Métodos actuales de

Apropiación de dominios

HackMeeting 2003
Pamplona, 24-26 de Octubre

Vicente Aguilera Díaz
vaguilera@isecauditors.com

Contenido

1. Introducción
2. Registro de dominios
3. Métodos de ataque
4. Conclusiones y recomendaciones
5. Referencias

1.1 INTRODUCCIÓN. Quién es quién

1991 **ISOC** 1992 **NSI** **IANA** Jon Postel 1996 Explosión dominios 1998 **ICANN** 2000 **Verisign** compra NSI

ISOC:
- desarrollo mundial de Internet
- constituye:
  - IAB (Internet Architecture Board),
  - IESG (Internet Engineering Steering Group)
  - IETF (Internet Engineering Task Force)
  - IANA (Internet Assigned Numbers Authority)

NSI:
- control BBDD Whois
- control de la raíz A de Internet

ICANN:
- control del sistema de root servers
- parámetros control Internet
- gestionar DNS y asignación de direcciones IP
- coordinar registradores dominio

1.2 INTRODUCCIÓN. Explosión fenómeno dominios

- Año 1996: preocupación por el futuro de Internet

- Los dominios se comienzan a ver como marcas

- Aparece la figura del *cibersquatter*

- Año 1999: España figura en la 3a. posición del ránking mundial en cuanto a delitos de ciberocupación

- Casos:
    * business.com: 7.5 millones de dolares (finales de 1999)
    * mcdonalds.com, elpais.com, campofrio.com
    * barcelona.com !!!

2.1 REGISTRO DE DOMINIOS. Búsqueda de información

¿Qué nombre de dominio elegir?

- Imaginación!
- Banco de dominios: http://www.goldnames.com
- Subastas de dominios:
  - http://www.websitenames.com
  - http://www.greatdomains.com

¿Existe el dominio que quiero registrar?

- http://www.networksolutions.com/en_US/whois/index.jhtml
- http://www.checkdomain.com/
- http://www.register.com
- http://www.corenic.org
- http://www.uwhois.com/cgi/domains.cgi?User=NoAds
- ...

¿Quién gestiona la IP del dominio?

- RIPE: http://www.ripe.net – dominios europeos
- ARIN: http://www.arin.net – dominios americanos/africanos
- APNIC: http://www.apnic.net - dominios asia/pacífico
- LACNIC: http://www.lacnic.net - dominios latinoamericanos/caribe

2.2 REGISTRO DE DOMINIOS. El proceso de registro

Registrante (persona física/jurídica)

- Petición de registro

Agente registrador

- Intermediario cliente/registro
- Asesoramiento a clientes
- Proporcionar servicios adicionales

Registro

- Directorio central
- Según el modelo CORE:
  - . Aceptar peticiones de registro
  - . Generar fichero de zona utilizado en los DNS
  - . Poner a disposición de los usuarios el servicio WHOIS

3.1 MÉTODOS DE ATAQUE. Introducción

Objetivo

Apropiación de un dominio propiedad de terceros (de forma temporal o permanente).

Consecuencias

Servicios inoperativos: web, correo, ftp, ... y otros que se encuentren en el dominio atacado.

Ataques

Los métodos empleados dependerán de la entidad atacada:

- Registrante
- Agente registrador
- Registro

3.2 MÉTODOS DE ATAQUE. Ataques al registrante (I)

Responsabilidades del registrante

- Seleccionar un AR que ofrezca garantías de seguridad

- Revisar política de privacidad del AR para conocer cómo procesa la información personal (posibilidad de ocultar información a consultas WHOIS)

- Guardar información de registro del dominio

- Activar todas las medidas de seguridad que ofrezca el AR

- Mantener la información de WHOIS actualizada

- Revisar y leer periódicamente las cuentas de correo

- Utilizar cuentas de correo “seguras”

- Utilizar contraseñas robustas

3.2 MÉTODOS DE ATAQUE. Ataques al registrante (II)

Ataques

1. Obtener información:

   - Identificar y verificar información

   - Buscar en WHOIS.

   - Agente registrador

   - Fecha creación/expiración del dominio

   - Personas de contacto, direcciones de e-mail, etc.

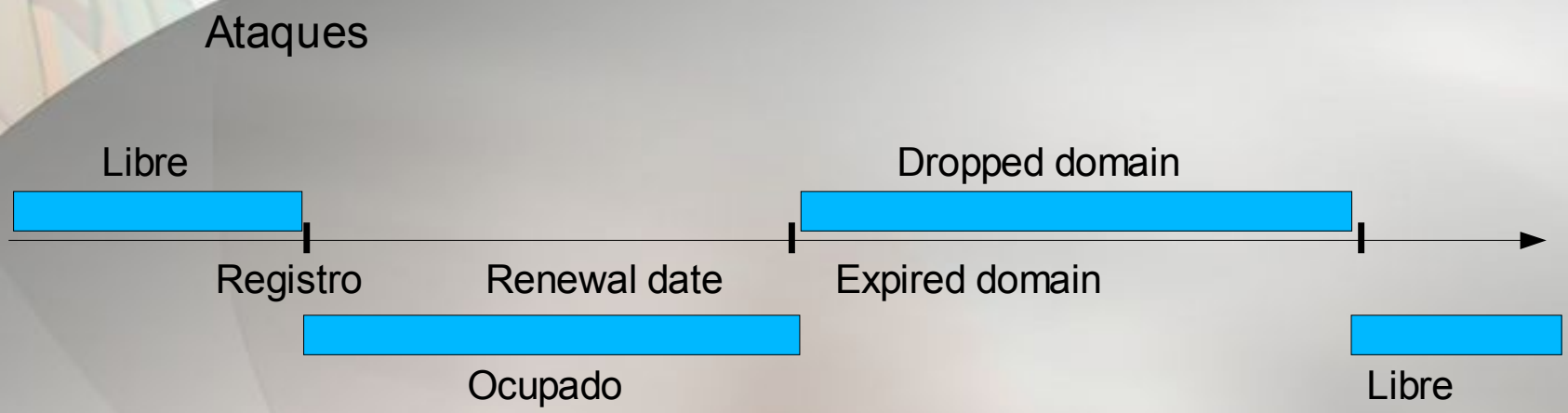
   - DNS

   - Buscar en RIR (RIPE,ARIN,APNIC,LACNIC) datos propietario IP

   - etc.

Consultas a Whois desde NSI:
"This code is an image that cannot be read by a machine. It prevents automated programs from requesting access to WHOIS information."

3.2 MÉTODOS DE ATAQUE. Ataques al registrante (III)



Expiración del dominio
- WHOIS, herramientas (Domain Name Analyzer, Snap Back, etc.)

Analizar cuentas de e-mail:
- Verificar si utiliza servicios inseguros de e-mail (hotmail, terra, etc.)
- Verificar robustez de las contraseñas: *password cracking*
- Verificar lectura de correo (enviar mails a todas las cuentas)
- Inundar de correo las cuentas (camuflar e-mails del AR)
- Ataques al servidor de correo

Ingeniería social
- Conseguir passwords

3.3 MÉTODOS DE ATAQUE. Ataques al AR (I)

Responsabilidades del AR

- Ofrecer acceso seguro a la gestión del dominio

- No permitir actualizaciones vía fax/teléfono

- Servicio “domain lock” o “registrar lock”

- Solicitar confirmación antes de realizar modificaciones

- Notificar de cualquier cambio realizado en el dominio

- Contar con fuertes mecanismos de seguridad y cifrado (PGP, GPG, etc.)

- Mantener actualizada Whois a partir de la información del cliente

- Informar de peticiones de transferencia de dominio (el nuevo AR debe asegurarse de quién realiza la petición)

3.4 MÉTODOS DE ATAQUE. Ataques al AR (II)

Responsabilidades del AR

- No alardear sobre su nivel de seguridad...

Por ejemplo: http://www.publihospedaje.com/faqsdominios.htm

"... Los dominios comprados con nosotros estan protegidos contra robo ya que ofrecemos la posibilidad de bloquear o no según quiera el usuario este tipo de operaciones (transferencias de dominios). No se arriesgue a ser victima de este tipo de ataque con otros registradores confie en nuestra experiencia en seguridad informática, ¡único en el mercado!"

3.5 MÉTODOS DE ATAQUE. Ataques al AR (III)

Ataques

1. Obtener información:

   - Analizar vias de comunicacion permitidas (telefono, fax, e-mail, etc.).

   - Identificar y validar las medidas de seguridad adoptadas (encriptacion, contraseñas robustas, confirmacion y notificacion de cambios, "domain renewal reminders", "domain lock", etc.).

   - Analizar el contrato que proporciona el AR buscando posibles deficiencias de seguridad.

   - Analizar todas las posibles operaciones permitidas por el AR (registro de dominio, modificacion de los datos de registro, transferencia de dominio, destrucción del dominio, cambio de propietario del dominio, envio de password, modificacion de password via e-mail, etc.).

3.6 MÉTODOS DE ATAQUE. Ataques al AR (IV)

Ataques

1. ...obtener información:

   - Verificar que se encuentren habilitadas todas las medidas de seguridad que ofrezca el AR (domain lock, confirmaciones via e-mail, notificaciones de cambios, etc.).

   - Identificar la informacion personal (y posibles documentos) que solicita al registrar un dominio.

   - Analizar la politica de privacidad y verificar su cumplimiento. Validar que la informacion personal que nos solicita no es excesiva ni se facilita a terceras personas.

   - Identificar la información personal (y posibles documentos) que solicita al realizar cualquiera de las operaciones permitidas (modificacion de datos de los contactos, destrucción del dominio, etc.).

3.7 MÉTODOS DE ATAQUE. Ataques al AR (V)

Ataques

2. Modificar datos propietario/contacto administrativo

- Registrarnos en el AR objetivo, con usuario ficticio.

- Identificar la informacion personal (y posibles documentos) que solicita al registrar un dominio.

- Identificar la información personal (y posibles documentos) que solicita al realizar cualquiera de las operaciones permitidas (modificacion de datos de los contactos, cambio de propietario, etc.).

- Comparar información y documentos de los dos puntos anteriores para detectar qué información puede ser falseada.

- Solicitar las modificaciones.

3.6 MÉTODOS DE ATAQUE. Ataques al AR (VI)

Ataques

2. Transferir dominio a otro AR

- Analizar diferentes AR buscando el más “inseguro”.

- Solicitar transferencia de dominio.

- Para evitar que los contactos del dominio puedan leer la posible notificación de la transferencia por parte del AR:

  . realizar la petición en epoca de vacaciones.
  . inundar las cuentas de e-mail de los contactos con correo basura.

- Suplantar la dirección de correo del contacto administrativo y realizar la petición de transferencia desde esta cuenta (por si el AR utiliza autenticación “MAIL-FROM”).

- Una vez realizada la transferencia con éxito, modificar el contacto administrativo/propietario, etc. aprovechando las deficiencias de seguridad que habíamos detectado.

3.7 MÉTODOS DE ATAQUE. Ataques al AR (VII)

Ataques

3. Destruir dominio

- Comprobar si el AR objetivo permite esta operación (si es necesario, registrarnos en el AR con usuario ficticio).

- Si el AR objetivo no lo permite, transferir el dominio a otro AR que sí lo permita.

- Identificar la informacion personal (y posibles documentos) que solicita al registrar un dominio.

- Identificar la información personal (y posibles documentos) que solicita al realizar la destruccion del dominio.

- Comparar información y documentos de los dos puntos anteriores para detectar si la información puede ser falseada.

- Utilizar herramientas para ponernos en la “cola” de registrodel dominio objetivo. Solicitar la destrucción del dominio.

3.8 MÉTODOS DE ATAQUE. Ataques al AR (VIII)

Ataques

4. Analizar robustez de las contraseñas

- Comprobar el nivel de permisibilidad que ofrece el AR (longitud contraseñas, codificación, etc.)

- Identificar ID de usuario y comprobar la robustez de la contraseña mediante *password cracking.*

- Comprobar debilidad en procesos de cambio de contraseña

5. Ataques a los DNS

- Verificar nivel de seguridad de los DNS

- Modificar tablas de mapeo, envenamiento de la cache (Birthday), etc

- Ataques a los Root Servers (Junio 2000: 4 RS más de ½ hora)

- Caso RSA Security

3.4 MÉTODOS DE ATAQUE. Ataques al registro

Ataques

- Whois es el directorio central

- Whois se encuentra dividida (RIRs/LIRs)

- Dónde encontrar Whois:

  whois.ARIN.net
  whois.APNIC.net
  whois.RIPE.net
  whois.NetworkSoluctions.com
  whois.InterNIC.net (VeriSign Inc.)
  whois.ISI.edu
  whois.NRL.Navy.mil
  ...

  http://www.psychotekk.de/appendix/appendix1.shtm

- Suplantación de AR: modificación disponibilidad y propietario (sólo los AR acreditas por la ICANN disponen de acceso)

4. Conclusiones y recomendaciones

- **Ser conscientes que debemos tomar medidas que nos permitan aumentar el nivel de seguridad sobre nuestro dominio** (podemos perderlo aún siendo los propietarios!)

- Seleccionar un AR con las máximas medidas de seguridad (y habilitarlas!)

- Revisar periódicamente nuestra información en Whois

- Utilizar cuentas de correo seguras (si es necesario dedicar una dirección de correo en exclusiva para los datos de contacto)

- Revisar periódicamente el correo (por si el AR nos notificara)

- Bloquear las transferencias de zona

- Utilizar contraseñas robustas en todas nuestras cuentas (gestión AR, e-mail, etc.)

- Si el DNS lo gestionamos nosotros, mantenerlo actualizado y securizado

5. Referencias

IANA – Internet Assigned Numbers Authority
www.iana.org

ICANN – Internet Corporation for Assigned Names and Numbers
www.icann.org

NSI – Network Solutions Inc.
www.nsi.com

ISOC – Internet Society
www.isoc.org

Listado Root Servers y Whois
http://www.psychotekk.de/appendix/appendix1.shtm

Consultas whois y FAQs
www.whoisquery.com

DNS Free
soa.granitecanyon.com

Lista de AR acreditados por la ICANN
http://www.icann.org/registrars/accredited-list.html

Referencias centralizadas gTLD/ccTLD/RIR
http://www.uwhois.com/cgi/domains.cgi?User=NoAds

Comentarios, opiniones, sugerencias...

?

Métodos actuales de

Apropiación de dominios

Gracias por vuestra atención

HackMeeting 2003
Pamplona, 24-26 de Octubre

Vicente Aguilera Díaz
vaguilera@isecauditors.com