



Dumpster diving du 21ème
siècle

The garbage is leaking juice

HACKFEST COMMUNICATION

<https://www.hackfest.ca>

Shameless Plugs

Hackfest Formations:

- Sécurité 101/102 (575\$)
- Analyse de Malware (1250\$)
- CST Introduction au développement de systèmes d'exploitation (Gratuit)
- Corelan ADVANCED (2500\$)
- Corelan Foundations (1499\$)

Shameless Plugs

Hackfest Inscription Conférence + CTF (220+ personnes, meilleur endroit pour apprendre) :

- <https://www.hackfest.ca/fr/inscription/>
- 85\$ (1 à 4 personnes)
- 75\$ (5 à 10 personnes)
- Moins cher si vous êtes plus!




Hackfest XMPP (chat)

<https://xmpp.hackfest.ca/>


Hackfest XMPP (chat)

#hackfest (👤) - General Room

 **Pier-Luc** @plmaltais

ouliin on cherche de quoi du plus "client friendly" :/

Today at 9:16 AM


 **gp** @gp

certaines scanners peuvent importer les scans nmap

Today at 9:17 AM


i ylmk

I think

 **Pier-Luc** @plmaltais


yeah doit avoir une façon de la faire dans nexpose, j'leur ai écrit

Today at 9:17 AM

 **Dave** @stackfault


Hey morning!

Today at 9:19 AM

 **gp** @gp


hello

Today at 9:20 AM

 **Mart** @mdube


morning

Today at 9:31 AM

 **Mart** @mdube

it's a reporting week !


Today at 9:40 AM


 **gp** @gp


clair


Today at 9:40 AM


Who's Here (13)


 **maboum**
@maboum


 **chaput**
@chaput


 **Dimitri**
@dimitri


 **Pier-Luc**
@plmaltais


 **jsgrenon**
@jsgrenon

 **Francois G**
@francois


 **Mart**
@mdube

 **madmantm**
@madmantm

 **beubleliss**
@beubleliss

 **braindeaddev**
@braindeaddev

Files

 **1474156537570.jpg**
madmantm · 16kb

\$./prez.sh --help

- Intro
- Analyses
 - ↗ Quelques chiffres + Demo
- Utilisations
 - ↗ Cassage de hash + Demo
 - ↗ Réutilisation de mots de passe
- Responsabilités
 - ↗ Sysadmin / Dev
 - ↗ Utilisateurs
 - ↗ Hackers

\$ w | grep mdube

- Père de famille
- Analyste en sécurité chez GoSecure
 - ↗ Penetration Testing
- Co-administrateur du HF de 2011 à 2015
 - ↗ Organiser War Games / CTFs
- Ninja en devenir!
- Drink Scotch/Bourbon
- Intérêt: Système sécurisé par défaut

\$ w | grep (vn|Vincent)

- A oeuvré autant dans le secteur public que privé
 - ↗ *sysadmin* et *data recovery*
- Ardent promoteur au droit du choix libre d'OS,
 - ↗ Peut facilement avoir l'air d'un Windows lover mais déteste eventvwr autant que le GUI sur Linux.
- Temps libres
 - ↗ Super connecteur de communautés
 - ↗ Geolocation stuff
 - ↗ Lectures de culture générale ou géopolitique
- Foodie & boozie (old fashioned ftw)
- @sys6x sur Twitter

ONE DOES NOT SIMPLY

START A PROJECT WITHOUT CONSIDERING ETHICS



DID
YOU
HEAR
?

Sep 22, 2016

An Important Message to Yahoo Users on Security



[« Previous Release](#)

SUNNYVALE, Calif.--(BUSINESS WIRE)-- A recent investigation by Yahoo! Inc. (NASDAQ:YHOO) has confirmed that a copy of certain user account information was stolen from the company's network in late 2014 by what it believes is a state-sponsored actor. The account information may have included names, email addresses, telephone numbers, dates of birth, hashed passwords (the vast majority with bcrypt) and, in some cases, encrypted or unencrypted security questions and answers. The ongoing investigation suggests that stolen information did not include unprotected passwords, payment card data, or bank account information; payment card data and bank account information are not stored in the system that the investigation has found to be affected. Based on the ongoing investigation, Yahoo believes that information associated with approximately 500 million user accounts was stolen and the investigation has found no evidence that the state-sponsored actor is currently in Yahoo's network. Yahoo is working closely with law enforcement on this matter.

Yahoo is notifying potentially affected users and has taken steps to secure their accounts. These steps include invalidating unencrypted security questions and answers so that they cannot be used to access an account and asking potentially affected users to change their passwords. Yahoo is also recommending that users who haven't changed their passwords since 2014 do so.

Yahoo encourages users to review their online accounts for suspicious activity and to change their password and security questions and answers for any other accounts on which they use the same or similar information used for their Yahoo account. The company further recommends that users avoid clicking on links or downloading attachments from suspicious emails and that they be cautious of unsolicited communications that ask for personal information. Additionally, Yahoo asks users to consider using [Yahoo Account Key](#), a simple authentication tool that eliminates the need to use a password altogether.

Yahoo! Inc. (YHOO) - NASDAQ
\$43.95 ↓ 0.19 (0.43%)

3:54PM EDT - Nasdaq Real Time

Day High

Day Low

52-Week High

52-Week Low

[More Stock Information](#)

Shareholder Tools

[Briefcase](#)

[Contact](#)

[Downloads](#)

[FAQ](#)

[Email Alerts](#)

[Request Info](#)

[RSS Feeds](#)

Follow Yahoo



Uh oh, aujourd'hui chez Yahoo...

- ➔ *Based on the ongoing investigation, Yahoo believes that information associated with at least **500 million user accounts** was stolen and the investigation has found no evidence that the state-sponsored actor is currently in Yahoo's network.*
 - Yahoo is notifying **potentially affected users** and has taken steps to secure their accounts. These steps include invalidating unencrypted security questions and answers so that they cannot be used to access an account and asking potentially affected users to change their passwords. Yahoo is also **recommending that users who haven't changed their passwords since 2014** do so.
 - The account information may have included names, email addresses, telephone numbers, dates of birth, hashed passwords (the vast majority with bcrypt) and, in some cases, encrypted or unencrypted

Participation du public!

- Public: 0 email reçu
- Friends: 3 email reçu
- Équipe du HF: Après 3 appels à la participation, 7/18

- Constat:



Data Breach > Data Leak > Password Leak

→ Data Breach

- ↗ ISO/IEC 27040: compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data transmitted, stored or otherwise processed.

→ Data Leak

- ↗ Fuite de: Données clients, fiscales. Secrets d'entreprise.

→ Password Leak

- ↗ Fuite d'identité de clients. Généralement une association usager-mot_de_passe.

Autres sortes de *leaks*

- Codes propriétaires (HL2, W2k...)
- Secrets d'entreprise/gouvernementaux (Snowden)
- Photos
- Exploit kits (Equation group parmi d'autres)
- Infos bancaires
- Informations d'identité (doxxing)
- Accès à des ressources non-autorisées
- etc.



Analyses

WTF is in there?

\$ ls -l *.txt


source	hash	ct
MySpace	SHA1 unsalted	359 339 047
Adobe 155M	3des (key not found yet)	147 913 099
VK	cleartext	92 286 282
Linkedin	SHA1 unsalted	73 791 996
Mate 1	cleartext	27 403 818
000webhost	cleartext	15 268 730
Twitter	cleartext	12 723 215
Ashley Madison	bcrypt salted (\$2a\$12\$)	588 528


\$ man leaks

- ➔ <https://haveibeenpwned.com>
 - ↗ Site éthique. Permet de chercher si votre courriel est affecté.
 - ↗ ~1.4 milliard d'entrées
- ➔ <https://leakedsource.com>
 - ↗ Analyses de plusieurs leaks
 - ↗ Permet d'afficher les données brutes (ex. Les mots de passes)
 - ↗ ~2.2 milliard d'entrées
- ➔ <https://leakforums.net>
 - ↗ Communauté de partage et discussions
- ➔ <http://weknowyouremail.com> <https://www.thecthulhu.com>
<http://dumps.bhafsec.com/infosec/dumps/> and others
 - ↗ Rendent disponible le téléchargement de leaks

Oh no — pwned!

Pwned on 2 [breached sites](#) and found no [pastes](#) ([subscribe](#) to search sensitive breaches)

 [Notify me when I get pwned](#)

 [Donate](#)



Breaches you were pwned in

A "breach" is an incident where a site's data has been illegally accessed by hackers and then released publicly. Review the types of data that were compromised (email addresses, passwords, credit cards etc.) and take appropriate action, such as changing passwords.



Dropbox: In mid-2012, Dropbox suffered a data breach which exposed the stored credentials of tens of millions of their customers. In August 2016, they forced password resets for customers they believed may be at risk. A large volume of data totalling over 68 million records was subsequently traded online and included email addresses and salted hashes of passwords (half of them SHA1, half of them bcrypt).

Compromised data: Email addresses, Passwords



LinkedIn: In May 2016, LinkedIn had 164 million email addresses and passwords exposed. Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.

Compromised data: Email addresses, Passwords

\$ grep \$pwned | wc -l leaks.txt

Domain	Occurrence	Unique	Duplicate
bell.net	34 509	32 166	2 343
cgi.com	3 461	3 351	110
ulaval.ca	2 082	2 009	73
hydro.qc.ca	1 109	1 098	11
csst.qc.ca	116	111	5
cspq.gouv.qc.ca	112	111	1

\$ less vk.txt

- Count: 100M
- Hash Format: Cleartext
- Breach Date: 2012, Disclosure Date: 2016-06
- Scope: Russian Facebook
- Incident Handling: Bad
 - ↗ They denied that the site had been breached.
- Biggest cleartext password leak released.
- Make sure all your tools support UTF-8 if you want to play with it.

\$ less mate1.txt

- Count: 28M
- Hash Format: Cleartext
- Breach+Disclosure Date: 2016-02 (February)
- Scope: Dating Site
- Incident Handling: Bad
 - ↗ They did not acknowledge the incident.
- Bonus
 - ↗ First and Last Name
 - ↗ Date of birth
- Lulz
 - ↗ The “Forgot password” feature was sending the pass in cleartext

\$ less 000webhost.txt

- Count: 15M
- Hash Format: Cleartext
- Breach+Disclosure Date: 2015-03 (March)
- Scope: Hosting Company
- Incident Handling: Excellent
 - ↗ Apologized.
 - ↗ Investigated and fixed the issue the same day.
 - ↗ Promoted user awareness.
 - ↗ <https://www.000webhost.com/000webhost-database-hacked-data-leaked>

\$ grep -f friends.txt 000webhost.txt

➔ Boom

source	email	username	pwd
000webhost	pl.maltais@hotmail.com	Pier-Luc	family13
000webhost	marcandremeloche@gmail.com	Richard Smith	1&h2isi92H!@H

\$ less twitter.txt

- Count: 12M (~33M including duplicates)
- Hash Format: Cleartext
- Breach+Disclosure Date: 2016-06 (June)
- Scope: Social Network
- Vulnerability exploited: None
 - ↗ They were not breached. A botnet sniffed the data on user's computers and pushed it on the CnC.
- Incident Handling: Good
 - ↗ They acknowledge that the data was valid.
 - ↗ However, they asked people to "scrutinize the merits of any credential claim."
- Bonus
 - ↗ Password history / Login attempt?

\$ less myspace.txt

- Count: 360M
- Hash Format: **Unsalted SHA1 (first 10 char, lowercase)**
- Breach Date: 2008, Disclosure Date: 2016-05
- Scope: Social Media for everyone
- Incident Handling: OK
 - ↗ They have invalidated the affected accounts.
 - ↗ No apologies and kindly “race to the bottom”.
 - ↗ We run automated tools... We’re starting criminal pursue.
 - ↗ <https://myspace.com/pages/blog>

\$ less linkedin.txt

- Count: 164M (Initially ~64M in 2012)
- Hash Format: **Unsalted SHA1**
- Breach Date: 2012, Disclosure Date: 2016-05
- Scope: All businesses.
- Incident Handling: **Bad**
 - ↗ **Took 5 days** to force a password reset
 - ↗ “We have demanded that parties cease making stolen password data available and will evaluate potential legal action if they fail to comply.”
(o rly?)
 - ↗ <https://blog.linkedin.com/2016/05/18/protecting-our-members>

\$ grep -f friends.txt linkedin.txt

source	email	enc_pwd
Linkedin	vive_ced_chaput@hotmail.com	55fc154660399368c77c31767f1dfe445dfdc2e3

[bingo1 MD5: 42d0c177db16473d1f85f7e84df8bdba decrypted ...](#)
[md5decoder.org/42d0c177db16473d1f85f7e84df8bdba](#) ▼
Decrypted MD5: 42d0c177db16473d1f85f7e84df8bdba is bingo1, other hashes: SHA1:
55fc154660399368c77c31767f1dfe445dfdc2e3, SHA2, RIPEMD, CRC, ...

[moneygem User Information - Pastebin.com](#)
[pastebin.com/SCRrvJZT](#) ▼
Apr 29, 2013 - **55fc154660399368c77c31767f1dfe445dfdc2e3** xtraciex.
1168d3aa465ea240caaf6fe2c277d6ff17fa031c grants20.

[null:9b2c982ecf06df73c1d7998ebc476fa48086e649 null ...](#)
[basedforums.com/databases/MyspaceTwitterVKTumblrLinkedin/Linkedin/6_1.txt](#)
... 2badf45cb0c7d292f28486145e25294569568b13
null:xxx null:ac3fa908e39820ca84d9aea9d670c41ccf94e277 null:xxx null:
55fc154660399368c77c31767f1dfe445dfdc2e3 ...

[5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8 ...](#)
[www.item.ntnu.no/fag/ttm4175/downloads/sha1.txt](#)
... 2badf45cb0c7d292f28486145e25294569568b13
55fc154660399368c77c31767f1dfe445dfdc2e3
8fb9684ec3e832606c45ae79430aed359681792d ...

\$ less adobe.txt

- Count: 155M
- Hash Format: Encrypted (Key not disclosed, yet.)
- Breach+Disclosure Date: 2013-10 (October)
- Scope: Product users, Clients
- Incident Handling: ?

- Bonus
 - ↗ Password Hints!

HACKERS RECENTLY LEAKED 153 MILLION ADOBE USER EMAILS, ENCRYPTED PASSWORDS, AND PASSWORD HINTS.

ADOBE ENCRYPTED THE PASSWORDS IMPROPERLY, MISUSING BLOCK-MODE 3DES. THE RESULT IS SOMETHING WONDERFUL:

USER	PASSWORD	HINT
4e18acc1ab27a2d6		WEATHER VANE SWORD
4e18acc1ab27a2d6		
4e18acc1ab27a2d6	a0a2876eb1ea1fca	NAME 1
8bab66279e06cb6d		DUH
8bab66279e06cb6d	a0a2876eb1ea1fca	
8bab66279e06cb6d	85e9da81a8a78adc	57
4e18acc1ab27a2d6		FAVORITE OF 12 APOSTLES
1ab29ae86dab6e5ca	7a2d6a0a2876eb1e	WITH YOUR OWN HAND YOU HAVE DONE ALL THIS
a1f9b2b6299e7a2b	ea0ec1e6ab797397	SEXY EARLOBES
a1f9b2b6299e7a2b	617ab0277727ad85	BEST TOS EPISODE
39738b7adb068af7	617ab0277727ad85	SUGARLAND
1ab29ae86dab6e5ca		NAME + JERSEY #
877ab7889d3862b1		ALPHA
877ab7889d3862b1		
877ab7889d3862b1		
877ab7889d3862b1		
877ab7889d3862b1		OBVIOUS
877ab7889d3862b1		MICHAEL JACKSON
38a7c9279codeb44	9dca1d79d4dec6d5	
38a7c9279codeb44	9dca1d79d4dec6d5	HE DID THE MASH, HE DID THE
38a7c9279codeb44		PURLOINED
a8ae5745a7b7af7a	9dca1d79d4dec6d5	EARL LATER-3 POKEMON

THE GREATEST CROSSWORD PUZZLE
IN THE HISTORY OF THE WORLD

\$ less ashley_madison.txt

- Count: 30M
 - Hash Format: Salted bcrypt (2^12 iter)
 - Breach+Disclosure Date: 2015-07 (july)
 - Scope: Dating site encouraging affairs
 - Incident Handling:
-
- Bonus
 - ↗ Looking for an affair?

\$ less dropbox.txt

- Count: 69M
- Hash Format: Salted bcrypt (2^8 iter) or Salted SHA1
- Breach Date: mid-2012, Disclosure Date: 2016-08
- Scope: File sharing on the cloud
- Incident Handling: Bad
 - ↗ Did not acknowledge the breach
 - ↗ Took 2 weeks to write a blog post
 - ↗ However, Dropbox has prompted users who may have been affected by the hack to reset their passwords.
 - ↗ But the prompt was selective
 - ↗ <https://www.dropbox.com/help/9257>

Demo

Boom, headshot.

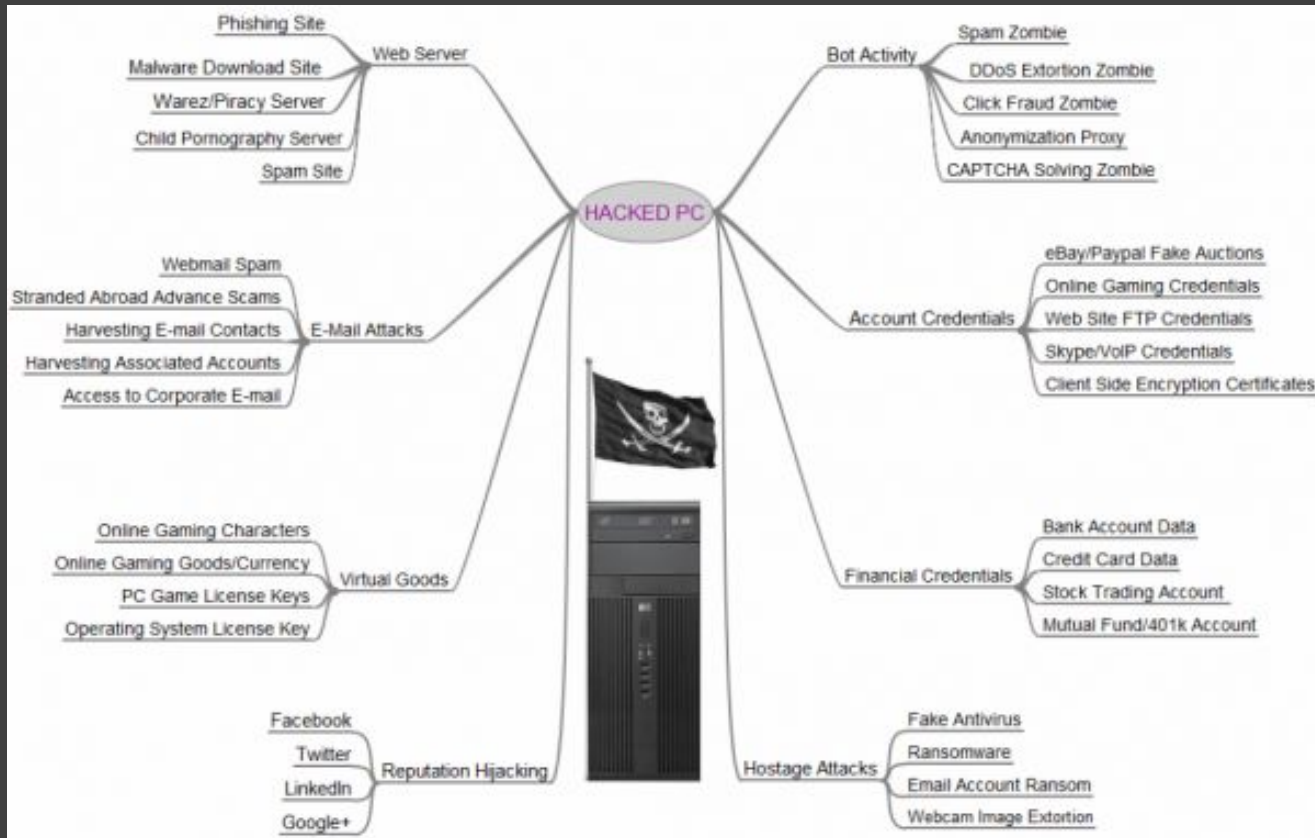
Utilisations

Que faire avec ces données?

Activités du *black market* liées à des *leaks* ou hacks

- DDoS
- CC batches
- Botnets
- Trolling
- Malware variés (cryptomining, RATs, ransomware, ...)
- Hits
- Drogues
- Phishing/spam
- Services de *rating* (falsifier des votes/reviews/réputations)
- Shipping/*muling*/livraison
- Fausses identités
- Briser des captchas

Contexte



On fait quoi avec un leak?

- Tester et améliorer des *wordlists*
 - Un hash pas cracké pour un même username dans une *leak* peut l'être à cause d'une autre liste - habitudes, séquences,
- Moar *leaks/hacks/data mining*!
 - Exploiter l'utilisation de mêmes *passwords* pour des utilisations différentes ex: exploiter un compte admin CMS pour déployer Pharma
- Transposer les comptes perso aux comptes professionnels
- *Ransomware* ciblé
- Big data/*social engineering*
- Spam
- PROFIT (for real...)

Utilisations?

- [Cleartext] Connexion sur des sites
 - ↗ Manuellement
 - ↗ Massivement
- [Cleartext] Bâtir un/des dictionnaires
- [Hash] Cracker
 - ↗ Easy mode
 - ↗ Hard mode
 - ↗ Unknown mode

Réutilisation de *passwords/credentials*

- Trop souvent, les *credentials* aux sites suivants sont trop similaires
 - ↗ Facebook
 - ↗ Twitter
 - ↗ LinkedIn
 - ↗ Google/OAuth
 - ↗ OWA du travail
 - ↗ YouTube
 - ↗ PornHub?
- En ayant un *username* ou un e-mail, il est facile de retrouver les comptes des autres sites
- Et si on recherchait “password” ou “mot de passe” dans la boîte de courrier?

Réutilisation de *passwords/credentials*

- ➔ <https://github.com/philwantsfish/shard>
 - ↗ A command line tool to detect shared passwords
 - ↗ Facebook, LinkedIn, Reddit, Twitter, Instagram, GitHub, BitBucket, Kijiji, DigitalOcean, Vimeo, Laposte, DailyMotion

```
{16-09-20 16:31}sarouman:~/Downloads mdube% proxychains java -jar shard-1.5.jar -u vive_ced_chaput@hotmail.com -p bingo1
```

```
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/libproxychains4.so
[proxychains] DLL init: proxychains-ng 4.11
16:31:48.871 [+] Selected single-user single-password mode
16:31:48.873 [+] Running 12 modules
[proxychains] Strict chain ... 127.0.0.1:9050 ... www.facebook.com:443
[proxychains] Strict chain ... 127.0.0.1:9050 ... www.linkedin.com:443
[proxychains] Strict chain ... 127.0.0.1:9050 ... www.linkedin.com:443
[proxychains] Strict chain ... 127.0.0.1:9050 ... www.reddit.com:80
[proxychains] Strict chain ... 127.0.0.1:9050 ... www.reddit.com:443
[proxychains] Strict chain ... 127.0.0.1:9050 ... www.reddit.com:80
[proxychains] Strict chain ... 127.0.0.1:9050 ... twitter.com:443 ..
[proxychains] Strict chain ... 127.0.0.1:9050 ... www.instagram.com:443
[proxychains] Strict chain ... 127.0.0.1:9050 ... github.com:443 ...
[proxychains] Strict chain ... 127.0.0.1:9050 ... github.com:443 ...
[proxychains] Strict chain ... 127.0.0.1:9050 ... bitbucket.org:443
[proxychains] Strict chain ... 127.0.0.1:9050 ... www.kijiji.ca:443
[proxychains] Strict chain ... 127.0.0.1:9050 ... cloud.digitalocean.
[proxychains] Strict chain ... 127.0.0.1:9050 ... cloud.digitalocean.
[proxychains] Strict chain ... 127.0.0.1:9050 ... vimeo.com:443 ...
[proxychains] Strict chain ... 127.0.0.1:9050 ... vimeo.com:443 ...
[proxychains] Strict chain ... 127.0.0.1:9050 ... www.laposte.net:443
[proxychains] Strict chain ... 127.0.0.1:9050 ... compte.laposte.net:
[proxychains] Strict chain ... 127.0.0.1:9050 ... www.dailymotion.com
16:34:25.199 [+] vive_ced_chaput@hotmail.com:bingo1 - Kijiji
```



HEY CAN I USE YOUR
EMAIL/PASS FOR
THE PRESENTATION?



YES. I CHANGED
ALL MY PASSWORDS.



Imgflip.com

Cleartext ou hashed, ça change quoi?

- En crackant un *leak*, une des premières choses à faire est d'y passer des *wordlists* connues...
 - Faire de la substitution (i.e.: a=4 e=3 A=@, j=y, p=r etc.)
 - Faire de la permutation (passw0rd, assw0rdp, ssw0rdpa, etc.)
 - Attaques hybride, incrémentales, bruteforce, règles de Markov, etc.
- On cracke, car c'est *hashed*, et on obtient un excellent %, mais on peut toujours s'améliorer...
- Des *leaks cleartext* nous donnent carrément un échantillon des parties non-crackées
- Ils sont donc excellents pour améliorer les *wordlists*

On fait quoi avec un *hash*? - LMGTFY

```
dakara@:/home/sys6x/.ssh# echo -n patate | md5sum  
945e9f0b4e381b13aa70b94b89a28709 -
```

Google search results for the MD5 hash 945e9f0b4e381b13aa70b94b89a28709. The search bar shows the hash and a magnifying glass icon. Below the search bar, there are tabs for All, Maps, Images, Videos, News, and More. The search results show about 98 results in 0.61 seconds. The first result is from md5cracker.org, titled "945e9f0b4e381b13aa70b94b89a28709 - md5cracker.org | The ...". The second result is from md5hashing.net, titled "Hash Md5: 945e9f0b4e381b13aa70b94b89a28709 - Md5hashing.net". The third result is from md5decoder.org, titled "patate MD5: 945e9f0b4e381b13aa70b94b89a28709 decrypted ...". The fourth result is from PasswordRandom.com, titled "PasswordRandom.com - Password Database cGF0YXRI".

List of all passwords

Did you like it? Well, then please consider making a [donation](#) :)

Your password is: patate

MD5 hash: 945e9f0b4e381b13aa70b94b89a28709

SHA1 hash: d311b1c8e5fe83187cf2d83c8e080dbcff9fc4ef

Database of all passwords *:



On fait quoi avec un *hash*? - easy mode

- Bruteforce
- Attaques hybrides *wordlists*+mask
- *Wordlists*
- Combinaison de *wordlists*
- Permutations
- Règles de Markov
- Essentiellement sur des *hashtypes* rapides
 - ↗ MD5
 - ↗ SHA-1

wordlist?

- *Rockyou.txt* a longtemps été la liste de référence
 - ↗ 32M non-uniques
 - ↗ *PLAINTEXT*
- Il y eu plusieurs *leaks* fort intéressants
 - ↗ Gawker
 - ↗ Stratfor
 - ↗ eHarmony
 - ↗ Evernote
 - ↗ ...
- Le *cracking* par GPU a remplacé les *rainbow tables*
 - ↗ Merci hashcat
- Survint le *leak* LinkedIn qui est maintenant la référence

Wordlist de référence

- Couvre bien plus des contextes variés
- Résume bien le style de mots de passes actuel
- Nouveaux patterns, nouvelles statistiques
- LinkedIn = 6x le data de rockyou
- Bien plus de monde utilise LinkedIn
- Plus récent
- Reset de 6.4M de comptes....
- ...sauf que 178M de comptes ont été *leaked*
- Causant ainsi plein d'utilisateurs à ne pas changer d'habitudes alors qu'ils auraient dû

YO DAWK, I HEAR YOU LIKE TO CRACK PASSWORDS

**SO THAT WE CAN LEARN ABOUT PASSWORDS WHICH HELPS
US CRACK MORE PASSWORDS TO ANALYZE AND CRACK EVEN MORE**

On fait quoi avec un *hash*? - hard mode

→ *Différents challenges*

↗ *Slow hashes*

- ↗ Bcrypt
- ↗ Scrypt
- ↗ Argon2
- ↗ PBKDF2
- ↗ Itérations

↗ *Salts*

```
john-1.7.9-jumbo-6/run/john -test -format=nt2 Benchmarking: NT MD4 [128/128 SSE2 intrinsics 12x]... DONE Raw: 30302K c/s  
real, 30302K c/s virtual
```

```
john-1.7.9-jumbo-6/run/john -test -format=bf Benchmarking: OpenBSD Blowfish (x32) [32/64 X2]... (6xOMP) DONE Raw: 5724  
c/s real, 947 c/s virtual
```

→ *Optimiser utilisation des wordlists et éviter bruteforce*

- ↗ Simple wordlists + rules
- ↗ Dépend quel est l'objectif, en *pentest*, besoin que d'un accès...

On fait quoi avec un *hash*? - *unknown mode*

- Contexte inconnu - les listes habituelles ont un très faible succès
- Langues étrangères?
 - ↗ Leak de VK: Passwords en cyrillic
 - ↗ <http://www.openwall.com/lists/john-users/2013/10/21/1>
- Implémentations WTFd
 - ↗ `bcrypt($password) ⇒ split(2,$password) && bcrypt($$1,"P£4",$$2)`
 - ↗ `md5($salt.rot14($password))`
- Algorithme Maison
 - ↗ Get rich or and die trying...
- Pipal
 - ↗ Utilisons les stats pour en cracker plus, avoir des pistes

Liste publique de wordlists

- <https://hashes.org/public.php>
 - Contient des wordlists associées à des leaks
 - 160M Linkedin = 96.87% cracked

4920	L1nk3d1n (SHA1)	20.09.2016 - 19:33:41	61'829'262	59'892'114 (96.87%)
------	-----------------	-----------------------	------------	---------------------



Quelques chiffres sur le benchmarking

- ➔ Specs: 3x GeForce GTX 980
 - ↗ 6144 cuda cores
 - ↗ < 10k \$

Technique	Hash Type	Speed
Pure wordlist	Unsalted SHA1	~3 700 000 000 H/s
Pure wordlist	Salted Bcrypt (2 ¹² iter = 4096)	~120 H/s
Wordlist + Rules	Unsalted SHA1	~31 000 000 000 H/s
Wordlist + Rules	Salted Bcrypt (2 ¹² iter = 4096)	~120 H/s
Pure bruteforce	Unsalted SHA1	~12 000 000 000 h/s
Pure bruteforce	Salted Bcrypt (2 ¹² iter = 4096)	~120 H/s

Quelques chiffres sur le benchmarking

- ➔ Specs: 6x GeForce GTX 970
 - ↗ 9984 cuda cores
 - ↗ < 10k \$

Hash Type	Speed
VeraCrypt PBKDF2-HMAC-Whirlpool + XTS 512 bit	205 H/s
Bitcoin/Litecoin wallet.dat	12141 H/s
bcrypt, Blowfish(OpenBSD)	38304 H/s
scrypt	1940.7 kH/s
MD5	64938.2 MH/s
NTLM	110.0 GH/s

Demo

Don't learn to hack, Hack to learn --Franck Desert

Responsabilités

Que faire pour mitiger les impacts?

Responsabilités?

- Mythes, *fails* & succès
- Bonnes et mauvaises pratiques
 - ↗ Stockage
 - ↗ Politiques
- Responsabilités
 - ↗ Sysadmins
 - ↗ Politiques de mots de passes (les gestionnaires aussi!!)
 - ↗ Stockage de mots de passes
 - ↗ Utilisateurs
 - ↗ Hacktivistes
- C'est quoi un bon mot de passe
- Mitigations

Mythes

- Je me suis pas fait hacker so...meh
 - ↗ Qui sait, peut-être qu'on lit vos e-mails sans que vous le sachiez, ou que votre compte est disponible, mais que personne a essayé encore
- C'est juste des hashes, bonne chance pour trouver mon mot de passe
 - ↗ Les taux de succès moyens en cracking de mots de passe varient de 70 à 96% en moins d'une semaine
- Bof c'est juste un compte e-mail de m...
 - ↗ Les humains ont souvent des habitudes prévisibles
 - ↗ Et si vous aviez réutilisé le mot de passe ailleurs? Ou une variante...

Mythes

- Les grosses compagnies ont assez d'argent pour bien sécuriser
- Les calculateurs de force de mots de passe sont efficaces

Password	Microsoft	The Password Meter
!!!!!!!!!!!!!!!!!!!!	Best	Very Weak
Jessica1234567	Strong	Very Strong
Qwertyabc123	Strong	Strong

- 2FA = solution ultime
- La complexité bat la longueur
- Le plus long le mot de passe, le mieux c'est

Stockage de mot de passe: FAIL

- Cleartext - \$password
 - Yeah! Encore utilisé en 2016!
- Encrypted - 3des(\$password, \$key)
 - Pass is reversible...
- Unsalted SHA1 - sha1(\$password)
 - Easy to compute (very fast)
- Unsalted MD5 - md5(\$password)
 - Easy to compute (very fast)
 - Collision en boni !
- Salted MD5/SHA1/Others - md5(\$salt:\$password)
 - Much Better. When properly done, requires other vulnerabilities to crack the dump
 - <https://crackstation.net/hashing-security.htm>



Stockage de mot de passe: Success

→ Critères

↗ Super lent

- ↗ Ne pas utiliser les algo conçus pour être performants (MD* et SHA*)
- ↗ Configurer des itérations afin de compenser l'évolution de la vitesse des machines

↗ Hash relativement long

- ↗ Rendre les collisions le plus rare possible

↗ Utiliser un ou plusieurs SALT(S)

- ↗ Salt unique à l'application - Nécessiterait d'autres vulnérabilités pour cracker un dump
- ↗ Salt unique à l'utilisateur - Rend inutilisable les compromis espace-temps (rainbow tables)

→ Le meilleur type de hash connu: bcrypt

- ↗ Holy Shit, Ashley Madison did it right !

Stockage de mot de passe: Success - bcrypt

Thanks stackoverflow.com

Stored in the database, a `bcrypt` "hash" might look something like this:

```
$2a$10$vl8aWBnW3fID.ZQ4/zo1G.q1lRps.9cGLcZEiGDMVr5yUP1KU0YTa
```

This is actually three fields, delimited by "\$":

- `2a` identifies the `bcrypt` algorithm version that was used.
- `10` is the cost factor; 2^{10} iterations of the key derivation function are used (which is not enough, by the way. I'd recommend a cost of 12 or more.)
- `vl8aWBnW3fID.ZQ4/zo1G.q1lRps.9cGLcZEiGDMVr5yUP1KU0YTa` is the salt and the cipher text, concatenated and encoded in a modified Base-64. The first 22 characters decode to a 16-byte value for the salt. The remaining characters are cipher text to be compared for authentication.

Mauvaises politiques de mots de passe

Sorry, but your password must contain an uppercase letter, a number, a haiku, a gang sign, a hieroglyph and the blood of a virgin.

som_{ee}cards
user card



Creating a password

cabbage

Sorry, the password must be more than 8 characters.

boiled cabbage

Sorry, the password must contain 1 numerical character.

1 boiled cabbage

Sorry, the password cannot have blank spaces.

50fuckingboiledcabbages

Sorry, the password must contain at least one upper



FFFFFFF
FFFFFFF
FFFFFFF
FFFUU
UUUU
UUUU
UUUU
UUUU
UUUU-

Mauvaises politiques de mots de passe

You must keep your new password for a **minimum of 24 hours** before attempting to change it again.
The password will expire 60 days after being created and can be changed before, on, or after the expiration date.

PASSWORD CRITERIA				
Password Must		Password Must Not		
Be EXACTLY 8 characters in length		Match any of your previous 10 passwords used		
Contain at least 1 Uppercase and 1 Lowercase letter		Contain your Logon ID or more than 2 consecutive characters from your first or last name		
Contain at least 1 Number		Contain consecutive repeating characters (e.g., 'aa', '\$\$', '22')		
Contain at least 1 of the following 3 special characters - @#\$ (No other special characters are allowed.)		Be too similar to your previous password – specifically, <i>must not contain 3 or more consecutive characters that match the same relative character positions with your previous password.</i>		
		Begin with any of these reserved words (list subject to change by DISA)		
		APPL	ASDF	BASIC
		DEMO	FOCUS	GAME
		LOG	NET	NEW
		ROS	SIGN	SYS
		VALID	VTAM	XXX
		1234		
		Begin with Month abbreviations – JAN, FEB, MAR, APR, MAY, JUN, JUL, AUG, SEP, OCT, NOV, DEC		

Trouble getting your new password to PASS? Click [HERE](#) to view a brief training video that can help (accessible from the ATRRS home page, Support => User Training => ATRRS-101 Online, ATRRS-101 Modules).

Mauvaises politiques de mots de passe

- Trop de conditions
- Restreindre l'entropie (caractères spéciaux, pas d'espace, ...)
 - ↗ Aucune bonne raison pour empêcher des caractères
- Tl;dr
- Longueur minimum trop élevée ou maximum trop bas
- Trop de restrictions et vous aidez les attaquants
 - ↗ Élimine des possibilités et sauve du temps aux attaquants

Mauvaises politiques de mots de passe

- Fait en sorte que les usagers:
 - ↗ Prennent des *passwords* prévisibles
 - ↗ Écrivent leurs mots de passe sur des *post-it*
 - ↗ Appellent souvent le support pour changer des MDP oubliés
 - ↗ Ignorent la politique et tentent de contourner
- Cause des *lockouts* et de la perte de productivité
- Max 8-10 caractères
- profit--;

Bonnes politiques de mot de passe

- Faire comprendre les avantages en éduquant
 - ↗ Inclut de la formation et des ateliers
- Tout pour compliquer la tâche de l'attaquant
- Ne pas assumer que personne n'accède aux *hashes*
 - ↗ *Multiples layers de sécurité*
- Politiques décrites clairement
- Intégrer la notion d'imputabilité dans la culture de l'organisation
- Entre 8 et 20 caractères
 - ↗ Plus et c'est *overkill* en termes de ratio performance/sécurité

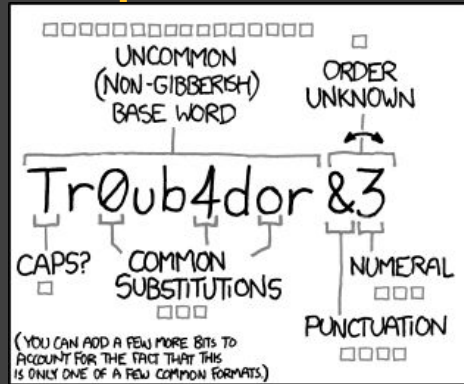
Bonnes pratiques pour l'utilisateur moyen

- Utiliser des mots de passe non-reliés d'un système à un autre
- Ne pas réutiliser/incrémenter de mots de passe
- Utiliser un gestionnaire de mots de passe comme KeePass
- Ne pas inscrire sur des post-it sous le clavier
- Employer des moyens mnémoniques
- Utiliser des termes peu connus, très spécifiques
- Gardez la complexité en fonction de ce qu'il y a à protéger
- Capacité de "taper sur les doigts"

Bonnes pratiques pour l'utilisateur moyen (2)

- Utiliser d'autres langues
 - ↗ Qui penserait que votre mot de passe est *dievushka* (деевушка)?
- Faites des fautes ou permutations intentionnelles
 - ↗ alibaabet04Vauleur
- Ne pas inclure de données personnelles
 - ↗ patate701004
- Longueur moyenne de 14-18 caractères
- Mixer des *charsets* et inclure des caractères uniques
 - ↗ jamÉlançeザンギエフ
- Filtrer les passwords de rockyou.txt et 500worstpws.txt
 - ↗ Et leurs traductions peut-être....

Ça l'air de quoi un bon mot de passe?



~28 BITS OF ENTROPY

$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$

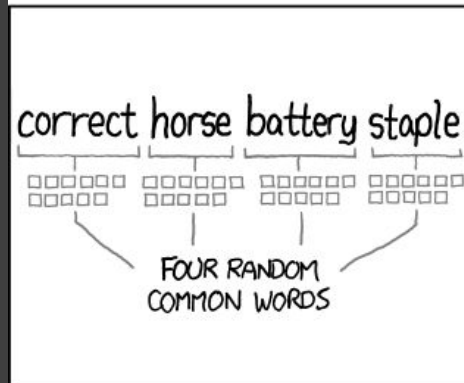
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS: **EASY**

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?

AND THERE WAS SOME SYMBOL...

DIFFICULTY TO REMEMBER: **HARD**



~44 BITS OF ENTROPY

$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$

DIFFICULTY TO GUESS: **HARD**

THAT'S A BATTERY STAPLE.

CORRECT!

DIFFICULTY TO REMEMBER: **YOU'VE ALREADY MEMORIZED IT**

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Les pires mots de passe en 2015

RANK	PASSWORD	CHANGE FROM 2014			
1	123456	Unchanged	8	1234	1 ↘
2	password	Unchanged	9	1234567	2 ↗
3	12345678	1 ↗	10	baseball	2 ↘
4	qwerty	1 ↗	11	welcome	NEW
5	12345	2 ↘	12	1234567890	NEW
6	123456789	Unchanged	13	abc123	1 ↗
7	football	3 ↗	14	111111	1 ↗

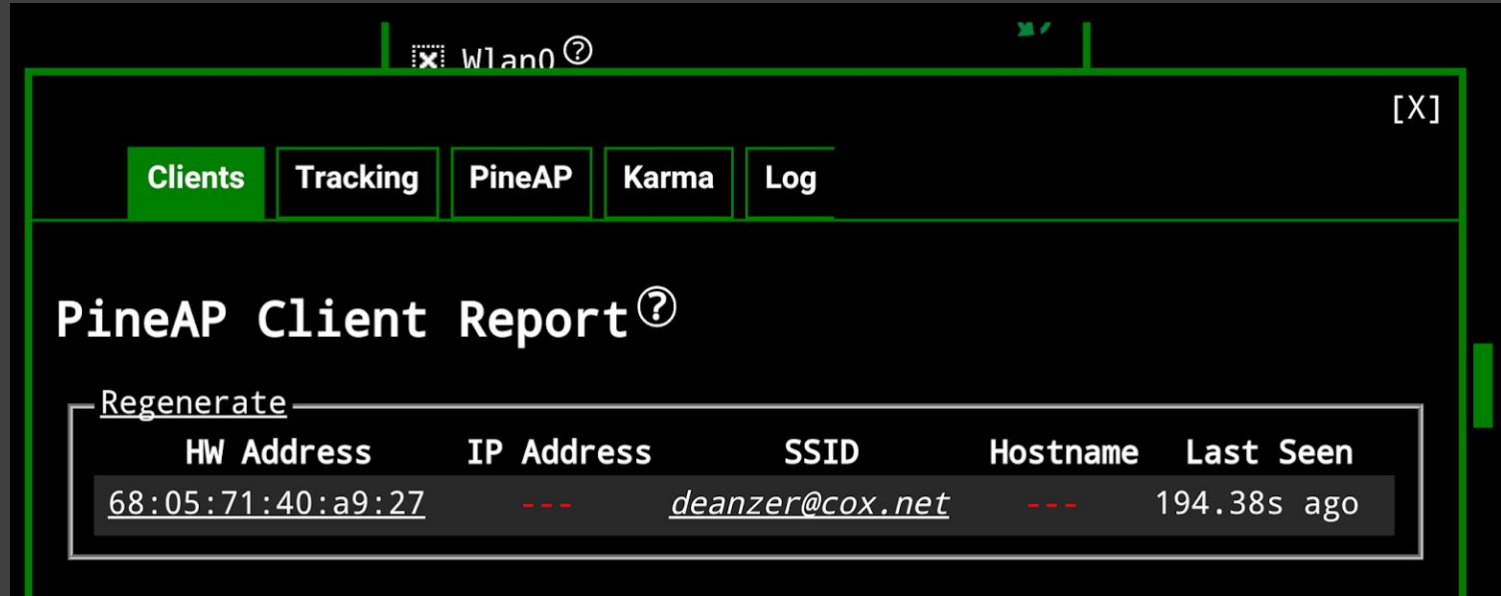
Responsabilités sous divers angles

- Administrateurs et gestionnaires
 - ↗ Mettre en place des politiques de mots de passe adéquates
 - ↗ Mettre le *software* et l'OS à jour
- Utilisateurs
 - ↗ Choisir un mot de passe adéquat
 - ↗ Garder celui-ci secret (ne pas l'écrire)
- Fournisseurs de service
 - ↗ Mettre en place des moyens de mitigation adéquats
 - ↗ Hasher et salter
 - ↗ Politique adéquate + sensibilisation
 - ↗ Pentests réguliers
 - ↗ Pratiques de développement sécuritaire
 - ↗ Disaster Recovery planifié
- *Responsible leaking* (à défaut d'un meilleur terme...)

Exemples de mitigation

- 2FA
- Ne pas réutiliser de mots de passe, même si c'est un +1
 - Andraia33 ==> Andraia34
- Faire changer les mots de passe régulièrement (pas trop souvent), surtout si c'est *leaked*
 - 120-180 jours
- Bloquer les mots de passe les plus fréquents ou d'un dictionnaire
- Bien choisir le type de hash (rapide vs lent, ...)
 - Et mettre du sel
- Faire en sorte que ça ne *leak* pas?
 - Mettre à jour
- Changer les mots de passe par défaut... ou les éviter
 - Facile d'oublier de changer!

What could go wrong?



Wlan0 ?

[X]

Clients Tracking PineAP Karma Log

PineAP Client Report ?

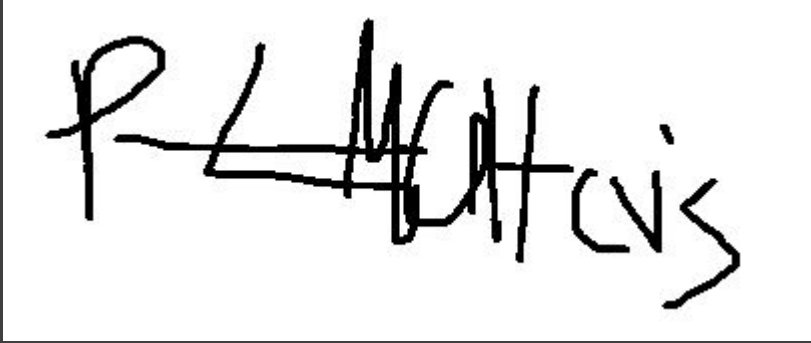
[Regenerate](#)

HW Address	IP Address	SSID	Hostname	Last Seen
<u>68:05:71:40:a9:27</u>	---	<u>deanzer@cox.net</u>	---	194.38s ago

Ressources intéressantes

- Forums hashcat
- Mailing-list openwall/johntheripper
- IRC
 - ↗ Irc.freenode.net
 - ↗ #hashcat
 - ↗ #openwall
- /r/passwords
- Cracking CTFs *writeups*
 - ↗ CMIYC
 - ↗ PHDays Hashrunner
 - ↗ ...*plenty more*

Thanks to participants



- And also
- Franck Desert
 - Stéphane Sigmen
 - Dave Cloutier
 - François Gagnon



- And also
- Marc-André Meloche
 - Maxime Mercier
 - Simon Nolet



YOU^W SHALL



NOT "REUSE YOUR" PASS

Thanks

By vn and Mart