What You Can Learn from Bad Guys and Hackers About Cracking Passwords (Sanitized)

Rick Redman
Senior Security Consultant
KoreLogic, INC

Intro:

Rick Redman – KoreLogic (rredman@korelogic.com)
Senior Security Consultant

Penetration Tester
Vuln Assessments
Web Application Security Tester
Password Researcher

Creator of 'Crack Me If You Can' password cracking Contest at DEFCON.

@CrackMeIfYouCan on twitter.com

Speaker at: Derbycon, DEFCON, BSides, Techno Forensics Conferences, Austin Hackers Anonymous, ISSA Meetings.

What you can learn...

Idea:
The best source of data for password research...
Is leaked passwords.

5 years ago – there was little/no public password leaks

Now? Approx 170 million passwords/hashes leaked
In the last 12 months.

Why do this? Wordlists and Patterns.
Brute Forcing is a very “old method” - not logical.

Are **YOUR** users at risk ? Have **YOUR** users been leaked?
(Insert stories here..)

As Auditors...

Password audits help you identify risk. So do it correctly.

Go back and review policies and standards and make sure the advice to end-users is appropriate and correct.

When making recommendations – make sure you remember what we talk about today. The landscape is changing. Rethink your policies.

Points such as “what hash format do you store your users' passwords in” used to not be a big issue on an audit. Someone go ask LinkedIn if its a big issue there or not. (All sarcasm intended)

What you can learn...

Idea:

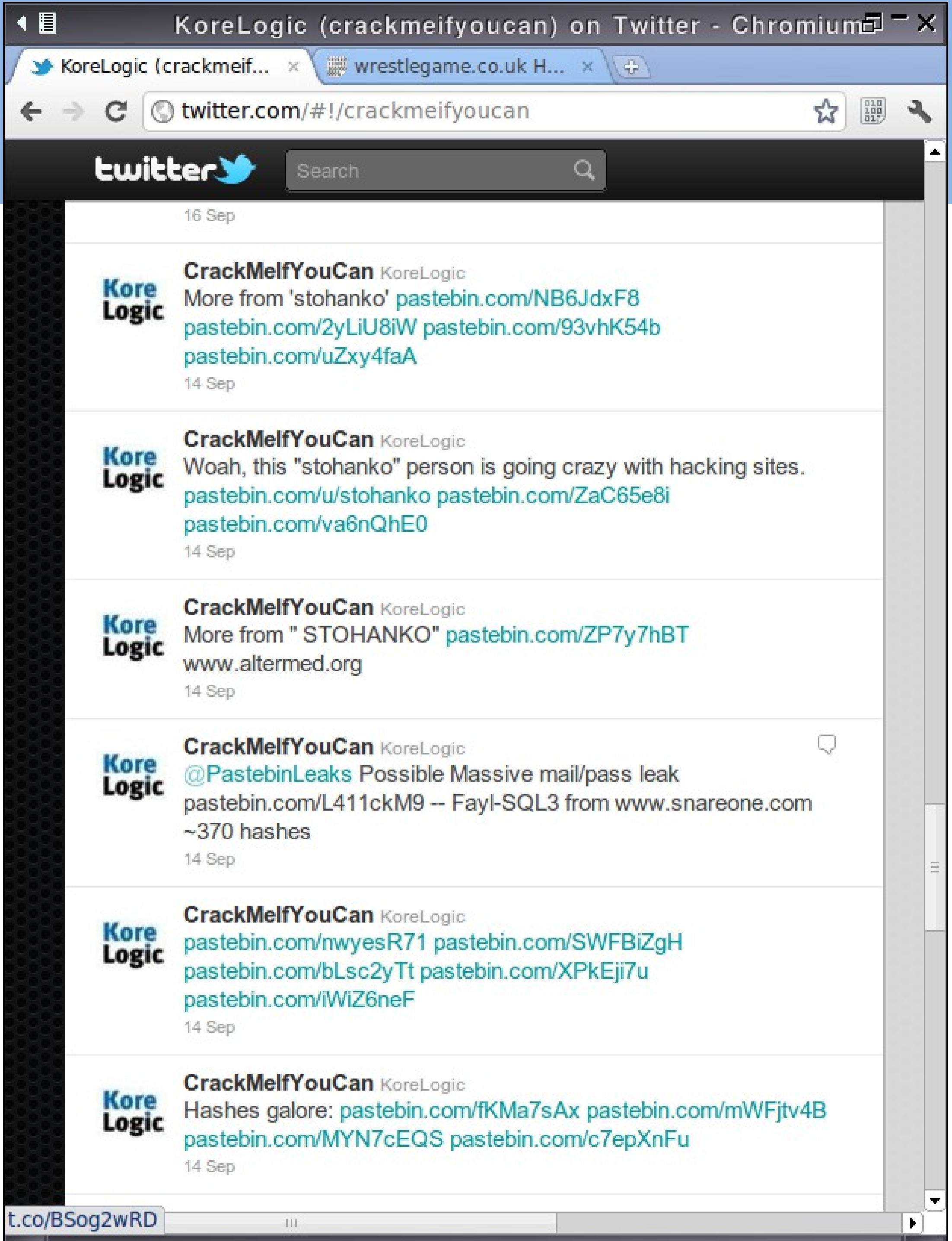
If we can do research off this public data, why can't we do the same research on our own internal passwords?

How do I do that? (dump hashes – start cracking)

- Pattern analysis (Numbers / Specials / Words)
- Which wordlists work the best?

Do UNIX passwords match Windows passwords?

- What if they are 1 'digit' different ?
- What if they rotate ? Or switch back and forth?


KoreLogic (crackmeifyoucan) on Twitter - Chromium
KoreLogic (crackmeif...
wrestlegame.co.uk H...
twitter.com/#!/crackmeifyoucan
twitter
Search
t.co/BSog2wRD

16 Sep

CrackMeIfYouCan KoreLogic
More from 'stohanko' pastebin.com/NB6JdxF8 pastebin.com/2yLiU8iW pastebin.com/93vhK54b pastebin.com/uZxy4faA
14 Sep

CrackMeIfYouCan KoreLogic
Woah, this "stohanko" person is going crazy with hacking sites. pastebin.com/u/stohanko pastebin.com/ZaC65e8i pastebin.com/va6nQhE0
14 Sep

CrackMeIfYouCan KoreLogic
More from " STOHANKO" pastebin.com/ZP7y7hBT www.altermed.org
14 Sep

CrackMeIfYouCan KoreLogic
@PastebinLeaks Possible Massive mail/pass leak pastebin.com/L411ckM9 -- Fayl-SQL3 from www.snareone.com ~370 hashes
14 Sep

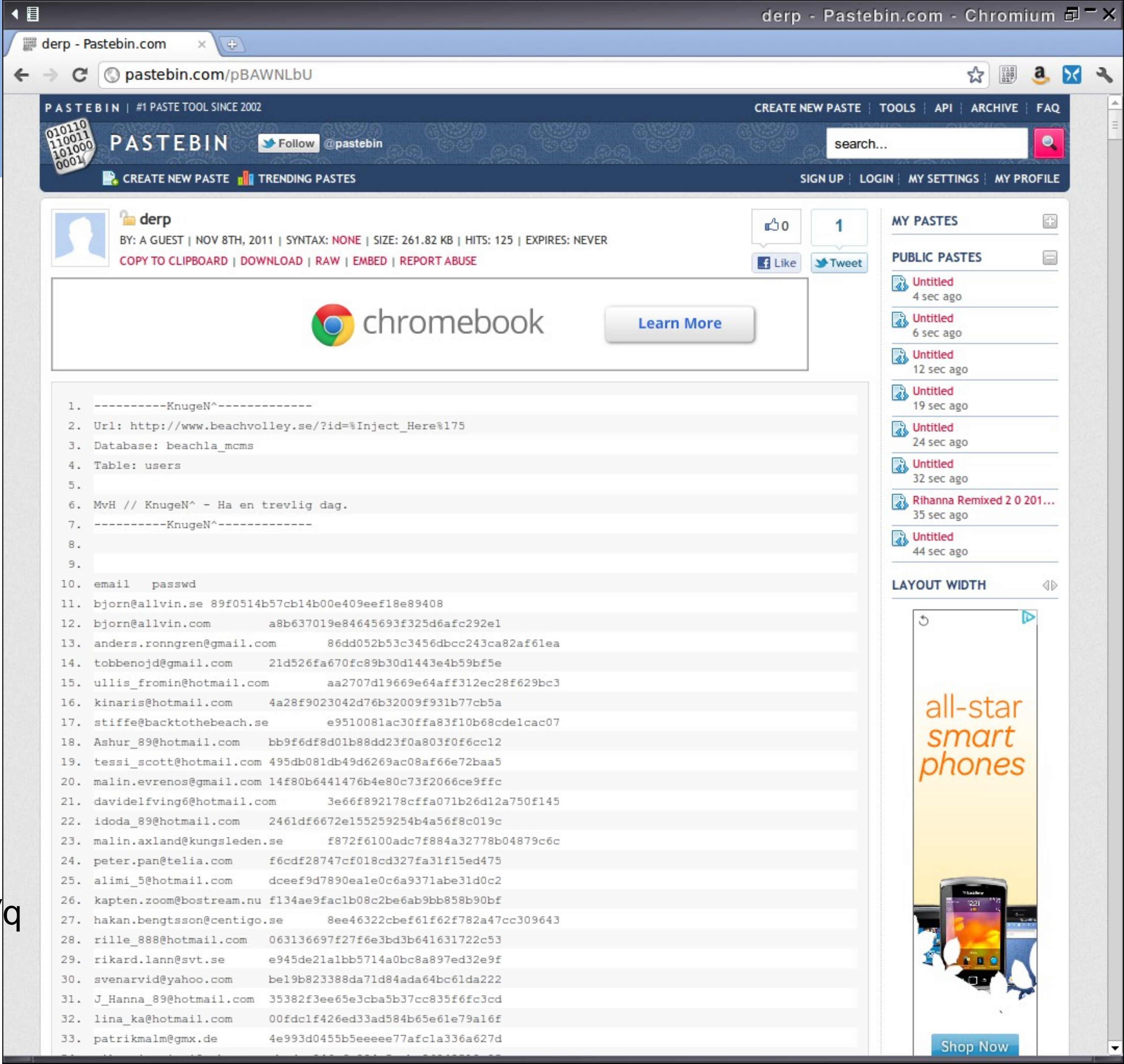
CrackMeIfYouCan KoreLogic
pastebin.com/nwyesR71 pastebin.com/SWFBiZgH pastebin.com/bLsc2yTt pastebin.com/XPkEji7u pastebin.com/iWiZ6neF
14 Sep

CrackMeIfYouCan KoreLogic
Hashes galore: pastebin.com/fKMa7sAx pastebin.com/mWFjtv4B pastebin.com/MYN7cEQS pastebin.com/c7epXnFu
14 Sep

~5396 Hashes

2311 password hashes cracked, 3085 left in 5 minutes on laptop

```
  #  Password
-----------------
72
64 beach
41 super123
11 123456
 8 beachvolley
 5 stockholm
 5 skorpan
 5 katten
 4 y17Gwk3VVq
 4 volleyboll
```



derp

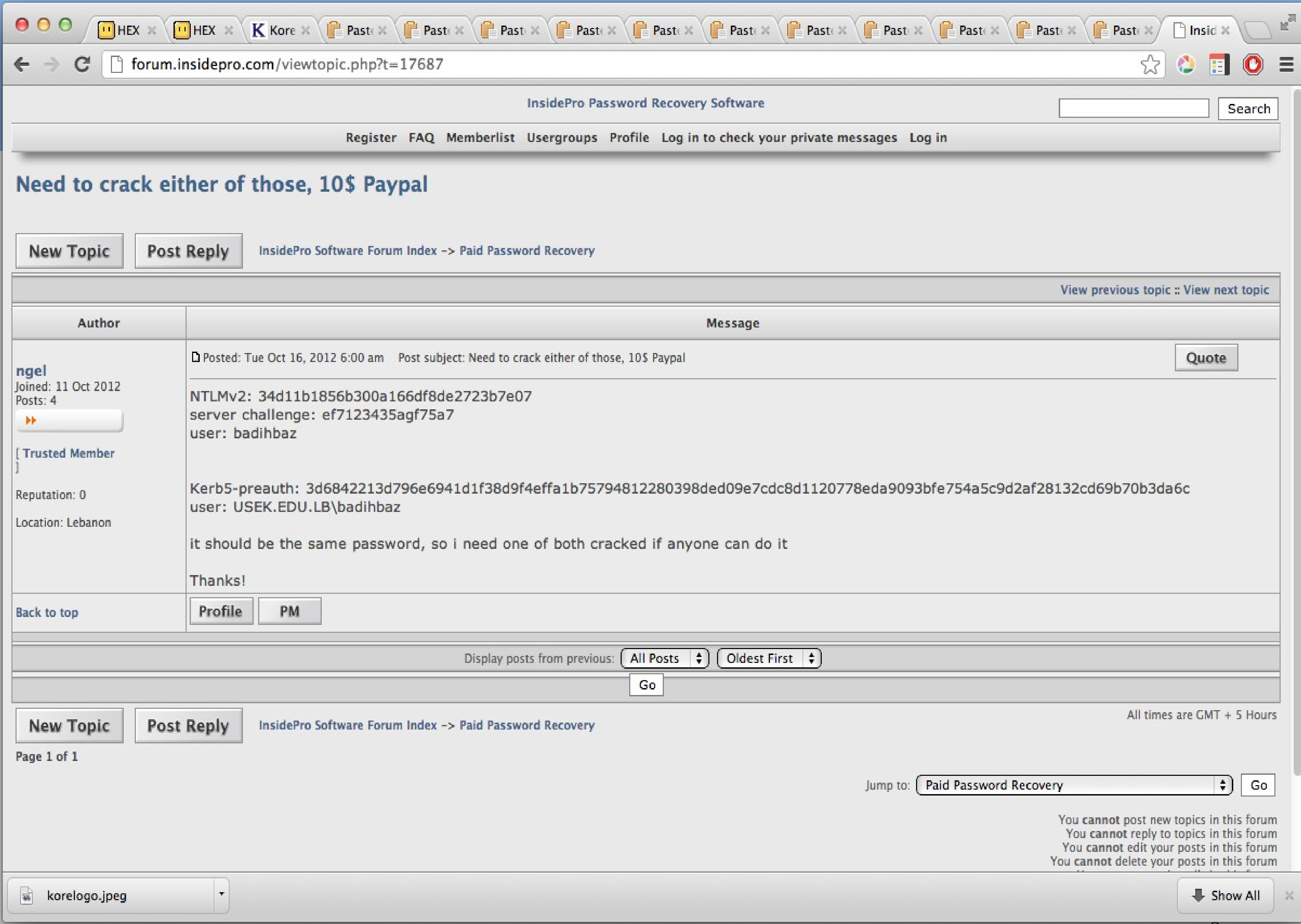
BY: A GUEST | NOV 8TH, 2011 | SYNTAX: NONE | SIZE: 261.82 KB | HITS: 125 | EXPIRES: NEVER

COPY TO CLIPBOARD | DOWNLOAD | RAW | EMBED | REPORT ABUSE

```
----------KnugeN^-------------
Url: http://www.beachvolley.se/?id=%Inject_Here%175
Database: beachla_mcms
Table: users

MvH // KnugeN^ - Ha en trevlig dag.
----------KnugeN^-------------


email   passwd
bjorn@allvin.se 89f0514b57cb14b00e409eef18e89408
bjorn@allvin.com        a8b637019e84645693f325d6afc292e1
anders.ronngren@gmail.com       86dd052b53c3456dbcc243ca82af61ea
tobbenojd@gmail.com     21d526fa670fc89b30d1443e4b59bf5e
ullis_fromin@hotmail.com        aa2707d19669e64aff312ec28f629bc3
kinaris@hotmail.com     4a28f9023042d76b32009f931b77cb5a
stiffe@backtothebeach.se        e9510081ac30ffa83f10b68cde1cac07
Ashur_89@hotmail.com    bb9f6df8d01b88dd23f0a803f0f6cc12
tessi_scott@hotmail.com 495db081db49d6269ac08af66e72baa5
malin.evrenos@gmail.com 14f80b6441476b4e80c73f2066ce9ffc
davidelfving6@hotmail.com       3e66f892178cffa071b26d12a750f145
idoda_89@hotmail.com    2461df6672e155259254b4a56f8c019c
malin.axland@kungsleden.se      f872f6100adc7f884a32778b04879c6c
peter.pan@telia.com     f6cdf28747cf018cd327fa31f15ed475
alimi_5@hotmail.com     dceef9d7890ea1e0c6a9371abe31d0c2
kapten.zoom@bostream.nu f134ae9fac1b08c2be6ab9bb858b90bf
hakan.bengtsson@centigo.se      8ee46322cbef61f62f782a47cc309643
rille_888@hotmail.com   063136697f27f6e3bd3b641631722c53
rikard.lann@svt.se      e945de21a1bb5714a0bc8a897ed32e9f
svenarvid@yahoo.com     be19b823388da71d84ada64bc61da222
J_Hanna_89@hotmail.com  35382f3ee65e3cba5b37cc835f6fc3cd
lina_ka@hotmail.com     00fdc1f426ed33ad584b65e61e79a16f
patrikmalm@gmx.de       4e993d0455b5eeeee77afc1a336a627d
```


HEX
HEX
Kore
Paste
Insid
forum.insidepro.com/viewtopic.php?t=17687

InsidePro Password Recovery Software

Search
Register FAQ Memberlist Usergroups Profile Log in to check your private messages Log in

Need to crack either of those, 10$ Paypal

New Topic
Post Reply
InsidePro Software Forum Index -> Paid Password Recovery
View previous topic :: View next topic

Author	Message
ngel Joined: 11 Oct 2012 Posts: 4 [Trusted Member] Reputation: 0 Location: Lebanon	Posted: Tue Oct 16, 2012 6:00 am Post subject: Need to crack either of those, 10$ Paypal

```
NTLMv2: 34d11b1856b300a166df8de2723b7e07
server challenge: ef7123435agf75a7
user: badihbaz


Kerb5-preauth: 3d6842213d796e6941d1f38d9f4effa1b75794812280398ded09e7cdc8d1120778eda9093bfe754a5c9d2af28132cd69b70b3da6c
user: USEK.EDU.LB\badihbaz
```

it should be the same password, so i need one of both cracked if anyone can do it

Thanks!

Quote
Back to top
Profile
PM
Display posts from previous: All Posts
Oldest First
Go
New Topic
Post Reply
InsidePro Software Forum Index -> Paid Password Recovery
All times are GMT + 5 Hours
Page 1 of 1
Jump to: Paid Password Recovery
Go

You **cannot** post new topics in this forum
You **cannot** reply to topics in this forum
You **cannot** edit your posts in this forum
You **cannot** delete your posts in this forum

Whats the source of the leaks?

But who is posting them?
Anonymous / LulzSec peeps / Other "bad" guys.

Once a site is hacked - it USED to be about replacing index.html
Now its about database dumping.
Get sensitive information - share it - embarrassing the company

This is "NEW" and popular.
This is the new dataset we are talking about it.

Password Cracking Forums (http://forum.insidepro.com/)
sharing lists and sharing cracks (Where LinkedIn was posted)

So you don't have to do any work - someone else has cracked stuff for you.

Whats the source of the leaks?

So how much data are we talking about?

Publicly: ~180 million raw-md5 hashes posted on forums/pastebin/googles/Interweb

Privately: 287,000,000+ Hashes leaked in the last year. (not including the stuff on pastebin/twitter/etc)

Where each site is 'sort | uniq' first

~195,000,000 hashes cracked in the last year.

~110,000,000~ Unique passwords cracked. (imagine that wordlist!).

Whats the size of the leaks?

Largest sites _privately_ leaked in the last year that I know of.

28.0 million md5(md5(pass).salt) email provider

17.3 million unique md5 (radio)

11.6 million unique md5 (romance)

9.3 million unique md5 (gaming)

6.4 million unique sha1 (LinkedIn)

5.4 million unique md5 (payment site - biz partner)

5.2 million unique md5 (torrent site)

3.4 million DES hashes (unknown source)

So how many users does 17.3 million unique passwords equal to?

I don't know.

Also: Notice MD5 !!!!!! People are _STILL_ using it to hash passwords.

LinkedIn : 6,458,020 unique hashes – 5,515,000 cracked (85% cracked)

What don't we find?

What don't you find ?

NTLMs (Active Directory)
{SHA} / {SSHA} (From large LDAP servers)

Or if you do - VERY few.

No active directory compromises. Pentesters aren't sharing ;)

No active directory compromises. bad guys aren't sharing ;)

Or - the "real" attackers aren't compromising internal AD/SSO server.

Patterns

So what can we learn?
Taking the 2 million most popular passwords:

```
 245017 ?d?d?d?d?d?d
 144439 ?l?l?l?l?l?l
 141014 ?l?l?l?l?l?l?l?l
 119474 ?l?l?l?l?l?l?d?d
 104935 ?l?l?l?l?l?l?l
  61575 ?l?l?l?l?l?l?l?l?l
  61459 ?d?d?d?d?d?d?d?d
  58632 ?l?l?l?l?l?d?d
  50217 ?l?l?l?l?l?l?l?d
```

Where ?d = 0123456789 ?l=abcdefghijklmnopqrstuvwxyz

Use these patterns to crack more passes.
Find words NOT in your wordlist. And add them to your lists.

What is your corporation's patterns ?u?l?l?l?l?l?l?d

Patterns

Sample patterns from a Fortune 100 Active Directory:
364061 password hashes cracked, 19630 left

20522	?u?l?l?l?l?l?d?d	Example:	Hippos11
15082	?u?l?l?l?l?l?d?d?s		Hippos11!
13644	?u?l?l?d?d?d?d?s		Hip1234!
8739	?u?l?l?l?d?d?d?d		Hipp1234
7852	?u?l?l?l?l?l?d?s		Hippos1!
7761	?u?l?l?l?l?d?d?s		Hippo11!
7657	?u?l?l?l?l?l?l?d?d		Hipposs11
7325	?u?l?l?s?d?d?d?d		Hip!1234
6929	?u?l?l?l?d?d?d?d?s		Hipp1234!
6285	?u?l?l?l?l?l?s?d?d		Hippos!12
6222	?u?l?l?l?l?l?l?l?d?d		Hippostu12
4952	?u?l?l?l?l?l?s?d		Hippos!1

All password meet “policy” of 8 chars – 1 upper case – 1 number

Whats your target?

Is your user/target in a “Commercial/business” environment?
Or an “non-business” environment ?

Workstation at a business ? → Business
Workstation at a home ? → Non-Business
Young or Old User ?
Was the attack malicious ?
Internal attacker/user ? Or External?

Why does this matter?

Because they choose different types of passwords.

- Most “rules” in tools are not based off of password patterns used in Business environments

Whats your target?

So – Are these from a Business or non-Business network ?

1700	Password1
761	Welcome01
259	Fall2011
225	Cisc0mail
175	Summer11
175	Pass123
133	Welcome02
127	client1
110	Client123
97	Summer2011
75	P@ssw0rd
71	July2011
70	Autumn11

Removed Numbers and got:
Password Welcome Summer Fall Client
Pass client August July Autumn Sept
Football Ford Harley Mike Mustang
Cowboys Batman Matthew June Dallas
P@sswrd Winter Abcd Orange Chevy
Jordan Ashley Austin Love Baseball
Steelers password Chicago Andrew Test
Qwer Hunter Michael Redsox Justin
Infosys Taylor Monday Amanda Maggie
Blue Jack Jake Charlie Yankees John
Jessica Bailey Nicole Tyler Soccer
Raiders Spring Madison Morgan Chris
Brandon Temp October Jesus James

Whats your target?

So – Are these from a Business or non-Business network ?

1099	password
760	12345678
525	baseball
523	football
458	qwerty
457	superman
402	abc123
377	696969
363	1234567
353	monkey
351	dragon
346	liverpool
330	letmein

Removed Numbers and got:
qwerty mike dragon blue monkey soccer password shadow pussy jordan love qwer mustang john money james pass hockey abcd michael ranger tiger alex batman master chevy hunter chris lucky buster andrew harley ford killer thomas robert honda green dallas june angel david lakers hustler charlie hello redsox

Your Policies Hurt You

Your password policy makes your users choose worse passwords over time.

Rotate every 30 days? Months!
Rotate every 90 days? Seasons!

Bertram58# → Bertram59# → Bertram60# → Bertram61#
Bertram58! → Bertram58@ → Bertram58# → Bertram58$

Rredman:S3cur3Pass
Rredmanadmin:S3cur3Pass1

How are you going to prevent this?

Your Policies Hurt You

Sample passwords from a small secure environment:

#	Password
13	Tig[engus
9	2@12chickenS
7	Tig[engus!
4	Tig[mengus
4	Tig[engus1
3	Tig[engus%

Strong passwords yes, but notice what users are doing behind the scenes.

Changing just a few characters.

What you can learn...

Idea:
The best source of data for password research...
Is leaked passwords.

5 years ago – there was little/no public password leaks

Now? Approx 170 million passwords/hashes leaked
In the last 12 months.

Why do this? Wordlists and Patterns.
Brute Forcing is a very “old method” - not logical.

Spammers

Spammers use the same passwords everywhere.
Proof? Google the string 0Tz9Kac193

Looks like a random password. Because it is. But name a public vBulletin site - and ONE of users will have this as their password. Your business' public site might have these.

There are at least 10,000 known shared passwords used by spammers. (Does your Internet-based site have any?)
Almost always 10 random characters.

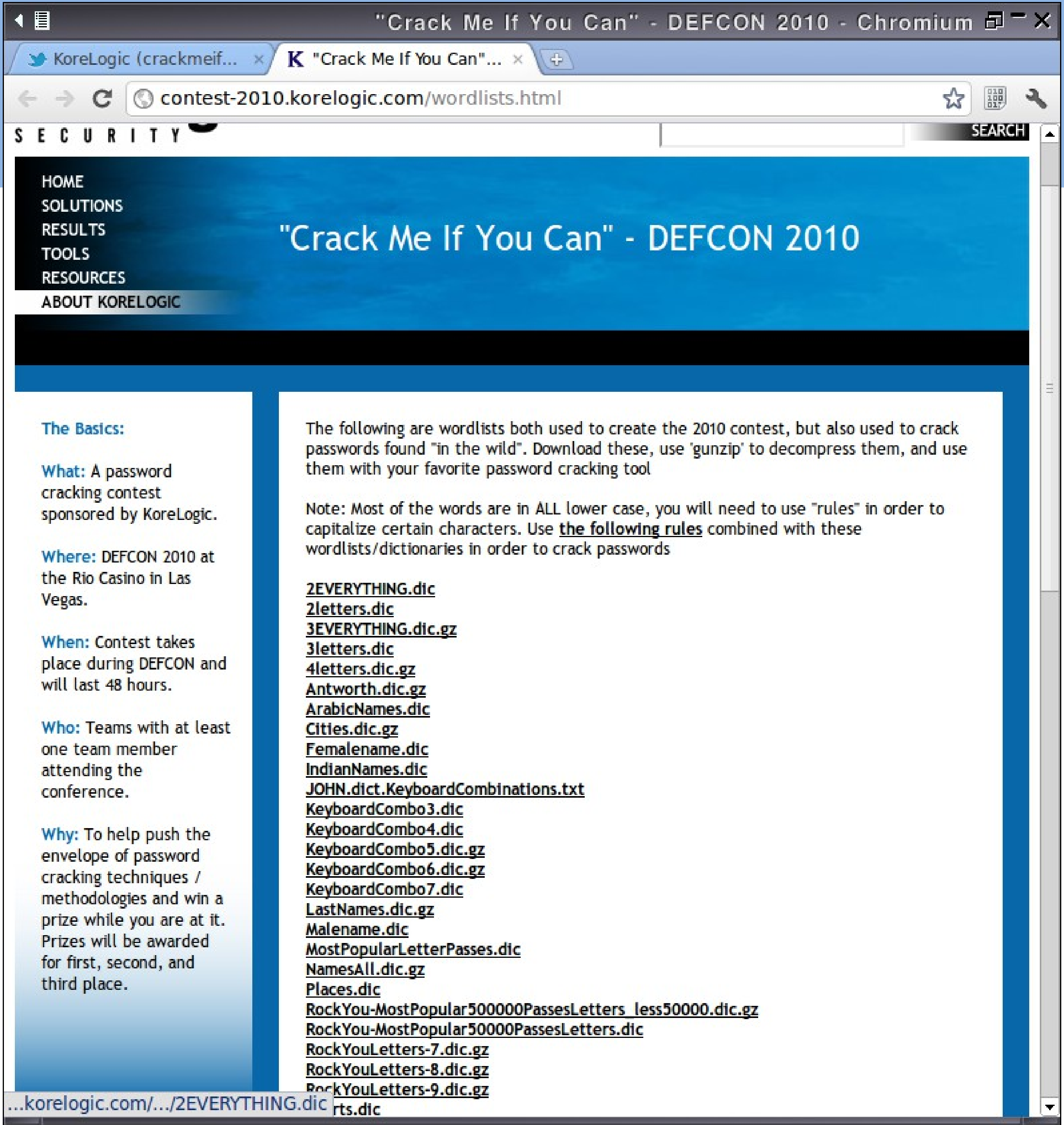
Ygvic574IO yH2pi6qq1W yiEfc353aH yirKfZF656
YIsvKWv818 YiurQLj321 yjAoRHw833 yjH1FHp679
Yjy5OzN912 YkBRYFt395 YkFOh6l613 ykoP3re761
YKWEnsp789 YlbUm8H517 YLcmxGy285 ym2JHWP338
Yme8Z6B767 ymg5iej472 ymS9awo764 yn28kE6lbR

Wordlists?

To get “Business” wordlists - use ours. (next slide)

Also, create your own targeted lists. Use the Googles!
Research the victim(s). Research the possible bad guy.

Local city / State (For all company locations)
Local sport team names (All of them)
Company's names (All of them)
Company's products (All of them)
Company's locations (All of them)
Local Colleges / Schools
Technology/Vendors used by the company
Password reset patterns (Every 3 months? Every 30 days?)


"Crack Me If You Can" - DEFCON 2010 - Chromium
KoreLogic (crackmeif...
"Crack Me If You Can"...
contest-2010.korelogic.com/wordlists.html
SECURITY
SEARCH
HOME
SOLUTIONS
RESULTS
TOOLS
RESOURCES
ABOUT KORELOGIC
...korelogic.com/.../2EVERYTHING.dic

"Crack Me If You Can" - DEFCON 2010

The Basics:

What: A password cracking contest sponsored by KoreLogic.

Where: DEFCON 2010 at the Rio Casino in Las Vegas.

When: Contest takes place during DEFCON and will last 48 hours.

Who: Teams with at least one team member attending the conference.

Why: To help push the envelope of password cracking techniques / methodologies and win a prize while you are at it. Prizes will be awarded for first, second, and third place.

The following are wordlists both used to create the 2010 contest, but also used to crack passwords found "in the wild". Download these, use 'gunzip' to decompress them, and use them with your favorite password cracking tool

Note: Most of the words are in ALL lower case, you will need to use "rules" in order to capitalize certain characters. Use the following rules combined with these wordlists/dictionaries in order to crack passwords

2EVERYTHING.dic
2letters.dic
3EVERYTHING.dic.gz
3letters.dic
4letters.dic.gz
Antworth.dic.gz
ArabicNames.dic
Cities.dic.gz
Femalename.dic
IndianNames.dic
JOHN.dict.KeyboardCombinations.txt
KeyboardCombo3.dic
KeyboardCombo4.dic
KeyboardCombo5.dic.gz
KeyboardCombo6.dic.gz
KeyboardCombo7.dic
LastNames.dic.gz
Malename.dic
MostPopularLetterPasses.dic
NamesAll.dic.gz
Places.dic
RockYou-MostPopular500000PassesLetters_less50000.dic.gz
RockYou-MostPopular50000PassesLetters.dic
RockYouLetters-7.dic.gz
RockYouLetters-8.dic.gz
RockYouLetters-9.dic.gz
rts.dic

Wordlists?

To get wordlists used on “Non-Business/Internet” sites

Find public leaks of passwords/wordlists/hashes. Best source of information:

Biggest/Best Plaintext List:

- “Rockyou.txt” - ~32 million passwords

Others: “fbnames” - LinkedIn passwords – http://blog.thireus.com/cracking-story-how-i-cracked-over-122-million-sha1-and-md5-hashed-passwords

Twitter.com and Pastebin.com

Follow:

1) The hacker groups (@lulzsec etc)
2) Me / KoreLogic (@CrackMeIfYouCan)

We released 172 million hashes that were obtained from hashes posted on Twitter/Pastebin.

Wordlists?

Examples of “Non-Business” common words/phrases:

What is “Naruto” ? Why is in the top 100 most common passwords on web-forums?

Why is “dragon” in the top 30 of most large password leaks?

What is 'slipknot' ? What is 'blink182' ? What is 'enimem' ?

Omg? Brb? Hahaha? Lol ? LolLol? Lulz ?

Do you trust your self to identify (and collect) the right kinds of wordlists for your victim? For your “target”.

Most Common Passwords..
(Internet based...)

123456 password 123456789 12345678 111111 123123 qwerty 12345 1234567 abc123 666666 123321 000000 654321 1q2w3e4r 7777777 121212 master 123qwe 1234 internet 112233 dragon 159753 123abc matrix 88888888 1qaz2wsx superman shadow iloveyou daniel asdfgh 1234567890 killer eminem samsung 123 q1w2e3r4 777777 qwe123 computer abcd1234 999999 qazwsx hahaha cocacola aaaaaa 11111111 zxcvbnm trustno1 letmein asdasd 987654321 1q2w3e 159357 12341234 michael google asdfasdf asd123 888888 222222 sunshine pokemon football diablo compaq 123654 william starwars monkey logitech lalala 555555 333333 232323 131313 123456a welcome qwerty123 qweasd princess batman asdfghjkl adidas 789456 147258 12344321 testtest george andrew 987654 snoopy slipknot silver robert qwertyuiop q1w2e3 london kawasaki joshua ginger diamond creative banana 1234qwer secret scarface pepper password1 nirvana jordan hello123 freedom chicken asdf1234 123123123 102030 101010 qqqqqq passw0rd oliver matthew lol123 justin jackass darkness cheese buster blink182 87654321 852456 whatever qwerty1 qazxsw patrick monster jessica hunter hardcore chelsea casper andrea alexander a123456 147852 111222 1 00000000 windows thomas slayer scooter sandra qwer1234 mustang martin lollol forever cookie blahblah 0123456 soccer sniper platinum phoenix pass123 juventus hacker charlie arsenal 1111111 11111 1111 007007 yamaha steven rainbow junior joseph jordan23 jennifer jackson ferrari chester benjamin 789456123 753951 212121 1q2w3e4r5t

Rules / Logic

You need more than good wordlists. You need logic:

Do you trust your tool to create rules?
password1 password2 password3 (but not password 9)
Why not?

Options:
- Use ours (free)
- Read 'john-users' and other mailing lists
- Follow 'hashcat' forums on hashcat.net
- Buy a $2,000 tool – and HOPE it does a good job

See my 1-hour talk about password rule-writing in business environments.

Rules / Logic

Example of fallacies:

```
# Some [birth] years...
l Az"19[7-96-0]" <+ >-
l Az"20[01]" <+ >-
l Az"19[7-9][0-9]" <+
l Az"20[01][0-9]" <+
l Az"19[6-0][9-0]" <+
```

This doesn't - Capitalize the word

But we know that 90% of “business” passwords have to have a capital letter. It is not logical to use this rule.

GPUs

GPUs are absolutely the best technology for password cracking.

In the last year – more and more formats are being supported. (DES GPU cracking didn't exist in 2010).

Also: .zip .doc .xls .rar formats
NTLM (Windows)
DES (Older Unix)
FreeBSD MD5 (1)

ATI : Faster / Better (especially for single-hash)
ATI : Pain in the *** to get to work. Drivers are NOT great.
Nvidia / GTX : Works out of box. More Power. “Slower”

GPUs

“All” password cracking “teams” use GPUs.

2nd place at our DEFCON contest team – 14 people – 46 GPU cards. (84 CPU cores).

ATI 7970 ~ 500 dollars - is currently the “best”. Anyone can buy one. (not the best speed for the $$$ though).

GPUs work via:
1) Brute force - ?u?l?l?l ?d?d?d?d Love2011 Hate2010
2) Wordlists (with append / prepend rules)
3) Combination Attackers (combine first/last name lists)

GPUs

1) Brute force - ?u?l?l?l ?d?d?d?d Love2011 Hate2010

What order are you going to do them in ?
What combinations are the most common for your environment? If you don't look at examples in advance, how are you going to know this?

2) Wordlists (with Append / Prepend rules)

What wordlists you going to use? (we know this now)
What characters are we going to have appended? prepended?

Should you bother with capital letters? (Ask yourself this – is your target and/or bad guy likely to use capital letters?)

GPUs

You do not need commercial($$$) tools for CPU or GPU cracking.

They are not better. They are not faster.

The “fastest” GPU cracking software (OCLHashcat-plus) is free.

GPUs

Cloud? Should you use it?

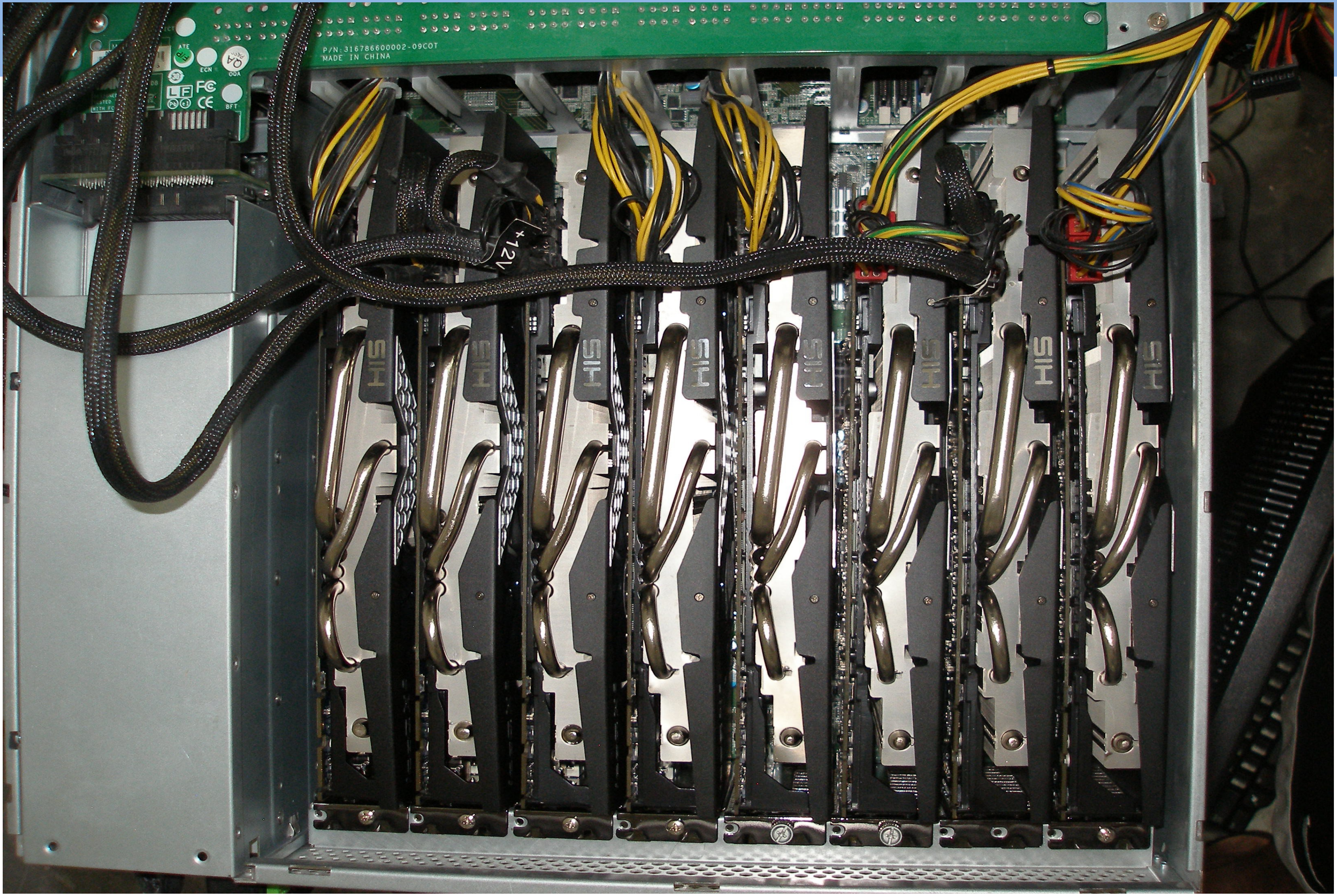
I have not – and will not - trust the “cloud” to help me crack passwords. I don't trust others.

Also – the GPU cards used by large datacenters (such as Amazon EC2) are <u>not</u> the best cards for GPU cracking. They are good for other scientific things – but NOT hash cracking.

A $300 ATI card in a regular PC case is a good rig.

If you plan on password cracking on GPUs more than once, buy your own system. Its more cost effective.

Machine built for fun..



Thats 8 GPU cards in one computer.
Source: http://ob-security.info/

Mimic the “bad guys”

- Build your GPU rig in advance
- Learn the tools
- Prepare wordlists in advance
- Prepare rules in advance
- Research common themes in advance on what types of passwords users are choosing (note: China example)
- Plan your strategy for distributing the work in advance. (Machines on standby – Amazon EC2 account already setup)
- Practice – Practice – Practice

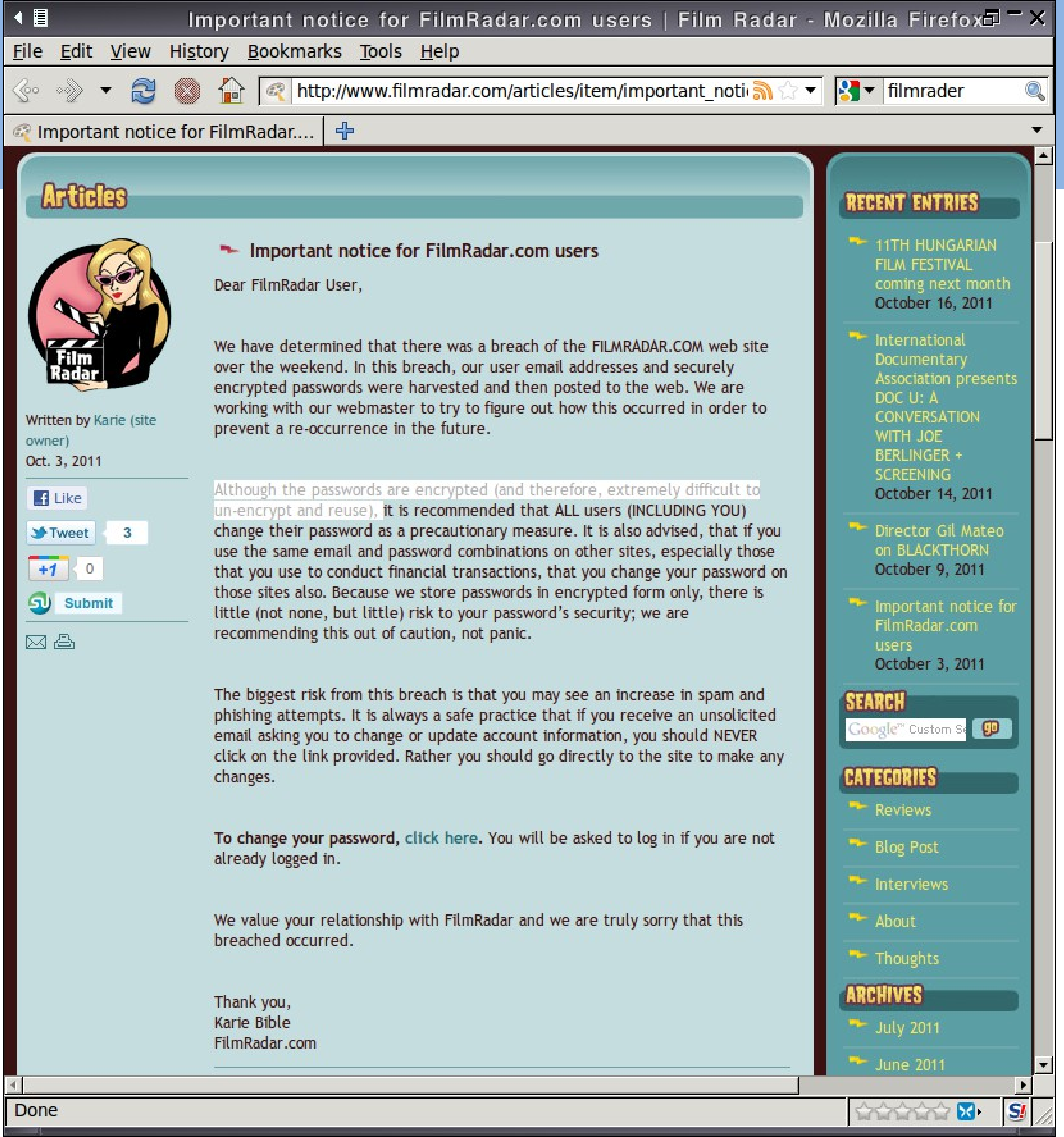
Notice the language used:

“extremely difficult” (See next slide)

“un-encrypt” - Its not encrypted. Its hashed. they don't understand the problem.

“biggest risk” - they Think the risk is spam.

Bad guys logged into paypal.com using the logins and passes from this site and stole money.


Important notice for FilmRadar.com users | Film Radar - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.filmradar.com/articles/item/important_noti
filmrader
Important notice for FilmRadar....
Articles
Film Radar
Like
Tweet 3
+1 0
Submit
RECENT ENTRIES
SEARCH
Google™ Custom Se
go
CATEGORIES
ARCHIVES
Done

Written by Karie (site owner)
Oct. 3, 2011

Important notice for FilmRadar.com users

Dear FilmRadar User,

We have determined that there was a breach of the FILMRADAR.COM web site over the weekend. In this breach, our user email addresses and securely encrypted passwords were harvested and then posted to the web. We are working with our webmaster to try to figure out how this occurred in order to prevent a re-occurrence in the future.

Although the passwords are encrypted (and therefore, extremely difficult to un-encrypt and reuse), it is recommended that ALL users (INCLUDING YOU) change their password as a precautionary measure. It is also advised, that if you use the same email and password combinations on other sites, especially those that you use to conduct financial transactions, that you change your password on those sites also. Because we store passwords in encrypted form only, there is little (not none, but little) risk to your password's security; we are recommending this out of caution, not panic.

The biggest risk from this breach is that you may see an increase in spam and phishing attempts. It is always a safe practice that if you receive an unsolicited email asking you to change or update account information, you should NEVER click on the link provided. Rather you should go directly to the site to make any changes.

To change your password, click here. You will be asked to log in if you are not already logged in.

We value your relationship with FilmRadar and we are truly sorry that this breached occurred.

Thank you,
Karie Bible
FilmRadar.com

11TH HUNGARIAN FILM FESTIVAL coming next month
October 16, 2011

International Documentary Association presents DOC U: A CONVERSATION WITH JOE BERLINGER + SCREENING
October 14, 2011

Director Gil Mateo on BLACKTHORN
October 9, 2011

Important notice for FilmRadar.com users
October 3, 2011

Reviews

Blog Post

Interviews

About

Thoughts

July 2011

June 2011

Tools:

Cpu Based:

- John the Ripper
- HashCat

GPU Based:

- OclHashcat
- OclHashcat-plus
- OclHashcat-lite

Others:

- Passware
- PassScape
- L0phtCrack
- PasswordsPro etc

I FIND YOUR LACK OF PASSWORD STRENGTH DISTURBING
quickmeme.com

Thanks:

Rick Redman
rredman@korelogic.com

@CrackMeIfYouCan on twitter

KoreLogic
SECURITY