Disclaimer and copyright

Only the author's views are expressed in this presentation and do not necessarily reflect those of Banco de España or the Eurosystem.

The original Spanish version of this work was presented on 7 June 2007 to the 4th Expania Meeting and can be downloaded from:

–http://aleph.csic.es/expania/organiza/reuniones-04/r04-comunica.htm

Introduction

The authors:

- José María Carrillo
  - *AIX and Networks Security expert,*
- José Luis Galán Cabilla
  - *Systems Librarian.*

Banco de España

- Security plays a central role.

Our SFX installation

- Small to medium size: 8,185 electronic journals in 34 active targets.
- Hosted by Greendata (the Spanish Ex Libris distributor).
- Very new: STP on January 2007.
- Demand of HTTPs and IP filtering to access SFX-Admin.

Objectives and Table of Contents

Objectives

- –Show the potential threats and vulnerabilities of SFX-Admin implementations.
- –Increase awareness about the importance of security in SFX implementations.
- –Provide recommendations and suggest measures for improving security.

Table of contents

Some conclusions of a recent experiment

Ramsborck, D.; Berthier, R.; Cukier, M. (2007):
Profiling Attacker Behavior Following SSH Compromises.

–Hackers attack computers every 39 seconds.

–Attackers use simple software-aided techniques to randomly attack large numbers of computers.

–The vast majority of attacks come from relatively unsophisticated *script kiddies* using *dictionary scripts*.

–*root* and *admin* are the most common usernames.

–43% of all password-guessing attempts simply re-entered the username.

A password should never be identical or even related to its associated username.

Script kiddies: unskilled but dangerous

Script kiddie

"…derogatory term used for an inexperienced malicious cracker who uses programs developed by others to attack computer systems, and deface websites. It is generally assumed that script kiddies are kids who lack the ability to write sophisticated hacking programs on their own.."

© Sthephen Thompson

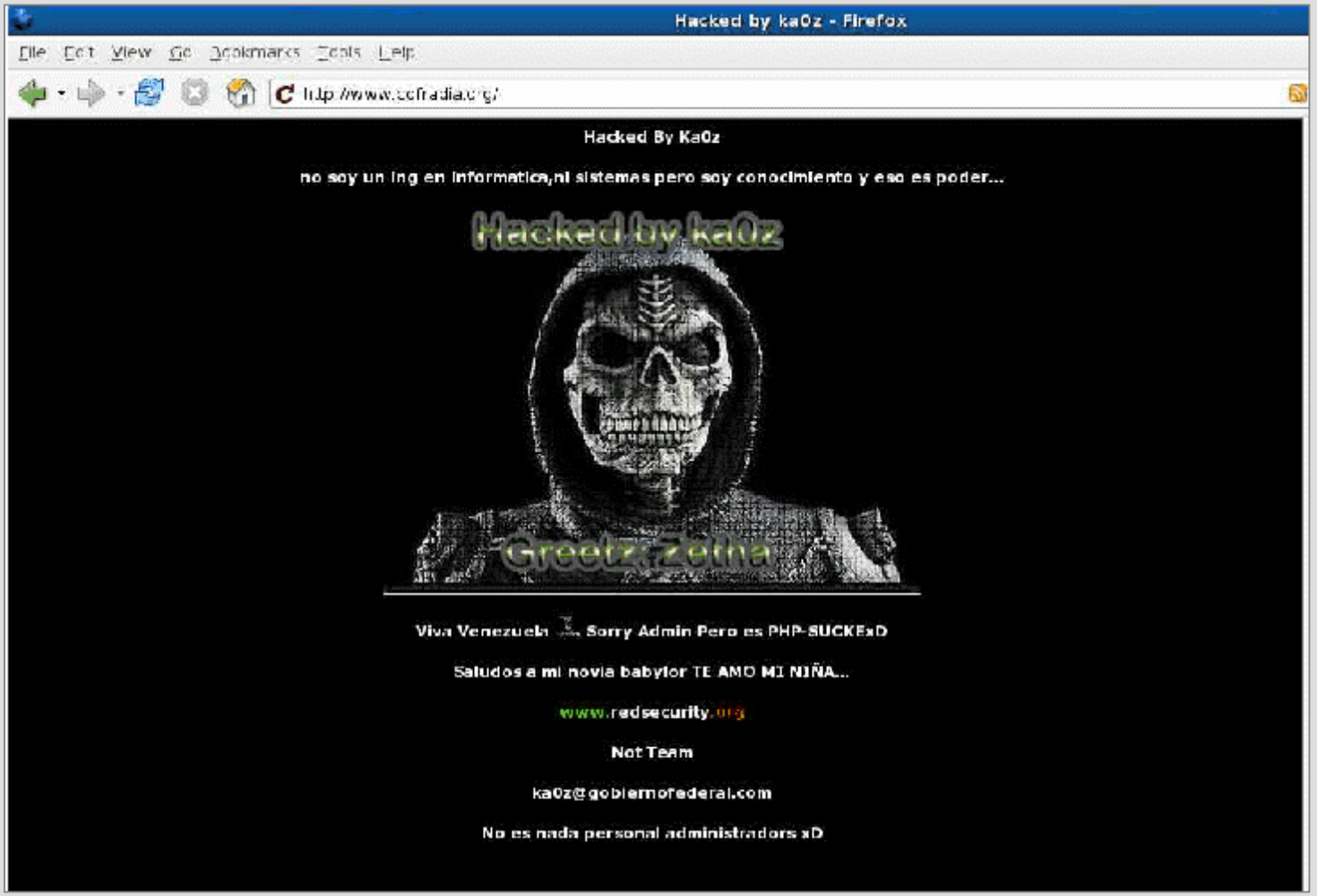
© sitnuna.com

To them, hacking is more for show than a goal in itself

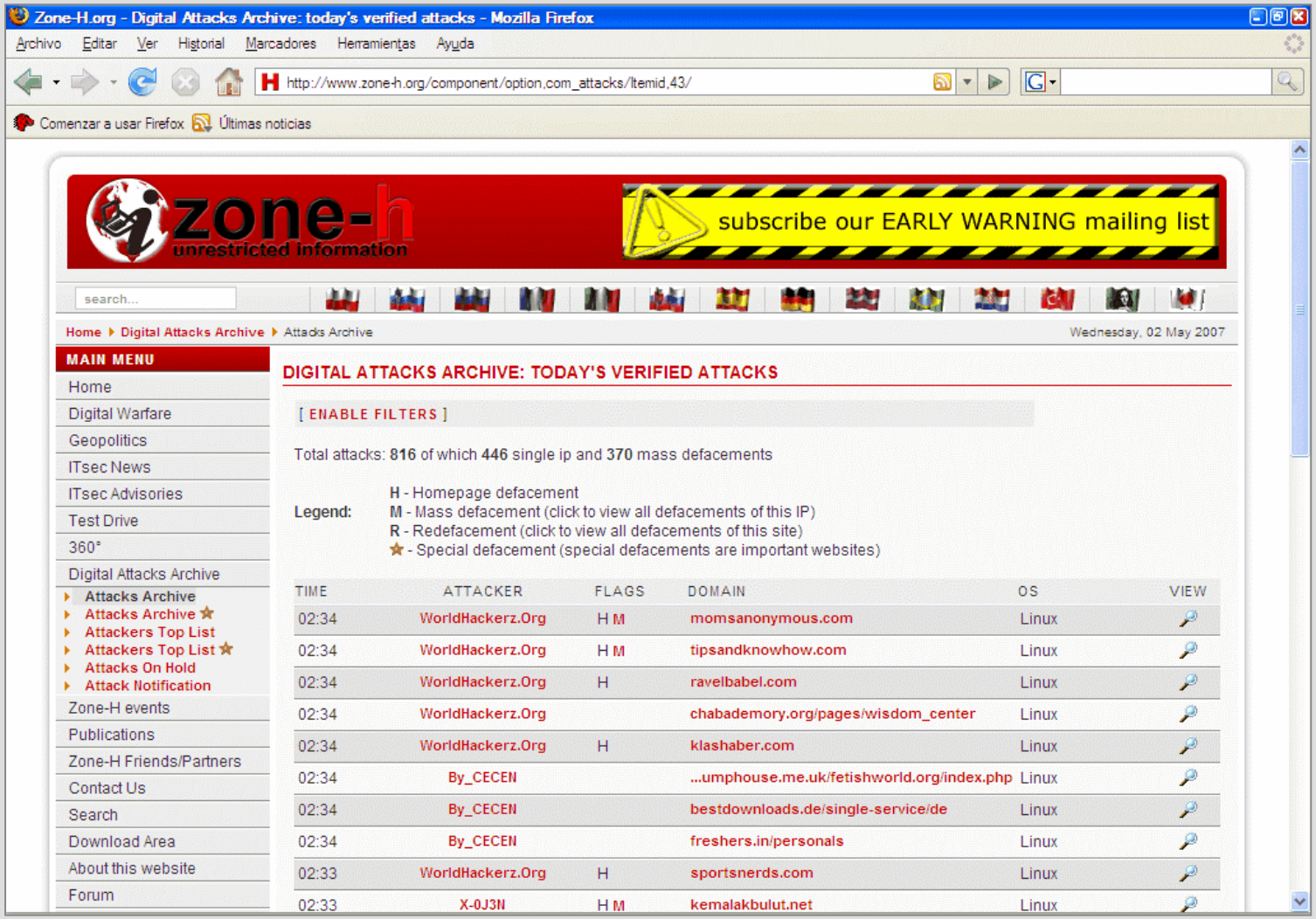
"…Their objective is to try to impress their friends or gain credit in underground cracker communities..." [Wikipedia]

"If you or your organization has any resources connected to the Internet, this threat applies to you ". [Honeynet Project]

Website *defacements*



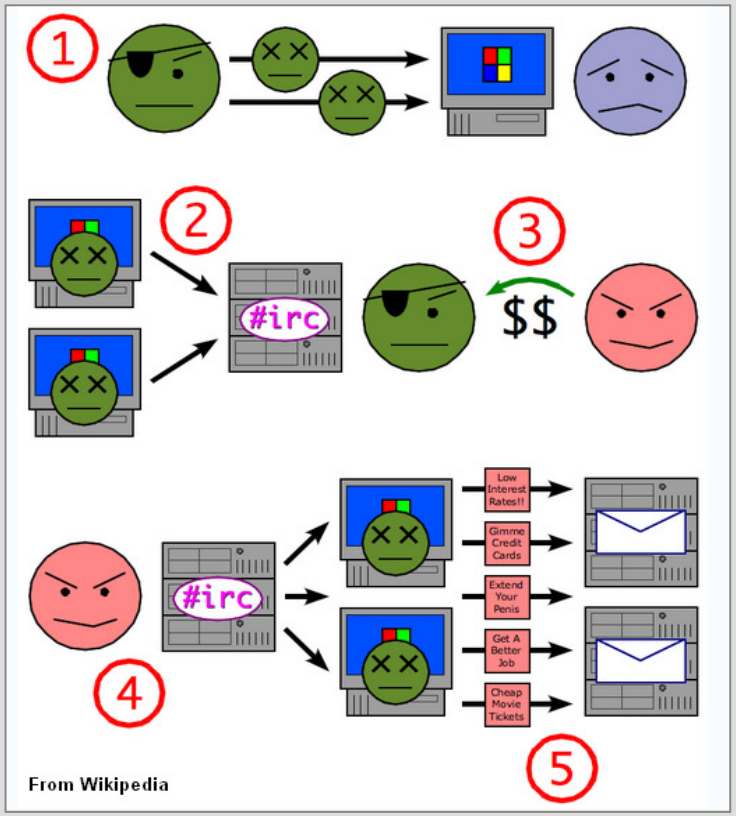
Website *defacements* archive



Botnets: the zombie-process

Diagram of the process by which spammers use zombie (virus-infected) computers to send spam:

http://en.wikipedia.org/wiki/Botnet



1. Virus writer sends out viruses, infecting ordinary users' Windows PCs.
2. Infected PCs log into an IRC server or other communications medium, forming a network of infected systems known as a botnet.
3. Spammer purchases access this botnet from virus writer or a dealer.
4. Spammer sends instructions to the botnet, instructing the infected PCs to send out spam.
5. The infected PCs send the spam messages to Internet users' mail servers.

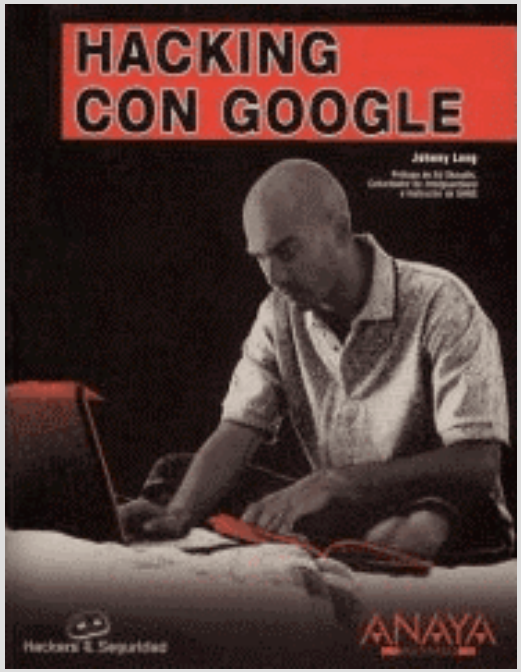
Low-level techniques

Googledorks, Google Hacking

–Using advanced search operators like Google, and other search engines, can be used to detect website vulnerabilities as well as to find private, sensitive information about others, such as credit card numbers, social security numbers, and passwords.

–**Johhny Long**

- *The googledorks database (1999-2004).*
- ***The Google Hacking Database*** *(from 2004).*
- *Google Hacking for penetration testers (2004).*



"Nowadays, pretty much any hacking incident most likely begins with Google." **[*Johnny Long*]**

URLs modification

```
http://john:secret@www.example.com:123/demo/example.cgi?country=us&state=ny#section1
Protocol  User  Password  Domain  Port  Path  Query  Anchor
```

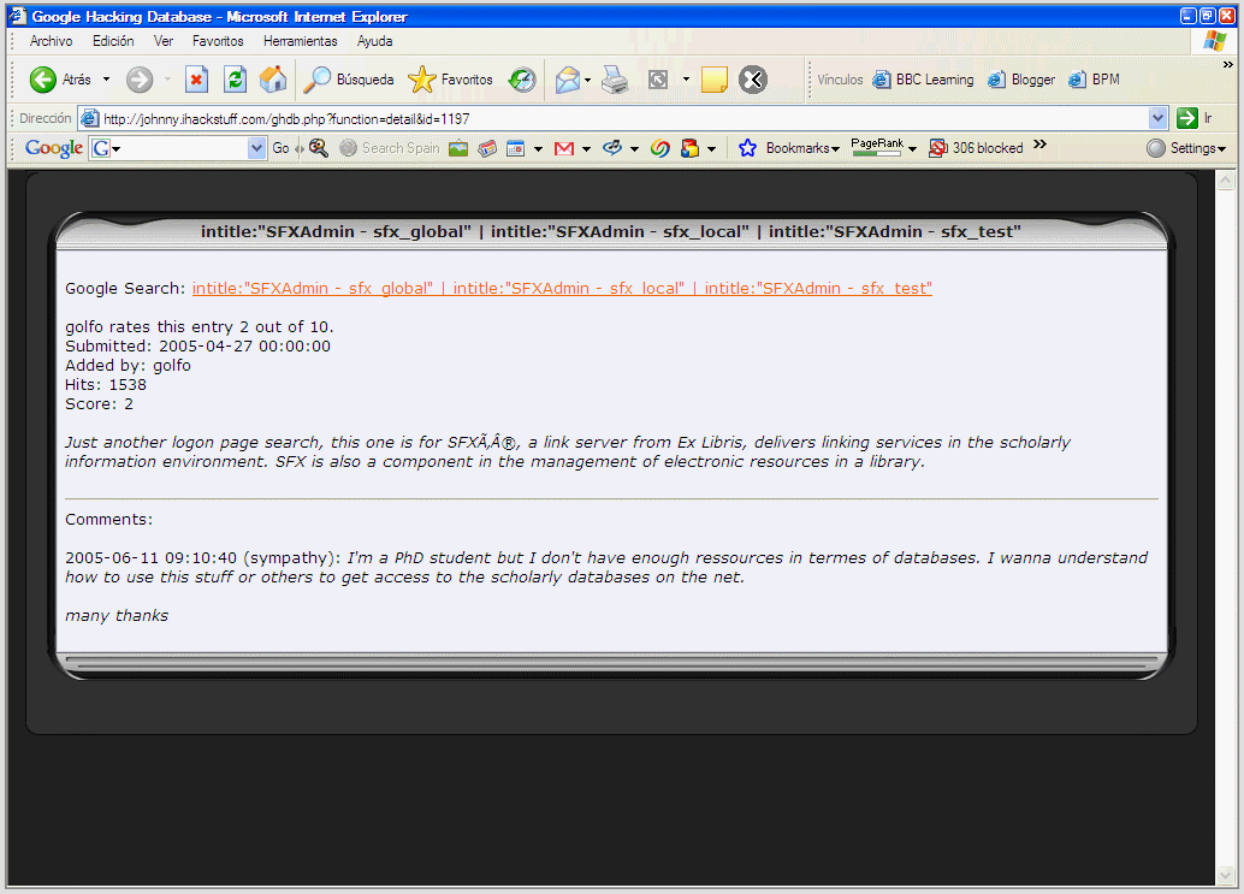
Password-guessing

Use of weak passwords.

"If everybody would enforce strong password policies... 90% of security problems would disappear..." [La Biblia del Hacker]

SFX-Admin on target

From 2005, SFX-Admin appears in *The Google Hacking Database*!



A padlock is a challenge

Every door is a potential security hole.

Every login page is a challenge to curiosity.

- –If it is locked, there must be something valuable behind.
- –Will it open easily?...

Why expose our implementations to these threats?

- –There is no need for our SFX-Admin to be easily located by anybody in the Net.
- –We should filter and control access to it.

"At last we achieve it... There is only one secure thing: the infinite insecurity of security". **[Wau Holland]**

Table of Contents

Casual origin of the study:

–Checking the operation of *HTTPs* in Spanish SFX implementations.

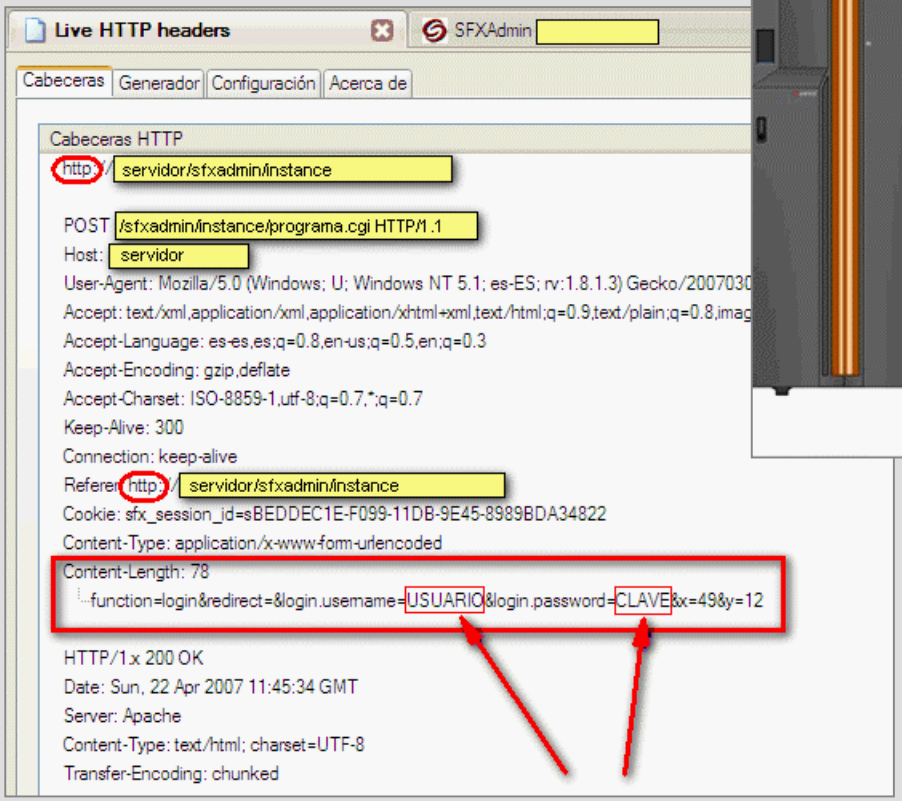
- *A question to our local distributor:*
  Why does HTTP *continue to be active if* HTTPs *are in operation?*

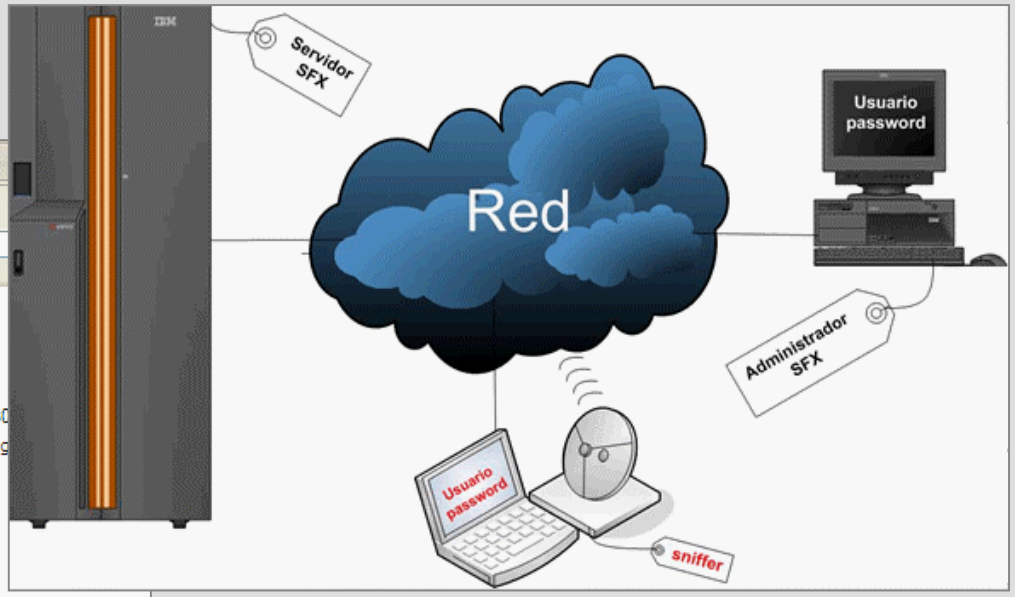
Could anybody locate and easily access SFX-Admins?

–Starting logical premises:

- *Access should be controlled.*
- *Localization by search engines should be avoided.*
- *It shouldn't be possible to locate it with simple URL modifications.*
- *It shouldn't be possible to access it with weak username-passwords.*

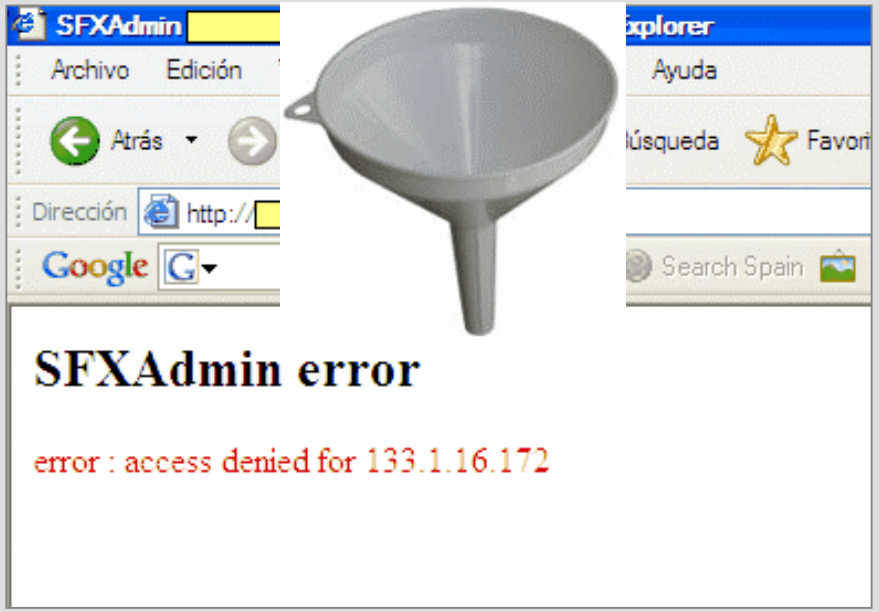
How do our passwords travel?





Is it being accessed only by those who ought to?

Access restriction by IP address filtering:

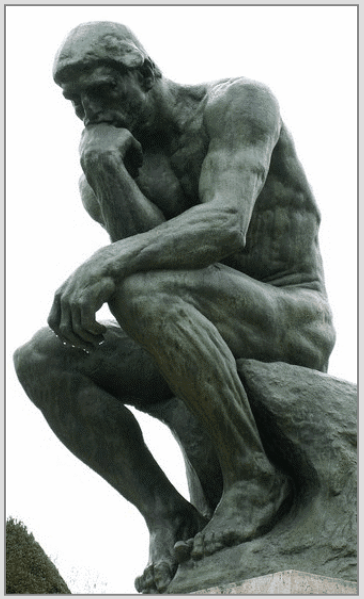


Location of SFX servers: limited sample.

- –Search limited to 2 sessions in a weekend = 129 international servers.
  - •*Nearly 10% of total SFX servers (1,481 in May 2007).*
  - •*Include all Spanish servers in production at that time (24).*
- –Use of low-level techniques.
  - •*Google, URLs modification.*
- –Anonymity of analysed servers.

Data analysis.

- –By wide geographical areas.
- –Typology according to vulnerability level.



2. Field study

***Hackers* (good and bad) are greedy readers.**

– *Hacking* books usually have more than 300 pages.

RTFM = *Read The Fucking (or Fine) Manual.*

– SFX User Guide (UG).

– SFX System Administrator Guides (SAG).

STFW = *Search The Fucking (or Fine) Web.*

Essential :

– Cooper, Jason (2006): ***Securing MetaLib & SFX***.
1st IGeLU Conference, Session 7b.
Stockholm, 5 September 2006.

© Biblioteca de Catalunya

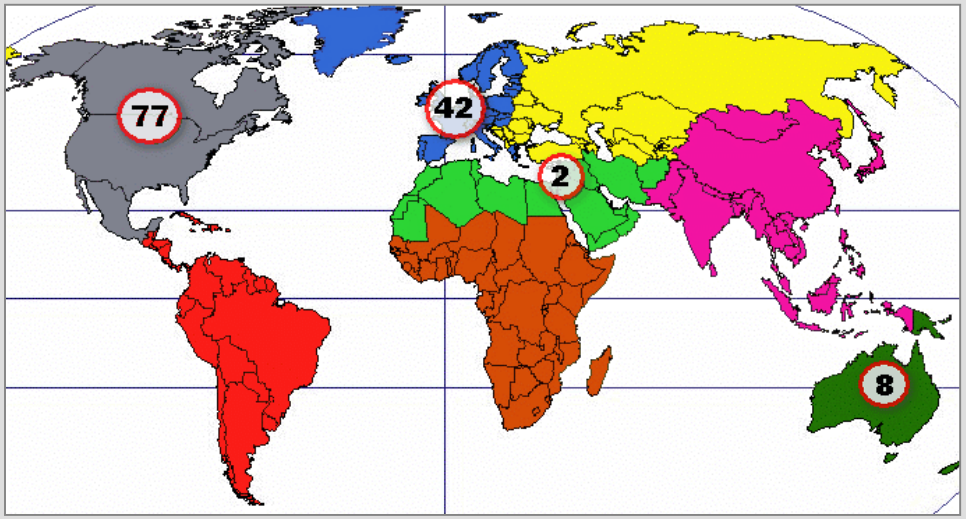
Geographical composition of the sample

EUROPE			
AT	1	0,8%	2,4%
CH	1	0,8%	2,4%
CZ	1	0,8%	2,4%
DK	2	1,6%	4,8%
FI	1	0,8%	2,4%
HU	1	0,8%	2,4%
IT	1	0,8%	2,4%
NL	3	2,3%	7,1%
PT	1	0,8%	2,4%
ES	24	18,6%	57,1%
GB	6	4,7%	14,3%
TOTAL	**42**	**32,6%**	100,0%

USA AND CANADA			
CA	2	1,6%	2,6%
US	75	58,1%	97,4%
TOTAL	**77**	**59,7%**	100,0%

OTHER AREAS			
AU	8	6,2%	80,0%
IL	2	1,6%	20,0%
TOTAL	**10**	**7,8%**	100,0%

TOTAL		
TOTAL	**129**	100,0%



Typology according vulnerability

	YES
[1] Are default instance names used?	1
[2] Is the site located with Google?	2
[3] Is only HTTP used to access?	4
[4] Is unrestricted IP access allowed?	8

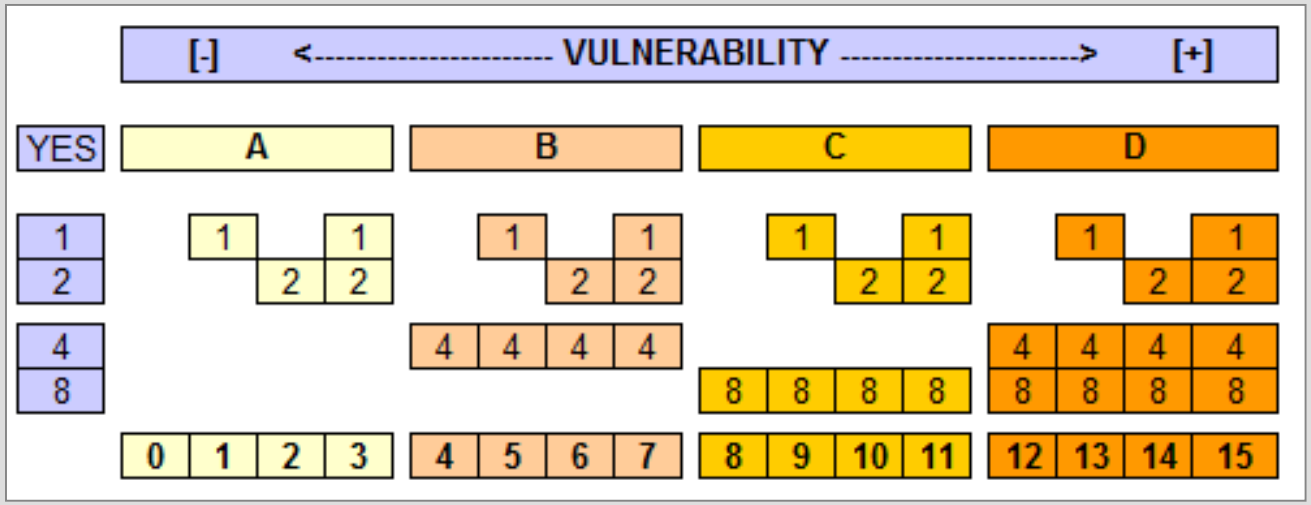


Table of Contents

Raw data

	[1]	[2]	[3]	[4]	[5]
Spain					
SI	6 25,0%	1 4,2%	24 100,0%	22 91,7%	11,7
NO	18 75,0%	23 95,8%	0 0,0%	2 8,3%	D
TOTAL	24 100,0%	24 100,0%	24 100,0%	24 100,0%	
Europe (without Spain)					
SI	17 94,4%	4 22,2%	18 100,0%	13 72,2%	11,2
NO	1 5,6%	14 77,8%	0 0,0%	5 27,8%	C
TOTAL	18 100,0%	18 100,0%	18 100,0%	18 100,0%	
USA and Canada					
SI	35 45,5%	68 88,3%	76 98,7%	71 92,2%	12,0
NO	42 54,5%	9 11,7%	1 1,3%	6 7,8%	D
TOTAL	77 100,0%	77 100,0%	77 100,0%	77 100,0%	
Other areas					
SI	6 60,0%	4 40,0%	10 100,0%	10 100,0%	13,4
NO	4 40,0%	6 60,0%	0 0,0%	0 0,0%	D
TOTAL	10 100,0%	10 100,0%	10 100,0%	10 100,0%	
Total (without Spain)					
SI	58 55,2%	17 16,2%	104 99,0%	94 89,5%	12,0
NO	47 44,8%	88 83,8%	1 1,0%	11 10,5%	D
TOTAL	105 100,0%	105 100,0%	105 100,0%	105 100,0%	
Total (included Spain)					
SI	64 49,6%	18 14,0%	128 99,2%	116 89,9%	11,9
NO	65 50,4%	111 86,0%	1 0,8%	13 10,1%	D
TOTAL	129 100,0%	129 100,0%	129 100,0%	129 100,0%	

Caption			
[1]	Are default instance names used?		YES = 1
[2]	Is the site located with Google?		YES = 2
[3]	Is only HTTP used to access?		YES = 4
[4]	Is unrestricted IP access allowed?		YES = 8
[5]	Typology / Average score (+ score = + vulnerability)	A	1 - 3
		B	4 - 7
		C	8 - 11
		D	12 - 21,5

Worrying conclusions

49% of installations have not changed the default names.

It is really easy to locate all the SFX-Admins.

- –Directly by Google (14%).
- –Indirectly by URLs modification (86%).

Access data are sent totally in the clear.

- –Only 1 installation (0,8%) uses HTTPs.

90% of the implementations allow anybody to access the Admin login page.

- –Only 13 installations (10%) use IP filtering.

Only 10% of servers have an acceptable security level.

- 12 of B level (use IP filtering).
- 1 of A level (use HTTPs and IP filtering).

Some odd surprises

¿?

Is it admissible on a production system that …

… all security relies exclusively on passwords?

… it provides direct link to the SFX-Admin of each library in a consortium?

…it limits access to SFX Journal Finder but not to SFX-Admin login page?

What about password strength?

The worst-case scenario

Suddenly...

- We can no longer access our Admin.
- We lose months-worth of work in the setup of targets and sources.
- Even worse, an intruder makes random changes during a long period of time without we realizing it.
- Other information in the same server has been compromised.
- We have become part of a malicious botnet.
- Our users can no longer access our electronic journals collection.
- The prestige of our institution is adversely affected.

Is it possible to react and recover quickly from an attack?

- Are we auditing the access logs?
- Do we have a good backup policy?

Table of Contents

Protect ourselves

"To keep silence even about the good things"
[The Rule of St. Benedict]

Prevent to be easily tracked down.

- –Avoid browser indexing: robots.txt.
- –Change default instances (SAG, p. 15).
- –IP filtering (SAG, p. 52).

Protect security information (passwords, etc.).

- –Change default user-password immediately after installation.
- –HTTPs instead of HTTP (SAG, p. 55).
- –Force strength password and employ password policies.
  - *Example:* Password Policy *(SANS Institute, 2006).*

More information in our post *Asegurar el acceso al SFXAdmin*:

- –http://manualillo.blogspot.com/search/label/Seguridad

Involvement

Ex Libris.

- More attention to the security of their products.

Distributors.

- More attention to the security of their implementations and specially when they are offering hosting services.

User groups.

- Discuss security issues at IGeLU PWGs.
- Request the necessary security enhancements of the products.

Ourselves.

- Demand responsibility for the security of our implementations from our providers.
- Consult security experts if we don't know the environment well enough.
- Define a security policy.

Improve: some proposals from Expania

1. **Pay attention to security in product manuals.**
2. **Change default instances and passwords after installation process.**
3. **Protect SFX-Admin against indexing by search engines.**
4. **Always use *HTTPs* and IP filtering.**
5. **Reduce failed login attempts to the minimum.**
6. **Limit *time-out* as much as possible.**
7. **Prevent access through "back button and refresh" after *log off*.**

Improve: proposals along the lines of Aleph 19

SCHECTER, Moshe (2007):

***Staff Permissions: Acces Rights and UI Workflow*.**

Ex Libris System Seminar, Potsdam, Germany. May 13-16, 2007.

– Enhanced Staff Password Control:

- *Set up expiration date for user accounts.*
- *Force password minimum length.*
- *Force combination of alpha and numeric characters.*
- *Force password change immediately after new user's first login.*
- *Disable non-active users past a specific threshold.*
- *Disable users after a fixed failed login attempts.*
- *Require periodic change of passwords.*
- *Prevent the re-use of old passwords.*

Basic checklist

Securing *S•F•X Admin* checklist

- [x] 1. Chose between close your eyes, pray, trust in your good luck... or get down to work on security
- [ ] 2. Have we read the manuals?
- [ ] 3. Have we changed default instance names?
- [ ] 4. Have we made anything to avoid search engines indexation?
- [ ] 5. Have we changed default users and passwords in all instances?
- [ ] 6. How many accounts we really need?
- [ ] 7. Have we got a password policy?
- [ ] 8. Have we configured HTTPs and disabled HTTP access?
- [ ] 9. Have we limited access by IP filtering?
- [ ] 10. Have we defined a procedure to supervise the *access logs*?
- [ ] 11. Have we got a solid backup policy?
- [ ] 12. Have we got a written and accepted security policy?
- [ ] ...

Final words

- **Internet could be a very hostile medium if we are not prepared.**
- **Attacks occur frequently and not always to others.**
- **Don’t forget to change default users-passwords of all instances.**
- **HTTPs increases security by encrypting information we exchange with the server.**
- **It is not safe to allow everyone to access to our SFX-Admin portal and rely exclusively on username-password for security.**
- **IP filtering is very easy to set up and increases security by controlling who can access the SFX-Admin.**
- **The involvement of everyone is needed in order to increase awareness about security and improve it.**
- **Ex Libris should enhance SFX security and include options allowing the definition of password policies.**