ArCERT

Lic. Gastón Franco

Oficina Nacional de
Tecnologías de Información
Subsecretaría de la Gestión Pública

26 de junio de 2007

Coordinación de Emergencias en Redes Teleinformáticas de la Administración Pública Argentina

Argentina - Computer Emergency Response Team

Principales características

CREADO **Julio de 1999**

MARCO LEGAL **Resolución N° 81/1999**
Aprueba creación y establece funciones

Disposición N° 01/1999
Aprueba Reglamento de Operación

Decreto N° 1028/2003
Acciones de la ONTI en materia de seguridad informática

AMBITO **Organismos Públicos**

Principales Objetivos

OBJETIVO PRINCIPAL

Incrementar los niveles de Seguridad Informática del Sector Público

OBJETIVOS ESPECIFICOS

Atención de Incidentes de Seguridad

Actividades Preventivas

- Capacitación
- Difusión de Alertas e Información
- Servicios y Productos
- Políticas de Seguridad de la Información

Representación en Foros Internacionales

- Miembro del FIRST desde abril de 2004
- Punto de Contacto para OEA
- Participación en MERCOSUR

Coordinación con otros CERTs

39 países – 189 Equipos

FIRST
Improving Security Together
MEMBER

Políticas de Seguridad de la Información

OBJETIVOS

- Establecer un marco normativo para gestionar la seguridad de la información (DA Nº 669/2004)
- Proteger adecuadamente la información en poder del Estado
- Promover la concientización a nivel de toda la organización
- Asignar responsabilidades

Servicios y Productos

- Firewall (basado en software de libre disp.)
- SiMoS - Sistema de Monitoreo de Seguridad
- DNSar – Análisis de Servidores y Dominios DNS
- CAL - Sistema de Sensores (en desarrollo)
- RAM – Recolección y Análisis de Malware (en desarrollo)

SiMoS

¿QUE ES?	**Sistema de monitoreo remoto de seguridad**
OBJETIVO	**Detectar vulnerabilidades en servidores que brinden servicios en Internet**
BASADO EN	**Herramientas de libre disponibilidad** **Interface Web de usuario** **Planificador de actividades**
ACUERDOS	**Autorización previa por Convenio** **Compromiso de confidencialidad**

Interface Web de usuario

DNSar

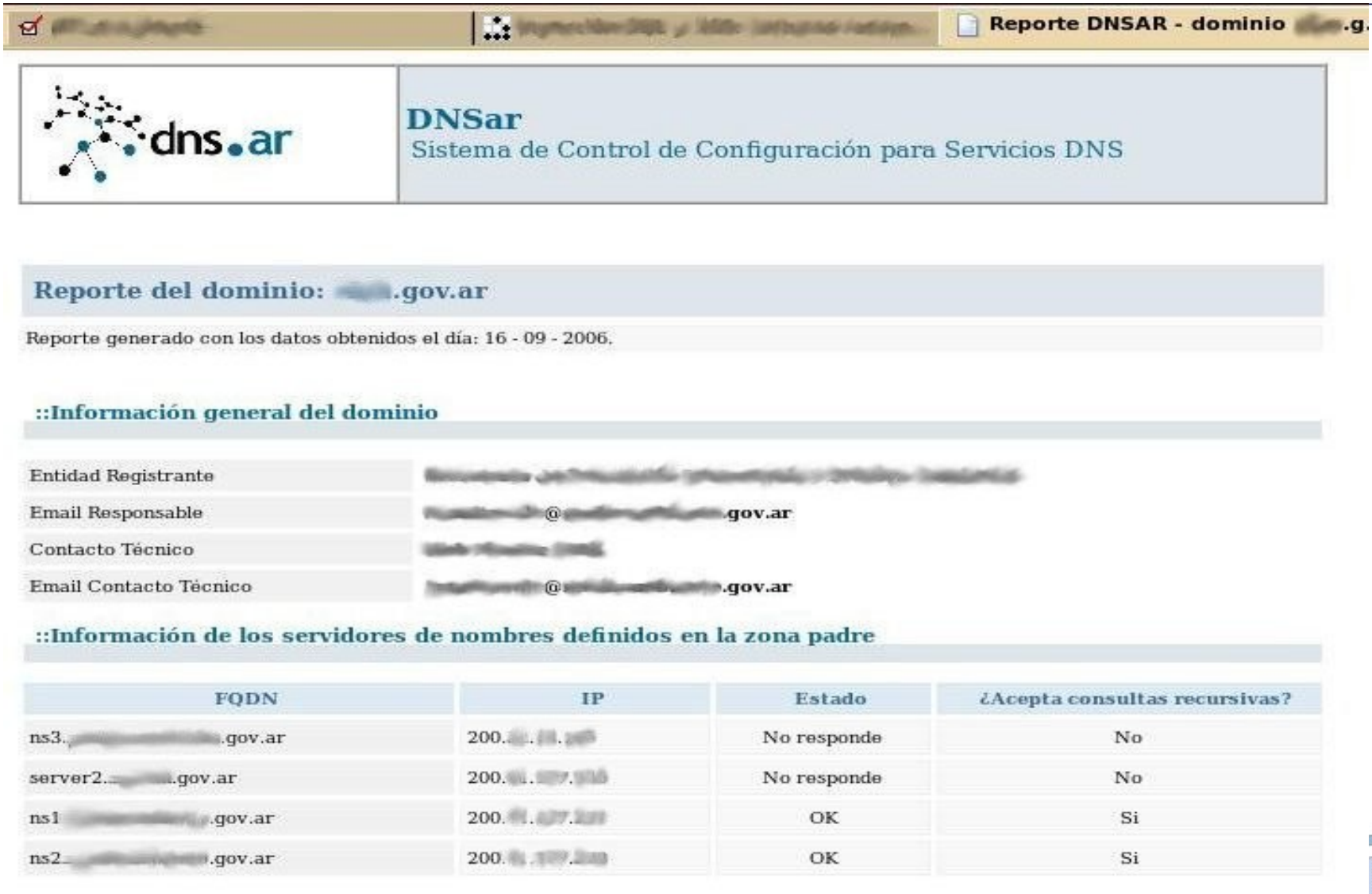
¿QUE ES? **Sistema de análisis de servidores y dominios DNS**

OBJETIVO **Detectar y alertar sobre falencias en los servidores DNS de los Organismos**

Mantener una base de datos histórica con dicha información

Generar información estadística

DNSar


Reporte DNSAR - dominio
DNSar
Sistema de Control de Configuración para Servicios DNS
Reporte del dominio: .gov.ar
Reporte generado con los datos obtenidos el día: 16 - 09 - 2006.
::Información general del dominio
Entidad Registrante
Email Responsable
.gov.ar
Contacto Técnico
Email Contacto Técnico
.gov.ar
::Información de los servidores de nombres definidos en la zona padre
FQDN
IP
Estado
¿Acepta consultas recursivas?
ns3. .gov.ar
200.
No responde
No
server2. .gov.ar
200.
No responde
No
ns1 .gov.ar
200.
OK
Si
ns2 .gov.ar
200.
OK
Si

ALGUNOS DATOS

2282 dominios - 1203 servidores

- ✓ **39%** servidores **aceptan consultas recursivas**
- ✓ **37%** dominios con algún servidor que permite **transferencia de zona**
- ✓ **48%** tienen **sólo 1 registro mx**
- ✓ **41%** dominios tienen, al menos, un **NS que no responde**
- ✓ **5,6%** dominios con, al menos, un ***lame delegation***
- ✓ **2,6%** utilizan **cnames en MX o NS** (RFC 2181)
- ✓ **0,5%** incluyen **direcciones IP privadas** (RFC 1918)

Reporte de Incidentes

- **Se reciben reportes que:**
  - Afecten al Sector Público o Bancario Argentino
  - Estén relacionados con ataques originados desde nuestro país (phishing, alojamiento de malware, etc)
  - No estén vinculados con SPAM

- **Fuentes:**
  - Organismos de gobierno
  - Sector bancario
  - ISPs
  - Ciudadanos
  - Equipos de respuesta a incidentes y organizaciones afectadas a nivel mundial.
  - Fuentes de información públicas y privadas
  - Recolección y análisis de malware
  - Herramientas de detección

Algunos casos tratados

- Sustitución de Páginas Web (Defacement)
- Phishing (engaños)
- Código malicioso (Virus, gusanos, troyanos, etc)
- Botnets y Ataques de DDoS
- Intrusiones de mayor complejidad

Defacements de Páginas Web

[SPYKIDS Group]

Mais bunitinhus que um Ford Ka

Mais fofos que um Etiópio

Mais meigos que um Rinoceronte

YOU ARE OWNED!

#SPYKIDS on gigachat.net

:: Members::
poerschke - _CaKe_ - guns_1 - Hualdo - Creative_MX - Lemarck

Defacements de Páginas Web

Defacements de Páginas Web

Casos de Phishing

De: update@amazon.com <update@amazon.com>
Para: undisclosed-recipients : ;
Asunto: Please Update Your Amazon Account !
Fecha: Mon, 3 Jul 2006 19:59:40 +0300 *(13:59 ART)*
Transporte: Microsoft Outlook Express 6.00.2600.0000

amazon.com.

Dear **Amazon®** member,

It has come to our attention that your **Amazon** order Information records are out of date.That requires you to update the order Information If you could please take 5-10 minutes out of your online experience and update your order records, you will not run into any future problems with Amazon online service.

However, failure to update your records will result in account termination. Please update your records in maximum 24 hours.

Once you have updated records, your **Amazon** session will not be interrupted and will continue as normal.

To update your **Amazon** order Information click on the following link:

http://www.amazon.com/exec/obidos/account-access-login/ref=/index

Best Regards ,
Amazon Security Departament

Casos de Phishing

Incremento considerable en los últimos meses

Casos que afectaban a clientes de Bancos de Argentina

Acciones:

- Se recibieron reportes del incidente.
- Se contactó a los Bancos afectados.
- Se informó a los responsables de los proveedores de Internet que hosteaban los sitios con contenido malicioso.
- Se notificó al CERT Nacional de competencia.

Casos de Phishing

Algunos datos interesantes:

El sitio malicioso estaba alojado en un servidor que físicamente estaba en un país del sudeste asíatico (GMT+8).

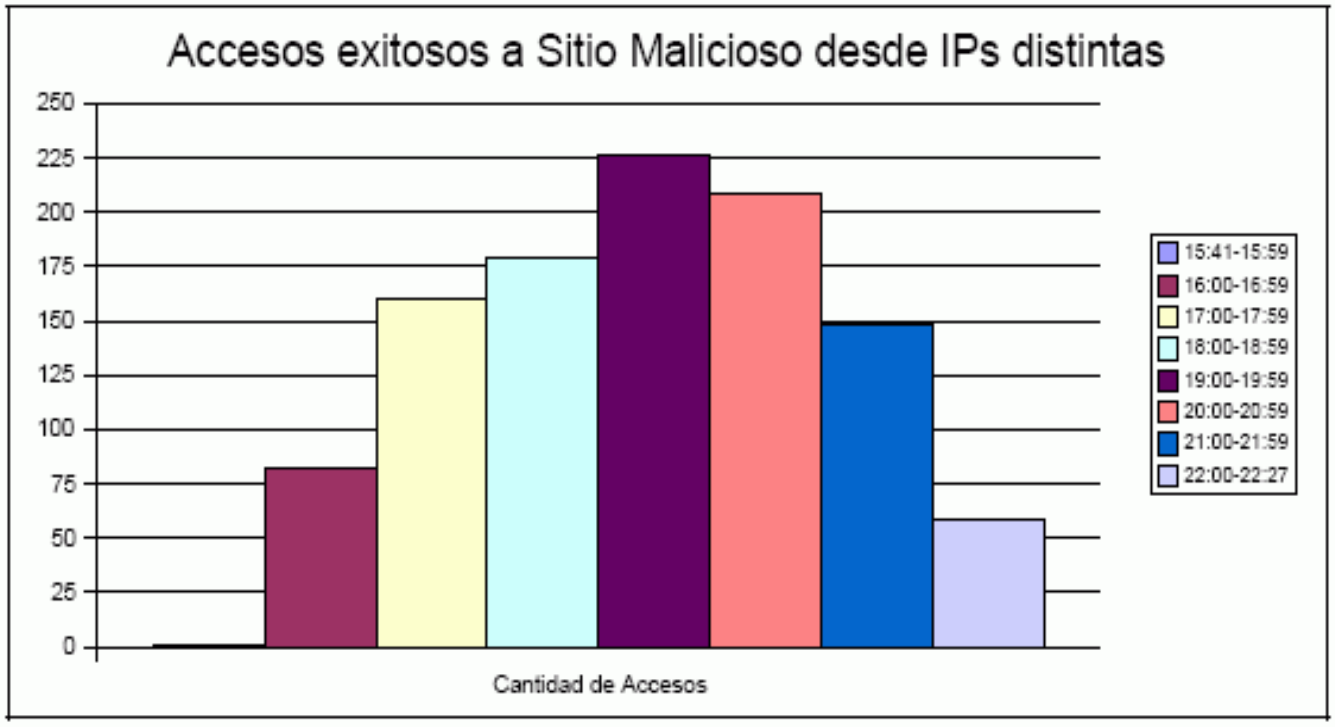
La información que los usuarios enviaban era almacenada en otro servidor, que se encontraba en un país de Europa (GMT+2).

15:41	Primer acceso al sitio malicioso desde un IP en Atlanta, USA
16:32	ArCERT recibe el primer reporte
16:58	Se contacta al Banco. Se envían pedidos de baja al ISP y al CERT Nacional
22:27	El sitio es dado de baja

Casos de Phishing

Accesos al sitio malicioso:

- Tiempo de vida: 6 horas, 46 minutos
- Más de 1000 IPs distintas



Código malicioso distribuido por e-mail

Ataque DDoS utilizando DNS recursivos

Reporte de ataque de DDoS contra un ISP estadounidense

- Tráfico DNS superior a 1Gbps
- Utilizaba 175.000 servidores DNS que permitían consultas recursivas

Con respecto a Argentina

- 2600 servidores correspondían a nuestro país
- 62 entidades involucradas (ISPs y otras organizaciones)
- Se les notificó el incidente, indicando posibles soluciones al problema de configuración.

La actividad pudo efectuarse en 5 horas aprox.

Problemas de Malware / botnet

Problema detectado

- La red interna del organismo estaba saturada,
- Algunos servidores debían ser reiniciados cada 10 min.

Acciones

- Detección de binario malicioso que intentaba atacar a otros equipos y unirse a una botnet
- Análisis de los efectos del mismo
- Consejos para mitigar y restaurar los equipos.

Algunos Resultados

- **Incidentes de Seguridad: +870 atendidos**
- **Organismos Miembros: 122**
- **Capacitación: 24 cursos dictados**
  +600 personas capacitadas
- **Lista de Seguridad: +1800 suscriptores**
- **Alertas: 60 avisos enviados**
- **Publicaciones: 3 doc. públicos / 4 doc. de acceso restringido**

¡Muchas Gracias!

Preguntas y Comentarios

www.arcert.gov.ar

info@arcert.gov.ar