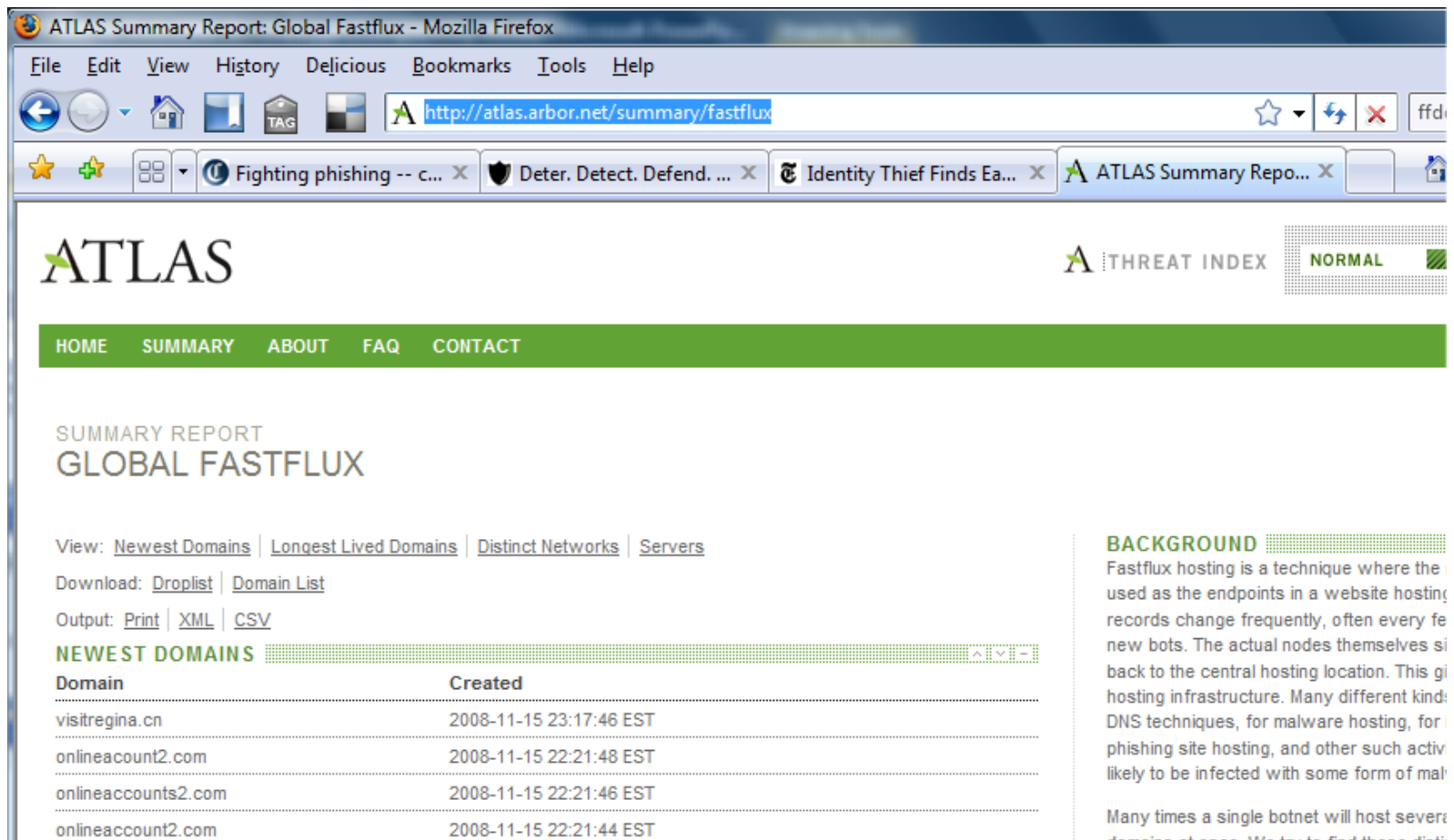
- Holz et al [1] proponen un criterio de *scoring* para detectar *FFSNs*
- Posibles parámetros:
 - ***nA***: el número de registros “A” devuelto por la consulta
 - ***nNS***: el número de registros “NS” devueltos por la consulta
 - ***nASN***: el número de sistemas autónomos diferentes representados en los registros “A”

Detección de *FFSNs* (2)

- Otros criterios:
 - Nombres reversos de las IPs devueltas en la consulta pertenecientes a redes de clientes ADSL, dialup o similares
 - Variaciones temporales nA o nNS
 - Respuesta a eliminaciones de nodos
 - TTLs en los registros pequeños
- Software
 - FFDetect
 - Biblioteca Java, Universidad de Wellington, *Open Source*
 - ffdetect.pl
 - Script Perl, CSIRT Antel, *Open Source*

Detección de *FFSNs* (3)

- Plataforma ATLAS (Arbor Networks)
 - <http://atlas.arbor.net/summary/fastflux>



The screenshot shows a Mozilla Firefox browser window displaying the ATLAS Summary Report for Global Fastflux. The browser's address bar shows the URL <http://atlas.arbor.net/summary/fastflux>. The page features the ATLAS logo and a navigation menu with links for HOME, SUMMARY, ABOUT, FAQ, and CONTACT. The main content area is titled "SUMMARY REPORT GLOBAL FASTFLUX" and includes options for viewing (Newest Domains, Longest Lived Domains, Distinct Networks, Servers) and downloading (Droplist, Domain List) the data. A table lists the newest domains, and a background section explains the Fastflux hosting technique.

ATLAS Summary Report: Global Fastflux - Mozilla Firefox

File Edit View History Delicious Bookmarks Tools Help

<http://atlas.arbor.net/summary/fastflux>

Fighting phishing -- c... x Deter. Detect. Defend. ... x Identity Thief Finds Ea... x ATLAS Summary Repo... x

ATLAS THREAT INDEX NORMAL

HOME SUMMARY ABOUT FAQ CONTACT

SUMMARY REPORT
GLOBAL FASTFLUX

View: [Newest Domains](#) | [Longest Lived Domains](#) | [Distinct Networks](#) | [Servers](#)

Download: [Droplist](#) | [Domain List](#)

Output: [Print](#) | [XML](#) | [CSV](#)

NEWEST DOMAINS

Domain	Created
visitregina.cn	2008-11-15 23:17:46 EST
onlineaccount2.com	2008-11-15 22:21:48 EST
onlineaccounts2.com	2008-11-15 22:21:46 EST
onlineaccount2.com	2008-11-15 22:21:44 EST

BACKGROUND

Fastflux hosting is a technique where the used as the endpoints in a website hosting records change frequently, often every few new bots. The actual nodes themselves si back to the central hosting location. This gi hosting infrastructure. Many different kind: DNS techniques, for malware hosting, for phishing site hosting, and other such activ likely to be infected with some form of mal

Many times a single botnet will host sever domains at once. We try to find these disti

Ejemplo de una *FFSN* detectada

- Dominio “81dns.ru” (salida de dig 81dns.ru)

```
;; ANSWER SECTION:
```

```
81dns.ru.      600      IN       A       61.64.210.29
81dns.ru.      600      IN       A       61.224.132.13
81dns.ru.      600      IN       A       68.200.93.27
81dns.ru.      600      IN       A       69.14.27.151
81dns.ru.      600      IN       A       70.196.175.168
81dns.ru.      600      IN       A       71.234.239.212
81dns.ru.      600      IN       A       81.202.211.11
81dns.ru.      600      IN       A       85.90.9.24
81dns.ru.      600      IN       A       85.225.209.183
81dns.ru.      600      IN       A       89.36.58.189
81dns.ru.      600      IN       A       99.149.197.114
81dns.ru.      600      IN       A       124.125.176.244
81dns.ru.      600      IN       A       210.97.124.66
81dns.ru.      600      IN       A       220.129.81.51
```

```
;; AUTHORITY SECTION:
```

```
81dns.ru.      345586  IN       NS      ns1.81dns.ru.
81dns.ru.      345586  IN       NS      ns2.81dns.ru.
81dns.ru.      345586  IN       NS      ns3.81dns.ru.
```

Ejemplo de una *FFSN* detectada (2)

- Reversos de “81dns.ru” (Registros “A”)

29.210.64.61	PTR	61-64-210-29-adsl-tpe.dynamic.so-net.net.tw.
13.132.224.61	PTR	61-224-132-13.dynamic.hinet.net.
27.93.200.68	PTR	27-93.200-68.tampabay.res.rr.com.
151.27.14.69	PTR	d14-69-151-27.try.wideopenwest.com.
168.175.196.70	PTR	168.sub-70-196-175.myvzw.com.
212.239.234.71	PTR	c-71-234-239-212.hsd1.ct.comcast.net.
11.211.202.81	PTR	81.202.211.11.dyn.user.ono.com.
24.9.90.85	PTR	24.9.90.85.lully.cust.dynamic.gpowernet.ch.
183.209.225.85	PTR	c-b7d1e155.82-6-64736c12.cust.bredbandsbolaget.se.
114.197.149.99	PTR	adsl-99-149-197-114.dsl.chcgil.sbcglobal.net.
51.81.129.220	PTR	220-129-81-51.dynamic.hinet.net.

Conclusiones

- Las FFSNs:
 - Dan redundancia y estabilidad a redes para entrega de contenido dudoso
 - Phishings y otros fraudes
 - Venta de productos farmacéuticos, etc.
 - Proveen de una capa adicional de anonimización a quienes operan estas redes
 - Difícilmente se puedan hallar logs en los PCs comprometidos (bots) que actúan de servidores web
 - Desde el punto de vista del ISP se debe ser cauteloso con las herramientas de gestión de DNS automatizadas de las que se proveen a los clientes
- Hace falta más investigación
 - Formas de detectar y de eliminar

Referencias

- [1] Holz T., Gorecki C., Rieck K. and Freiling F. C. *“Measuring and Detecting Fast-Flux Service Networks”*:
<https://pi1.informatik.uni-mannheim.de/filepool/research/p>
- [2] Know Your Enemy: Fast Flux Service Networks:
<http://www.honeynet.org/papers/ff/fast-flux.html>
- [3] SSAC Advisory 025: SSAC Advisory on Fast Flux Hosting and DNS:
<http://www.icann.org/en/committees/security/sac025.>
- [4] Nazario J., Holz T. *“As the Net Churns: Fast Flux Service Networks Observations”*; MALWARE’08:
<http://honeyblog.org/junkyard/paper/fastflux-malware08.p>

¡Muchas gracias por su atención!

