



CYBSEC
Security Systems

15 años de CYBSEC

Julio Ardita – Juan Sabalain

**28 de Septiembre de 2011
Buenos Aires - Argentina**

Nacimiento de CYBSEC

Junio 1996



CYBSEC®
Security Systems

1996 - Nuestro primer cliente



1997 - Nuestro primer PenTest



1998 – Capacitación

Curso Administrador de Seguridad

2 meses de duración



- Introducción a Seguridad Informática
- Políticas de seguridad
- Virus / Antivirus
- Seguridad Física
- Seguridad Lógica
- Seguridad Básica en un sistema
- Sistemas UNIX
- Sistemas Win NT
- Sistemas Mainframe
- Seguridad en redes
- Seguridad básica en Internet.
- Seguridad avanzada en Internet.
- Criptografía.
- Detección de intrusiones.

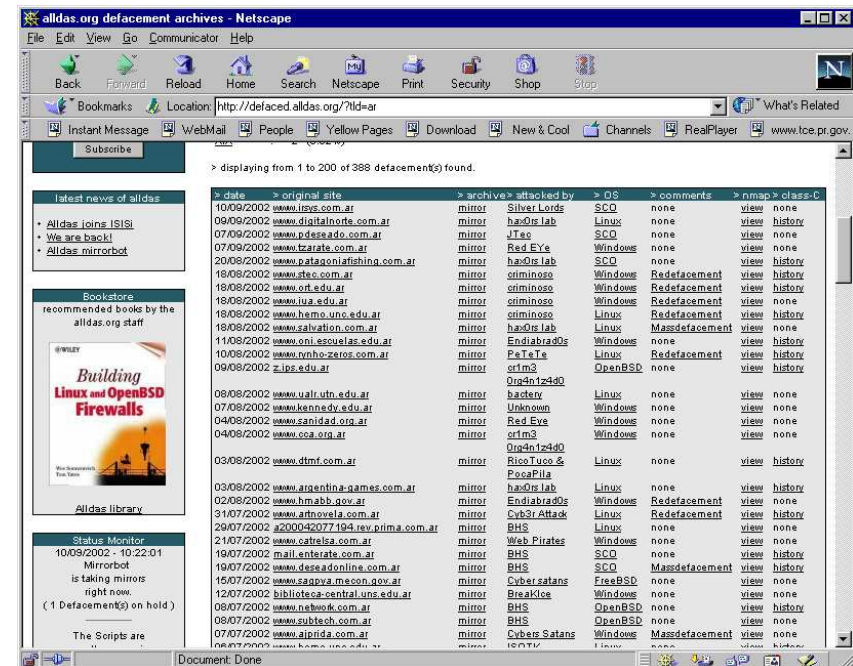
2000 - Boom de Internet



Explosión de la seguridad en Internet

Desde 1998 hasta el 18 de noviembre de 2000 hubo **388** ataques exitosos a páginas Web en la Argentina

Fuente: www.alldas.org



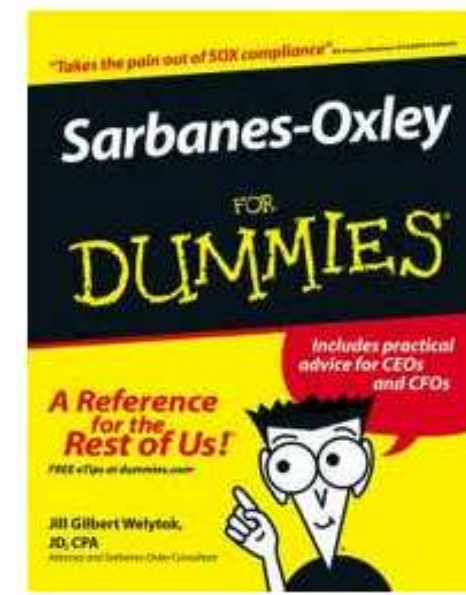
date	original site	mirror	attacker	OS	comments	mirror	class
10/09/2002	www.ipsa.com.ar	mirror	Silver Lords	SCO	none	view	none
09/09/2002	www.digitalnote.com.ar	mirror	ha0rs lab	Linux	none	view	history
07/09/2002	www.pdesedo.com.ar	mirror	JTao	SCO	none	view	none
07/09/2002	www.tzarate.com.ar	mirror	Red Eye	Windows	none	view	none
20/08/2002	www.patagoniarishina.com.ar	mirror	ha0rs lab	SCO	none	view	history
18/08/2002	www.stec.com.ar	mirror	oiminozo	Windows	Redefacement	view	history
18/08/2002	www.cft.edu.ar	mirror	oiminozo	Windows	Redefacement	view	history
18/08/2002	www.tya.edu.ar	mirror	oiminozo	Windows	Redefacement	view	none
18/08/2002	www.hemo.unc.edu.ar	mirror	oiminozo	Linux	Redefacement	view	history
18/08/2002	www.salvation.com.ar	mirror	ha0rs lab	Linux	Massdefacement	view	none
11/08/2002	www.oni.esuelas.edu.ar	mirror	Endiabrados	Windows	Redefacement	view	none
10/08/2002	www.hnho-zero.com.ar	mirror	PaTeTe	Linux	Redefacement	view	history
09/08/2002	www.ips.edu.ar	mirror	oim3	OpenBSD	none	view	history
08/08/2002	www.uall.uth.edu.ar	mirror	bactex	Linux	none	view	none
07/08/2002	www.kennedy.edu.ar	mirror	Unknown	Windows	none	view	none
04/08/2002	www.sanidad.org.ar	mirror	Red Eye	Windows	none	view	none
04/08/2002	www.cca.org.ar	mirror	oim3	Windows	none	view	none
03/08/2002	www.dtmf.com.ar	mirror	Ordn1z4d0	Linux	none	view	history
03/08/2002	www.argentina-games.com.ar	mirror	ha0rs lab	Linux	none	view	history
02/08/2002	www.hmabb.gov.ar	mirror	Endiabrados	Windows	Redefacement	view	none
31/07/2002	www.arnoveja.com.ar	mirror	CyB3r Attack	Linux	Redefacement	view	history
29/07/2002	www.g200042077194.nyu.prima.com.ar	mirror	BHS	Linux	none	view	none
21/07/2002	www.cafelga.com.ar	mirror	Web Pirates	Windows	none	view	none
19/07/2002	mail.entefer.com.ar	mirror	BHS	SCO	none	view	history
19/07/2002	www.desa.donline.com.ar	mirror	BHS	SCO	Massdefacement	view	history
15/07/2002	www.sappva.mecon.gov.ar	mirror	Cyber satans	FreeBSD	none	view	none
12/07/2002	biblioteca.central.uns.edu.ar	mirror	BreakIce	Windows	none	view	none
08/07/2002	www.netbook.com.ar	mirror	BHS	OpenBSD	none	view	history
08/07/2002	www.pubtech.com.ar	mirror	BHS	OpenBSD	none	view	none
07/07/2002	www.alpida.com.ar	mirror	Cyberz Satans	Windows	Massdefacement	view	none
06/07/2002	www.kompa.com.ar	mirror	ICNTV	Linux	none	view	history

2002 a 2007 - Regulaciones!!!

2002: Sarbanes Oxley

2006: BCRA A4609


2007: PCI-DSS



2004 – Primera vulnerabilidad descubierta

Denial of Service in WebSphere Edge Server Julio 2004

Hemos descubierto hasta
hoy 73 vulnerabilidades



CYBSEC S.A.
www.cybsec.com

Advisory Name: Denial of Service in WebSphere Edge Server.
Vulnerability Class: Denial of Service
Release Date:

Affected Applications:

- WebSphere Edge Components Caching Proxy 5.02 using JunctionRewrite with UseCookieDirective.

Not Affected Applications:

- WebSphere Edge Components Caching Proxy 5.02 NOT using JunctionRewrite with UseCookie directive.
- WebSphere Edge Components Caching Proxy 5.00

Affected Platforms:

- SUSE SLES 8
- SUSE SLES 8 Service Pack 1
- SUSE SLES 8 Service Pack 3
- SUSE SLES 8 Service Pack 3
- Apparently all platforms running WebSphere Edge Server

Local / Remote: Remote
Severity: High
Author: Leandro Meiners.

Vendor Status:

- Included in WebSphere Application Server 5.0.3 fix (to be released)
- Patch available from IBM for clients with Support Level 2 or 3

Reference to Vulnerability Disclosure Policy:
http://www.cybsec.com/vulnerability_policy.pdf

Overview:

WebSphere Edge Component Caching Proxy, part of WebSphere Application Server, is a reverse proxy designed to reduce bandwidth use and improve a Web site's speed and reliability by providing a point-of-presence node for one or more back-end content servers. It is built to work with content provided by one or more backend WebSphere Application Servers.

Vulnerability Description:

The vulnerability discovered allows a remote attacker to generate a denial of service condition against the WebSphere Edge Component Caching Proxy.

2006 - Comienzo de los incidentes

Comienzan los primeros incidentes de seguridad graves en la región.



CYBSEC lanza el FastTeam 365



2007 - Expansión regional



**Hemos prestado
servicios en
20 países**

2008 - Outsourcing de Seguridad



Distintos niveles y modalidades de outsourcing

2009 - Servicios de Tecnología

Comenzamos a brindar servicios especializados de Tecnología a nuestros Clientes



CYBSEC en números

- **46 personas integran el equipo de CYBSEC**
- **Cubrimos 130 áreas de conocimiento**
- **Hemos trabajado para más de 400 clientes**
- **Nuestro cliente continuo más antiguo posee 12 años de servicio**
- **La tasa de satisfacción de nuestros clientes es del 97%**



Pilares de CYBSEC

Confianza



Pasión



Valor



Esfuerzo



Orgullo



CYBSEC a 15 años de su nacimiento

Pasión por lo que hacemos

Orgullo por nuestro equipo humano

Profesionalismo y especialización

El más alto nivel de calidad de nuestros servicios

Colaboración con la comunidad de seguridad



Sebastián

Nosotros estaremos...

Nicolás

Pablo

Alicia

Ángeles

Jose

Juan Jorge

Valeria

Eduardo Julio

Iván

Gerónimo Omar

Charly Ariel

Guillermo Andrea

Carolina
Luis Sebastián

Juan Manuel

Santiago Esteban

Mauricio



Daniel Cecilia
Javier

Claudio Belén

Gustavo

Diego Iván

Raúl Juan Pablo

Natalia

Pablo

Nicolás



CYBSEC
Security Systems

Muchas gracias!!!

