

Be first to know about data breach

max goncharov
gmax@gmax.at





RECORDS	DATE	ORGANIZATIONS
<u>220,000,000</u>	2014-08-22	Unknown Organization
<u>152,000,000</u>	2013-10-03	Adobe Systems, Inc.
<u>150,000,000</u>	2012-03-17	Shanghai Roadway D&B Marketing Services Co. Ltd
<u>145,000,000</u>	2014-05-21	eBay Inc.
<u>140,000,000</u>	2013-06-08	Unknown Organization
<u>130,000,000</u>	2009-01-20	Heartland Payment Systems, Tower Federal Credit Union, Beverly National Bank, North Middlesex Savings Bank, Golden Chick
<u>110,000,000</u>	2013-12-18	Target Brands, Inc., Fazio Mechanical Services, Inc.
<u>104,000,000</u>	2014-01-20	Korea Credit Bureau, NH Nonghyup Card, Lotte Card, KB Kookmin Card
<u>94,000,000</u>	2007-01-17	TJX Companies Inc.
<u>90,000,000</u>	1984-06-01	TRW, Sears Roebuck

<http://pastebin.com/YUjExprE>

adam@em-b.co.uk	c694b125b35f7305bdc0201a3ecb31fb
ADAM@DUNLEYHOUSE.CO.UK	0f7751f2340cea4072259463f954c0ef
ADAM@DUNLEYHOUSE.CO.UK	0f7751f2340cea4072259463f954c0ef
Adam@directfoodexpress.co.uk	5d1597dd0790e336bea5402e99cdc421
adam@directfoodexpress.co.uk	56b262dbbc82d8ad2df1c3e1e01166e0
adam@crawfordadam.wanadoo.co.uk	4d4cee34b3df4a5db210cf13cbcdb2b8
adam@crawfordadam.wanadoo.co.uk	4d4cee34b3df4a5db210cf13cbcdb2b8
adam@casinopromotions.com.au	c50aaa4b8624a9517f98579a979afd9d
adam@candystudios.tv	3d796d8f8acd583e6395a92e117d5069
adam@brough95.fsnet.co.uk	8a52072cee5d17cc7bf85d6ca431fffa
adam@brightfla.me	c02d5c76483cf8ea55afb3c66082e748
adam@brightfla.me	4442eaef72feac05644a2a01363c45e2
adam@bodytronix.co.uk	bb1b3afdd7a02c88749d70a37cf624ef
adam@blurred.fsnet.co.uk	bb343fd97bebe9ae663daa703d45d8c1
adam@binners.co.uk	e9d27b09ef8daf3ef374e86e3231d22a
adam@bigbrothersite.co.uk	ca6b95b7e10ea197fe307bb7597f61f3
adam@benchmedia.co.uk	b60e7926d9ce0dfbc46af0376f43845f
adam@aquacooling.co.uk	e1021d76614afd8e166c043c2b4b8369
adam@am-photo.co.uk	053d4a40064c52e36a2221fe02be9964
adam@aevals91.orangehome.co.uk	4a8bfff75f89865bdc7f60b49a24753b
adam@adm-rec.co.uk	12f3af41c1c8c220afc3eb23961dde42
adam@adbmax.fsnet.co.uk	452d52139db6db3faff7a67ceeb83531
adam@adamish.com	6d02fa5cdf201d481434c74effdab2b6
adam@acs-cabins.co.uk	e790a1d73db268d31ee9c003cb7b3e73
adam@acgszr.freeseve.co.uk	ee2055701c742262f93d083f854350b9
adam@7410.co.uk	f14952d859b352735ecd17f72ed0fc9f
adam.z@live.co.uk	46a46b0a267201c0c742cee54685d62c
Adam.Young@express-gifts.co.uk	b9b507acdaa100f6590fda3779d15e99
adam.yates@doctors.org.uk	7c8ef330233c0b9cc60f11ff279ab984
adam.xland@hotmail.com	a19e1eeb71e35d213a3d585dae457cec
adam.wrestch@hotmail.com	16bff73d63a1632439fdcc8fc8ce6e2c

Structure of *usual* data leak

Password

user name

email

plain text

plain text

plain text

Hash

Hash + salt

Structure of *possible* data leak

Password

user name

email

file

plain text

plain text

plain text

document

Hash

image

Hash + salt

media

DARK MONEY

Everything can be cashed out!



Темы раздела : [Документы/сканы/базы данных](#) Опции раздела [v](#) Искать в этом разделе

	Тема / Автор	Рейтинг	Последнее сообщение	Ответов	Просмотров
	Важно: Продажа сканов/снилс/вод.уд/инн/загран (1 2 3 ... Последняя страница) aurelio00000	★★★★	Сегодня 14:54 от aurelio00000 >	<u>98</u>	4,791
	Важно: Техосмотр авто! Любые категории ТС. (Диагностические карты) TO.online	★★★★	Сегодня 13:47 от Sipoka >	<u>3</u>	139
	Важно: Сканы РУ 1 у.е. - штука! (1 2 3 ... Последняя страница) Viktor V	★★★★	Сегодня 12:55 от Viktor V >	<u>177</u>	8,857
	Важно: Отрисую сканы документов (1 2 3 ... Последняя страница) Fedor	★★★★	Сегодня 12:37 от Fedor >	<u>143</u>	12,837
	Важно: переклей ПАСПОРТа VIP качества legionem	★★★★	Сегодня 00:36 от Offelia >	<u>3</u>	118
	Важно: Пеереклей Паспортов РФ (1 2) Pasov	★★★★	Сегодня 00:10 от Offelia >	<u>19</u>	4,899
	Важно: Сервис по продаже сканов паспортов и дополнительных документов (1 2 3 ... Последняя страница) Трофим	★★★★	17.10.2014 11:29 от Трофим >	<u>392</u>	13,913
	Важно: Замена фотографии в Паспорте РФ (переклей). (1 2) halve	★★★★	14.10.2014 14:15 от Offelia >	<u>16</u>	2,315
	Распродажа Фото паспортов по 30 руб. (1 2 3 ... Последняя страница) Liberum	★★★★★	Сегодня 14:54 от Liberum >	<u>55</u>	2,151
	Продам сканы Украины. (1 2 3) ...	★★★★	Сегодня 14:38 от ... >	<u>29</u>	650
	Продам паспорт РФ Liberum	★★★★	Сегодня 14:28 от Liberum >	<u>0</u>	8
	Рисую документы, карты, биллы и многое другое (1 2 3) fenrion	★★★★	Сегодня 13:58 от fenrion >	<u>24</u>	3,547
	Продаю сканы паспортов - РФ, Украина, фото паспорт в руках, также продам базу сканов (1 2 3 ... Последняя страница) blizard	★★★★	Сегодня 13:38 от blizard >	<u>34</u>	1,028
	Продам сканы паспортов + комплекты Россия, Украина, Заграница. (1 2 3 ... Последняя страница) dioltóra	★★★★	Сегодня 13:23 от dioltóra >	<u>143</u>	4,699
	Продам паспорт гр. Укр	★★★★	Сегодня 12:19	<u>0</u>	0

Wouldn't be possible
to trace leak ?

spam
again



Create your Google Account

One account is all you need

A single username and password gets you into everything Google.



Take it all with you

Switch between devices, and pick up wherever you left off.



Name
First Last

Choose your username
 @gmail.com

Create a password

Confirm your password


Birthday
Month Day Year

Gender
I am...

Mobile phone

Your current email address

Prove you're not a robot
 Skip this verification (phone verification may be required)


Type the text:

Location

I agree to the [Google Terms of Service](#) and have read the [Privacy Policy](#).

[Learn more](#) about why we ask for this information.

Create your Google Account

One account is all you need

A single username and password gets you into everything Google.



Take it all with you

Switch between devices, and pick up wherever you left off.



Name
First Last

Choose your username
 @gmail.com

Create a password

Confirm your password

Birthday
Month Day Year

Gender

ol70r82x36hl6fuwcbmls1135@gmail.com

Prove you're not a robot
 Skip this verification (phone verification may be required)

Type the text:

Location
Germany (Deutschland)

I agree to the Google [Terms of Service](#) and have read the [Privacy Policy](#).

[Next step](#)

[Learn more](#) about why we ask for this information.

ol70r82x36hl6fuwcbmls1135@gmail.com



in:spam



Mail

Mail navigation buttons: checkboxes, refresh, More

1-50 of 70

Navigation arrows and settings gear

Delete all spam messages now (messages that have been in Spam more than 30 days will be automatically deleted)

COMPOSE

Inbox (11,595)

Important

Sent Mail

Drafts

Spam (69)

Follow up

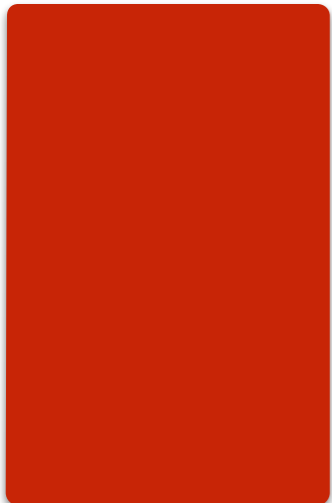
Misc

Priority

More

Contact search buttons: profile icon, search, refresh

Search people...



<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Olga	Why we stopped our communication? "I expected more, Olga! - Hey, why do not you write? You forgot about me? "I am v	2:47 pm
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Bank of America Merrill .	Bank of America Merrill Lynch - MasterCard SecureCode Profile Update Confirmation - [REDACTED]	10:43 am
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Olga	Why we stopped our communication? "I expected more, Olga! - Hey, why do not you write? You forgot about me? "I am v	Oct 19
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Marina	Hey - tell me your mobile - Marina from Russia. - Hello dear, do you remember how we communicated with you? Long ago	Oct 18
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Sports.ru	Почему сборную России не ждет ничего хорошего и как первый Гран-при России смотрелся вж... - Sports.ru дер	Oct 17
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Marina	Hello, my gentle sun, let's talk. - Hello dear, do you remember how we communicated with you? Long ago you could not see	Oct 16
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	RIW 2014	Новости RIW: новый формат, укрупнение, регистрация участников - Максим, здравствуйте! Регистрация на RIW 2	Oct 16
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Spor	RIW 2014 users@russianinternetweek.ru	Oct 15
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Vale	го появилось на Sports.ru за месяц - Хотим рассказать вам о полезных вещах, котор	Oct 15
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	—RU	y calm and well-balanced young lady. I do not like empty panic and never make fuss. I am	Oct 15
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Barr	- RUNET ID 194165 Максим, здравствуйте! Мы продолжаем анонсировать самые значи	Oct 14
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Ihr Geschenk	Add to contacts Emails	Oct 13
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Helena	Einmal, zweimal, dreimal so viel Geld - Schnappen Sie sich Ihren Ruby Palace Willkommensbonus heute und Sie können ll	Oct 13
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Ekaterina	Do you have web cam? Look at my pretty body! - My name is Helena, i'm looking for online sex partner, find me on http://n	Oct 11
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	weg.de - Gut beraten, be.	Look at my pretty Russian pussy! - Hi! My name is Ekaterina, photo of my pussy here http://rusdatingdd.ru nickname Ekate	Oct 11
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Ekaterina	Entdecken Sie die Welt: Traumziele zu TOP Preisen - Falls Sie unseren Newsletter nicht oder nur teilweise sehen können,	Oct 11
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Dewey White	Look at my pretty Russian pussy! - Hi! My name is Ekaterina, photo of my pussy here http://rusdatingdd.ru nickname Ekate	Oct 11
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		Read this now - Hi gmax, I got your voicemail yesterday about the stock tip you want, sorry I couldnt pick up the	Oct 10





o170r82x36hl6fuwcbmls1135@gmail.com

Web Site Compromise?

You or your recipients infected?

Web site sells your email address?

MitM on SMTP relays

You or your recipients infected?



LATEST INSTANCE OF PONY BOTNET PILFERS \$200K, 700K CREDENTIALS

You or your recipients infected?

Pony

BitCoin

FeatherCoin

eMails

LiteCoin

Passwords

You or your recipients infected?



Web site sells your email address?



easymoney1

Investor

Join Date :
Location :
Posts :

Jan

Email 80 Million - No Spam Complaints - 100% Resale Rights

Introducing the most powerful Email Blast products on the net- LET YOU ADVERTISE TO 80 MILLION EVERY MONTH.

PLUS Get 100% Resale Rights when you Join Today! And Keep All the Money From Sales!

Want to Increase your Web Traffic & Sales Overnight? Trying to Reach Targeted AUDIENCES DAILY?

80 MILLION MAILER MAKES IT POSSIBLE! AND WILL EXPLODES YOUR SALES OVERNIGHT!

(New Update Version) This mailer is very HOT on the net! Grab your membership today and your're granted with 100% resell rights to keep all the money from sales!

This is the most cost effective and reliable way to do email marketing.

No Validating Emails, 1-Click - Spam-Free!

100% safe, 100% legal, 100% bulletproof. You can not ever be accused of spam!

Type Your Ad, Click Send, You're Done!

IMAGINE YOUR SUCCESS ONLINE WITH THIS TOOL.

Web Site Compromise?

LinkedIn



PASTEBIN

6.5 million



InsidePro
PASSWORD RECOVERER SOFTWARE

MaKa 0th June 2012, 11:18

The LinkedIn database containing user credentials for over 6.5 million people, has been leaked on a Russian forum.

All passwords are stored in an unsalted SHA-1 format, meaning automated password guessing attacks are trivial to pull off. According to researchers the leak seems to be from 6-7 months ago, meaning it's not a recent attack in Internet time.

Users should change their LinkedIn password to a new complex password that's not used anywhere else.

The issue has most likely not been fixed yet, meaning passwords are still stored in the unsalted SHA-1 format.

Update:
LinkedIn is looking into the issue, but hasn't confirmed anything at this point in time.

References:
<http://forum.insidepro.com/viewtopic.php?t=14909>
Leaked Database: <http://r0ck.ru/d/56Hq-SK1ARpN>

MitM on SMTP relays

Open Systems Interconnection model (OSI)

OSI Model

	Data unit	Layer	Function
Host layers	Data	7. Application	Network process to application
		6. Presentation	Data representation, encryption and decryption, convert machine dependent data to machine independent data
		5. Session	Interhost communication, managing sessions between applications
	Segments	4. Transport	Reliable delivery of segments between points on a network.
Media layers	Packet/Datagram	3. Network	Addressing, routing and (not necessarily reliable) delivery of datagrams between points on a network.
	Bit/Frame	2. Data link	A reliable direct point-to-point data connection.
	Bit	1. Physical	A (not necessarily reliable) direct point-to-point data connection.



<http://leaktrap.com>

rfcapscz@mashmet.com



SMTP
mashmet.com



<http://leaktrap.com>

2014 max goncharov gmax@gmax.at

Web Resources

Web Resources



[decoy]@mashmet.com

REGISTER

[decoy]@mashmet.com

SMTP



<http://leaktrap.com>

2014 max goncharov gmax@gmax.at



www.verycoolsite.com

www.verycoolsite.com



dkcnqjnasakdasmdnc@mashmet.com

REGISTER

dkcnqjnasakdasmdnc@mashmet.com

SMTP



<http://leaktrap.com>

2014 max goncharov gmax@gmax.at



www.verycoolsite.com

www.doodlebox.com



dkcnqjnasakdasmdnc@mashmet.com

REGISTER

dkcnqjnasakdasmdnc@mashmet.com

SMTP



<http://leaktrap.com>

2014 max goncharov gmax@gmax.at



www.verycoolsite.com



dkcnqjnasakdasmdnc@mashmet.com



REGISTER





<http://leaktrap.com>

2014 max goncharov gmax@gmax.at

PASTEBIN | #1 paste tool since 2002

 **PASTEBIN**  Follow @pastebin  Like 189k

 create new paste  trending pastes

ad@temperleytaylor.co.uk	446f6c4111ab062dc71ff33700256153
ad@sina.com	0cc175b9c0f1b6a831c399e269772661
ad@mrbschumag.com	a53bc32f686de414475eabad41b2408a
ad@dorseteye.com	2a962b1e31cf46c115614cc3a096ecfc
ad@dixonuk.com	acc6bc5fb4b231ac595f92994d6597f0
ad.yg@hotmail.co.uk	3d08378c8d7c0a12241a2cb7d20d3246
ad.sargent@btinternet.com	79d8e340812f9db0bbfa508beb319dea
	6a85a21
	d184288
	1b918f2
ad.jarratt@gmail.com	173a90c6c2046d5169994d47c411ebb8
ad.hussain_786@hotmail.com	9766105f225adfe30d7746b904715bcd
ad.croston@hotmail.co.uk	84f9bd6d9aa4b91abdfd0a8b0204c9fc
ad.c@manx.net	f42087059b37ae7f4d9f0d3a475801a8
acyoung@onetel.com	3d1a2bb1df572f0297ae9ca43e006806
acy07@imperial.ac.uk	903010ac03abcc015f3f5227a392bd91
ACWOOD311@AOL.COM	29c37b51961d0fff9ea88a3ae90dc357
acwjlw@hotmail.co.uk	848069be239e0652978632c56c11b487
acwilkins@sky.com	298ceb77e3d9745fda2b1c8fdbee9a11
acwfp@btinternet.com	e11e8468cdf6044d9217ef7c7b9eae15
ACWallace@slb.com	b170db437a000d09b0a6d1f3bcd419b7
472@talktalk.net	8c7c9b1149e9de712b9e5abab45d700c
ada-1991@hotmail.com	7d184f84f392c16bae56367a04b669a5
ada-1991@hotmail.com	9766105f225adfe30d7746b904715bcd
ada0998@hotmail.co.uk	23ebc13f3c0c1adcb7dcc17f1e2c815d
ada.rzepska@yahoo.co.uk	c2d628ba98ed491776c9335e988e2e3b
adbmax.fsnet.co.uk	452d52139db6db3faff7a67ceeb83531
sh.com	6d02fa5cdf201d481434c74effdab2b6
acs-cabins.co.uk	e790a1d73db268d31ee9c003cb7b3e73
acgszr.freemove.co.uk	ee2055701c742262f93d083f854350b9
7410.co.uk	f14952d859b352735ecd17f72ed0fc9f
z@live.co.uk	46a46b0a267201c0c742cee54685d62c
Young@express-gifts.co.uk	b9b507acdaa100f6590fda3779d15e99
yates@doctors.org.uk	7c8ef330233c0b9cc60f11ff279ab984
wrestch@hotmail.com	16bff73d63a1632439fdcc8fc8ce6e2c
woodhouse@yahoo.co.uk	c1cac8ec37e38f0fe6aad67f3888c4eb

dkcnqjnasakdasmdnc@mashmet.com





<http://leaktrap.com>

2014 max goncharov gmax@gmax.at



<http://leaktrap.com>

register

login

generate decoy email

pdkvnwm@mashmet.com

<http://coolwebsite.com>

use decoy email on web site

confirm entered data

web site / url /comment

Monitor data on used decoy email

<http://leaktrap.com>

2014 max goncharov gmax@gmax.at





SERVER DE

TECH NOW

Pastebin Crawl

LAMP

SMTPd Sink

Spam Check

<http://leaktrap.com>

2014 max goncharov gmax@gmax.at





**EMAIL
+
PASSWORD
DECOY**

FILE DECOY

FUTURE

TEXT DECOY

**MEDIA
DECOY**



gmax ▾

About ▾

Inbox

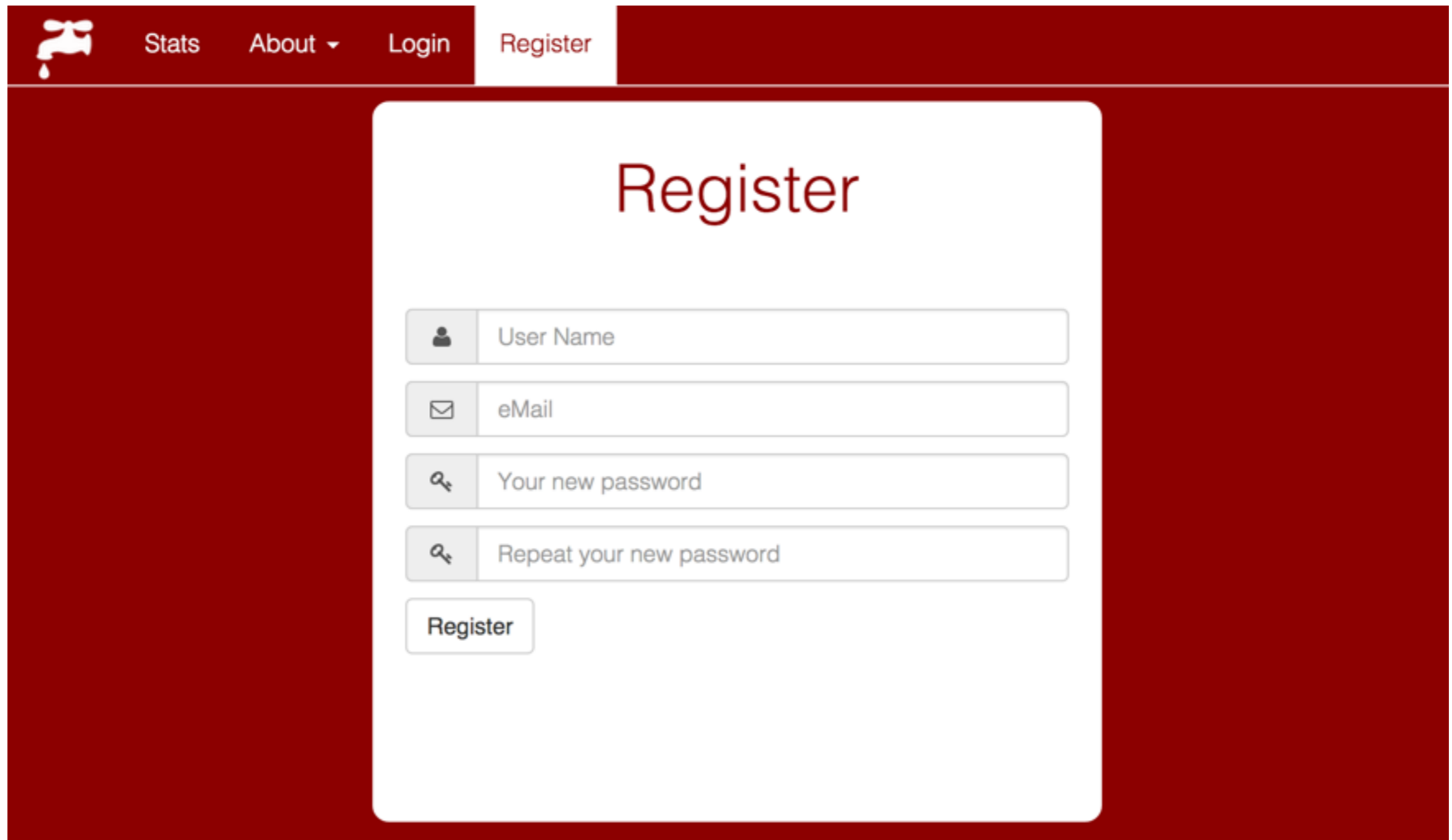
Email decoys

Add decoy

DEMO

<http://leaktrap.com>

http://leaktrap.com



Stats About Login Register

Register

User Name

eMail

Your new password

Repeat your new password

Register

http://leaktrap.com

Stats About Login Register

Sign in

Email address or user name

Password

[Forgot my Password](#) | [New to Leaktrap?](#)

Keep me logged in!

Sign in

<http://leaktrap.com>

2014 max goncharov gmax@gmax.at

http://leaktrap.com

gmax ▾ About ▾ Inbox Email decoys Add decoy

gmax's Inbox

From	To	Service	DKIM	SPAM	When
aol.com	tonxycnicl@mashmet.com	engadget.com	DKIM	checking	Today
warriorforum.com	mjjuwbnogo@mashmet.com	warriorforum.com	DKIM	checking	Yesterday
target.com	bcfwsyrmls@mashmet.com	target.com	DKIM	checking	Yesterday
mktomail.com	vanya.todds@mashmet.com	recode.net	None	checking	Yesterday
walmart.com	ljxjdngsu@mashmet.com	walmart.com	DKIM	no spam	Yesterday
habrahabr.ru	sfujkwfjfy@mashmet.com	tmtm.ru	DKIM	spam	Yesterday
aol.com	tonxycnicl@mashmet.com	engadget.com	DKIM	no spam	Yesterday

http://leaktrap.com

2014 max goncharov gmax@gmax.at



SLIPPERY
WHEN
WET



END