Monitoring pastebin.com

HITB Amsterdam 2012 - SIGINT

$ whoami

- Xavier Mertens (@xme)
- Security Consultant
- Security Blogger
- Volunteer for security projects:

EUROTR@SH
Security with Funny Accents

HACKING FOR B33R
BRUCON
WWW.BRUCON.ORG

$ cat disclaimers.txt

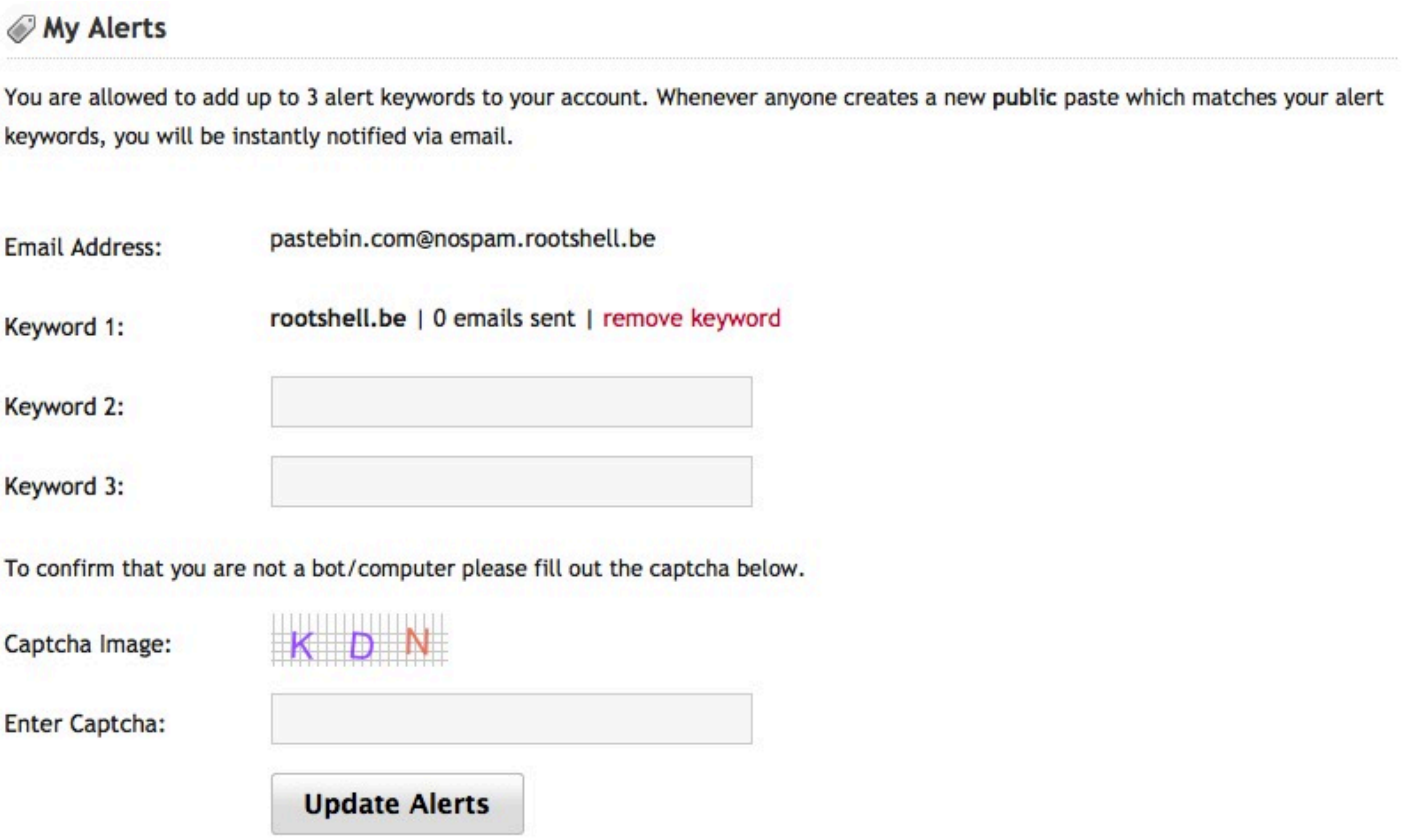
“The opinions expressed in this presentation are those of the speaker and do not reflect those of past, present or future employers, partners or customers”

“Do NOT flood pastebin.com”

pastebin.com

- Website where people can store text (a “pastie”) for a certain period of time (10 mins →∞)
- Focus on developers
- More and more used to spread interesting content anonymously
- ~ 1 new pastie every 2”

My Alerts?



My Alerts

You are allowed to add up to 3 alert keywords to your account. Whenever anyone creates a new **public** paste which matches your alert keywords, you will be instantly notified via email.

Email Address: pastebin.com@nospam.rootshell.be

Keyword 1: **rootshell.be** | 0 emails sent | remove keyword

Keyword 2:

Keyword 3:

To confirm that you are not a bot/computer please fill out the captcha below.

Captcha Image:

Enter Captcha:

What I needed?

- Continuous monitoring
- Regex powa!
- Alerting
- Open

pastemon.pl

- Based on Xavier Garcia's pastebin.py
- Written on Perl (I like Perl)
- Core features
    - Syslog output (CEF optional)
    - Dump original pastie (backup)
    - Display sample (x cars before/after the hit)
    - Wordpress XMLRPC output

Usage

```
$ ./pastemon.pl --help
Usage: ./pastemon.pl --config=filepath [--debug] [--help]
```

$ cat pastemon.conf

```
<!--
pastemon.pl main configuration file sample
Note: to disable a feature, comment it using "<!--" and "//-->"
//-->
<pastemon>
    <!-- Core features //-->
    <core>
        <ignore-case>yes</ignore-case>
        <pid-file>/var/run/pastemon.pid</pid-file>
        <regex-file>regex.conf</regex-file>
        <sample-size>256</sample-size>
        <proxy-config>proxies.conf</proxy-config>
        <dump-directory>/home/pastemon/dump</dump-directory>
        <http-timeout>15</http-timeout>
        <!-- Use Jaro-Winkler distance algorithm //-->
        <distance-min>0.95</distance-min>
        <distance-max-size>10240</distance-max-size>
    </core>
    <!-- CEF Output (ArcSight) //-->
    <cef-output>
        <destination>10.0.0.1</destination>
        <port>514</port>
        <severity>3</severity>
    </cef-output>
    <!-- Syslog Output //-->
    <syslog-output>
        <facility>daemon</facility>
    </syslog-output>
    <!-- Email Output //-->
    <smtp-output>
        <smtp-server>127.0.0.1</smtp-server>
        <from>pastemon@rootshell.be</from>
        <recipient>recipient@domain.com</recipient>
        <subject>PasteMon Alert</subject>
    </smtp-output>
    <!-- Wordpress Output (XMLRPC) //-->
    <wordpress-output>
        <site>www.myblog.com</site>
        <user>editor</user>
        <password>averystrongpassword</password>
        <category>favorite</category>
    </wordpress-output>
</pastemon>
```

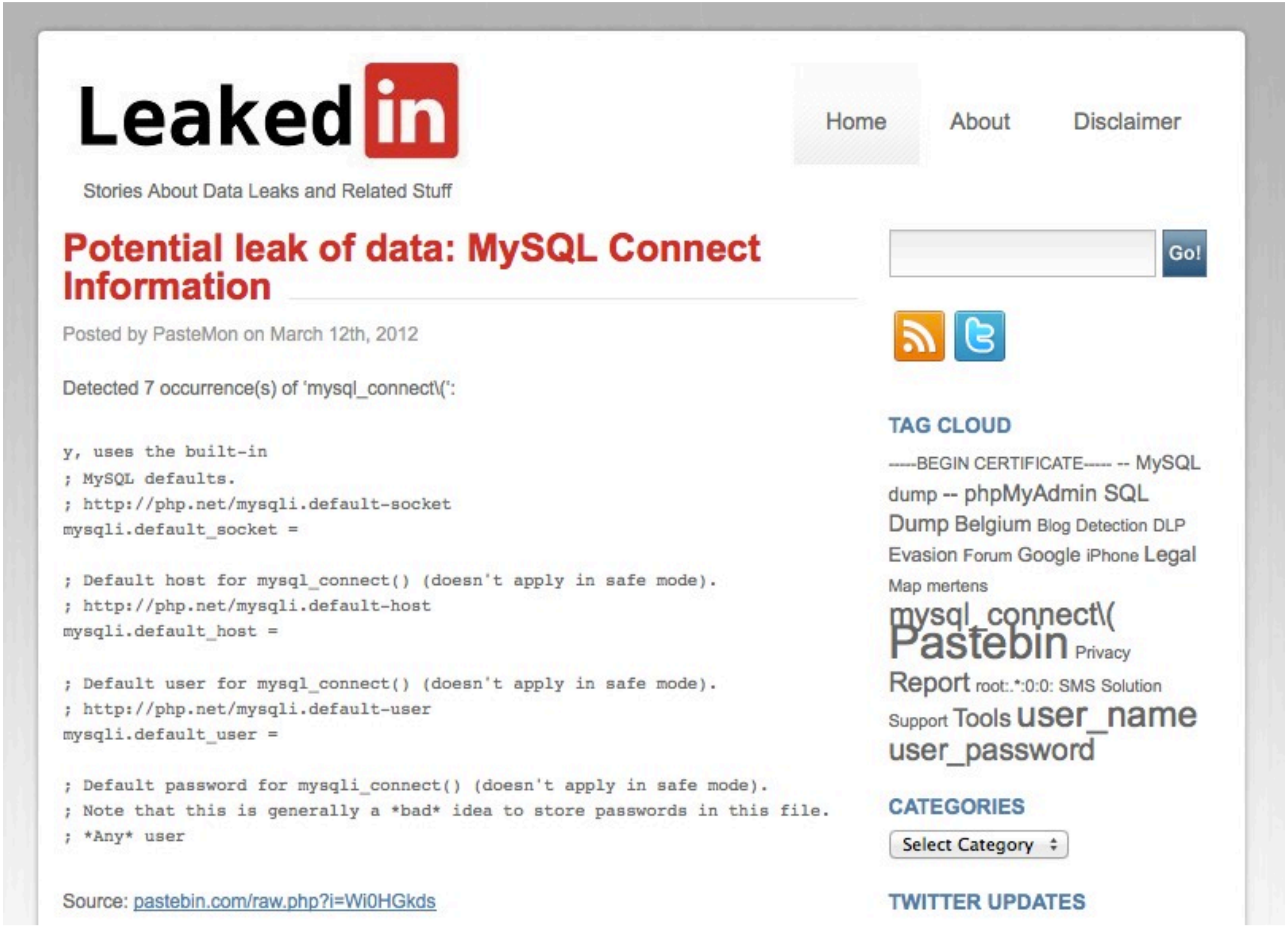
$ cat regex.conf

```
-----BEGIN RSA PRIVATE KEY-----
-----BEGIN DSA PRIVATE KEY-----
-- phpMyAdmin SQL Dump
-- MySQL dump
-----BEGIN CERTIFICATE-----
-----BEGIN PGP PRIVATE KEY BLOCK-----
\.HOIC
enable secret
encrypted password \".*\";
user_name
user_password
root:.*:0:0:
root:.*:0:99999:7:::
CN\=Admin
http://.*\:.*\@[a-zA-Z0-9-_].[a-zA-Z0-9-_]
ftp://.*\:.*\@[a-zA-Z0-9-_].[a-zA-Z0-9-_]
\?[a-zA-Z0-9-_]=.*UNION.*SELECT
mysql_connect\(
\.\.\/\.\.\/\.\.
```

Monitor Yourself!

- Your (nick)name
- Your logins
- Your IP addresses
- Your domains
- ...

leakedin.com


LeakedIn
Home
About
Disclaimer
Stories About Data Leaks and Related Stuff
Go!
TAG CLOUD
-----BEGIN CERTIFICATE----- -- MySQL dump -- phpMyAdmin SQL Dump Belgium Blog Detection DLP Evasion Forum Google iPhone Legal Map mertens mysql_connect\(Pastebin Privacy Report root:.*:0:0: SMS Solution Support Tools user_name user_password
CATEGORIES
Select Category
TWITTER UPDATES

Potential leak of data: MySQL Connect Information

Posted by PasteMon on March 12th, 2012

Detected 7 occurrence(s) of 'mysql_connect\(':

```
y, uses the built-in
; MySQL defaults.
; http://php.net/mysqli.default-socket
mysqli.default_socket =

; Default host for mysql_connect() (doesn't apply in safe mode).
; http://php.net/mysqli.default-host
mysqli.default_host =

; Default user for mysql_connect() (doesn't apply in safe mode).
; http://php.net/mysqli.default-user
mysqli.default_user =

; Default password for mysqli_connect() (doesn't apply in safe mode).
; Note that this is generally a *bad* idea to store passwords in this file.
; *Any* user
```

Source: pastebin.com/raw.php?i=Wi0HGkds

Future?

- Support for more “pastebin” sites (not easy)
- Granularity (report leak if # of occurrences > threshold)
- Suggestions are welcome!

Thank You!
Q&A?

http://blog.rootshell.be
http://twitter.com/xme