PatrOwl

Casser des mots de passe…

Vladimir KOLLA

Vlad - 14 mai 2019

Casser des ~~mots de passe~~ Condensats

...sans violence 😘

PatrOwl

1. **Pourquoi cette présentation ?**
   - Quelques justifications
   - La vraie raison !
2. Casser des condensats ?
3. L'outillage
4. Les familles d’attaque
5. « Cassages » récents (2019)
6. Une conclusion

Quelques justifications

Pourquoi ?

C’est rigolo

Mots de passe = Problématique de sécurité

Pour comprendre la psyché des gens

Votre profil psychologique en fonction de votre mot de passe LinkedIn (Jiss)
https://static.sstic.org/rumps2017/SSTIC_2017-06-08_P11_RUMPS_11.mp4

La vraie raison !

Vendredi

J> « Bidule » n’est plus disponible, qui le remplace ?

H> Malheureusement, je n'ai trouvé personne

Vlad> Je peux faire une «prez»

Hier soir

Femme de V> Tu ne dois pas faire une «prez» demain ?

V> Aaaaaaaaaaaaaahhhhhhhhhhhhhhhhhhh

ISO-1664 : **I**nternational **I**nstitute of **La R**ACHE

1. Pourquoi cette présentation ?

2. Casser des condensats ?

D’où viennent ces condensats ?
à quoi ça sert de casser des condensats ?

3. L'outillage

4. Les familles d’attaque

5. « Cassages » récents (2019)

6. Une conclusion

D'où viennent ces condensats ?

Local	Base SAM et « MS-Cache » Coffres-forts de mots de passe
Réseau	Défis-Réponse NTLM (Responder) SQLi, RCE, WiFi (PMKID)…
« God » mode	ntds.dit + Registre « SYSTEM » Leaks

À quoi ça sert de casser des condensats ?

Utilité ?

À rien, car il y'a **pleins** d'autres moyens de p0wn

En fait si, à cause du « **Password Spraying** »

1. Pourquoi cette présentation ?

2. Casser des condensats ?

3. L'outillage

- Le matériel
- Le logiciel

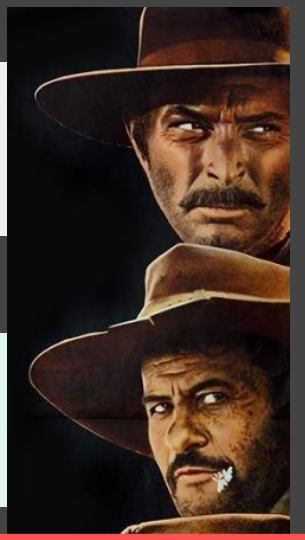
4. Les familles d’attaque

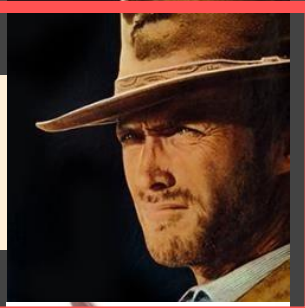
5. « Cassages » récents (2019)

6. Une conclusion

Le matériel

Le Pauvre	PC + GTX **1080Ti** (~60GH/s) ou GTX **1660Ti** (?)
Le Riche	**Sagitta** (NTLM: 311.6 GH/s) ou **Kraqozorus**
Le Cloud	VM **Azure** ou **AWS** 👌 (si occasionnel)
Le Malin	PC **Shadow** + GTX **1080** à 30€/mois





Le matériel

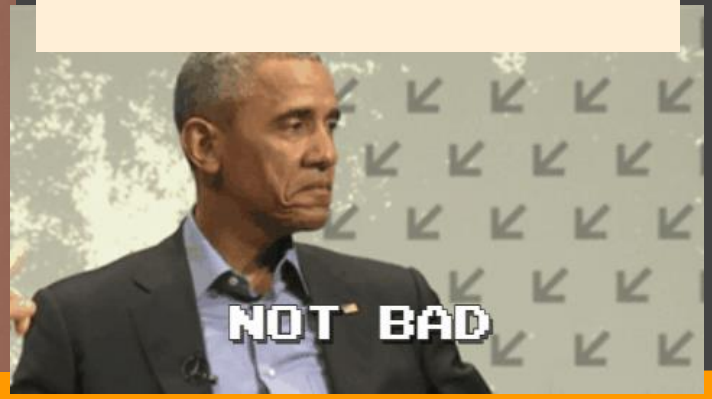
Azure	NV6	NV12	NV24
Cores	6 (E5-2690v3)	12 (E5-2690v3)	24 (E5-2690v3)
GPU	1 x M60 GPU (1/2 Physical Card)	2 x M60 GPU (1 Physical Card)	4 x M60 GPU (2 Physical Cards)
Memory	56 GB	112 GB	224 GB
Disk	380 GB SSD	680 GB SSD	1.44 TB SSD

~100€/jour
(3 jours suffisent)

En réalité: 0€ car droit à 12k€ de VM si partenaire

20 min. d'install

NTLM: 72.3 GH/s



Le logiciel

1. Pourquoi cette présentation ?

2. Casser des condensats ?

3. L'outillage

4. Les familles d’attaque

- ~~Les~~ Mes familles d’attaques
- Les dictionnaires

5. « Cassages » récents (2019)

6. Une conclusion

~~Les~~ **Mes** familles d'attaques

Exhaustive	1 à 7 caractères (<1h)	. . .
Formes usuelles	Mots capitalisés + chiffres +/- caractères spéciaux	`Aaaa11` ⇨ `Aaaaaaa1111` `Aaaa11$$` ⇨ `Aaaaaaa1111$$`
Dictionnaires	Dictionnaires +/- règles *(règles hashcat + « vlad » 3 millions)*	`Password` ⇨ `Password2019`

Les dictionnaires

Public	Crackstation	**15 Go**
Ciblé	Wikipedia, Articles, Blog, Site web Identifiants, combinaisons « nom/prénom » Mots, noms, prénoms… « locaux »	**< 10 Mo**
Leaks + Perso	Élevage bio, avec amour Manga, sport, films, tolkien...	**40 Go**

1. Pourquoi cette présentation ?

2. Casser des condensats ?

3. L'outillage

4. Les familles d’attaque

5. « Cassages » récents (2019)

- Statistiques NTLM
- Résultats par attaque
- Les pires et les rigolos

6. Une conclusion

« Cassages » récents (2019)

Statistiques NTLM

Mots de passe


Comptes machines non retrouvés

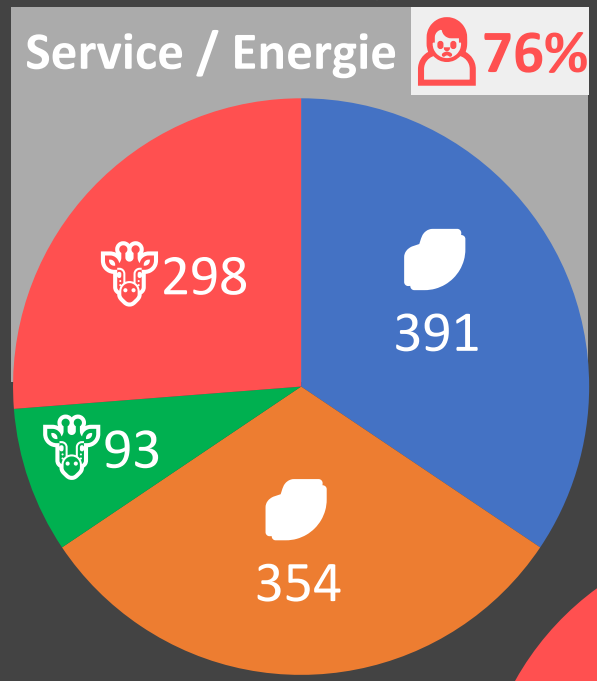

Cassés / retrouvés

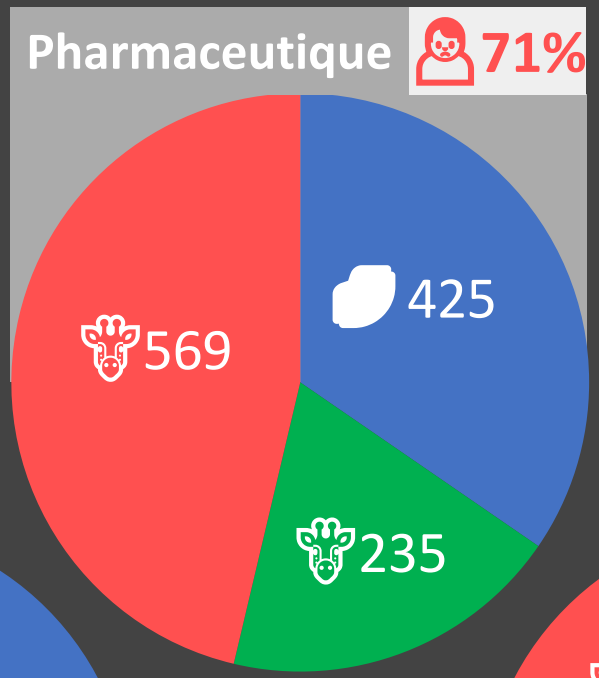

Comptes utilisateurs non retrouvés

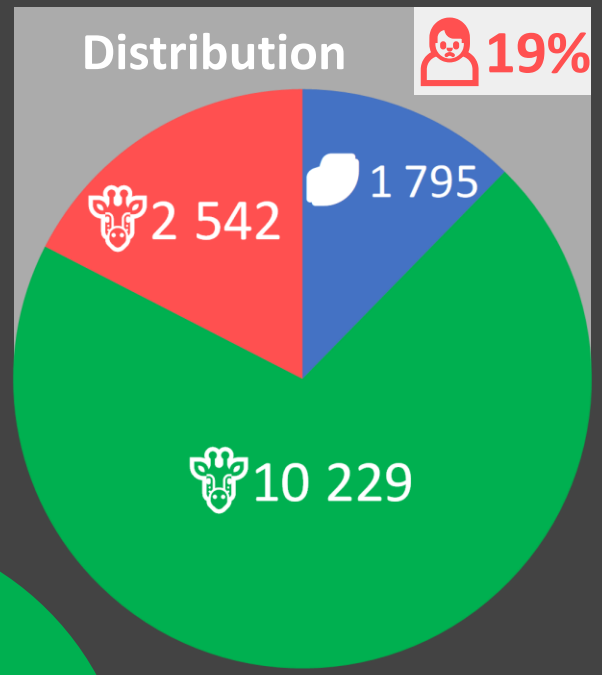

Cassés / retrouvés

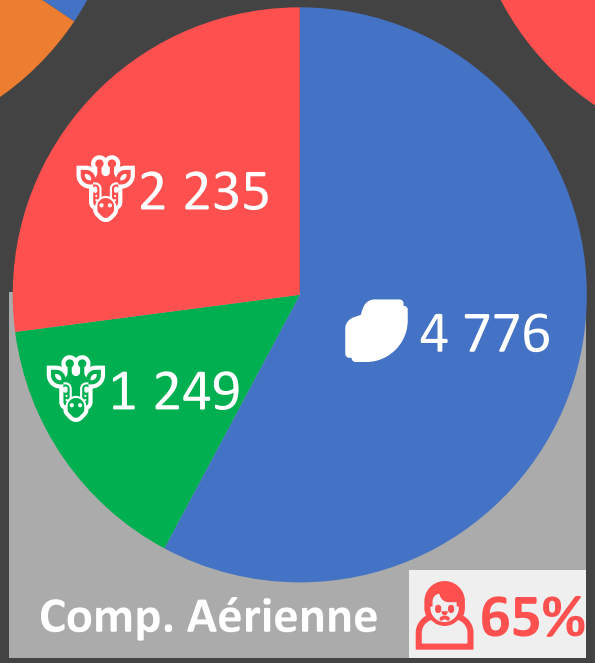
« Cassages » récents (2019)

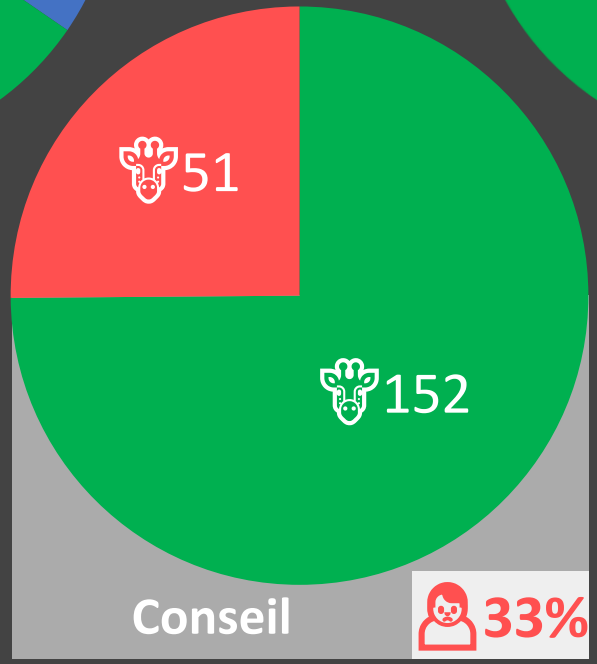
Statistiques NTLM











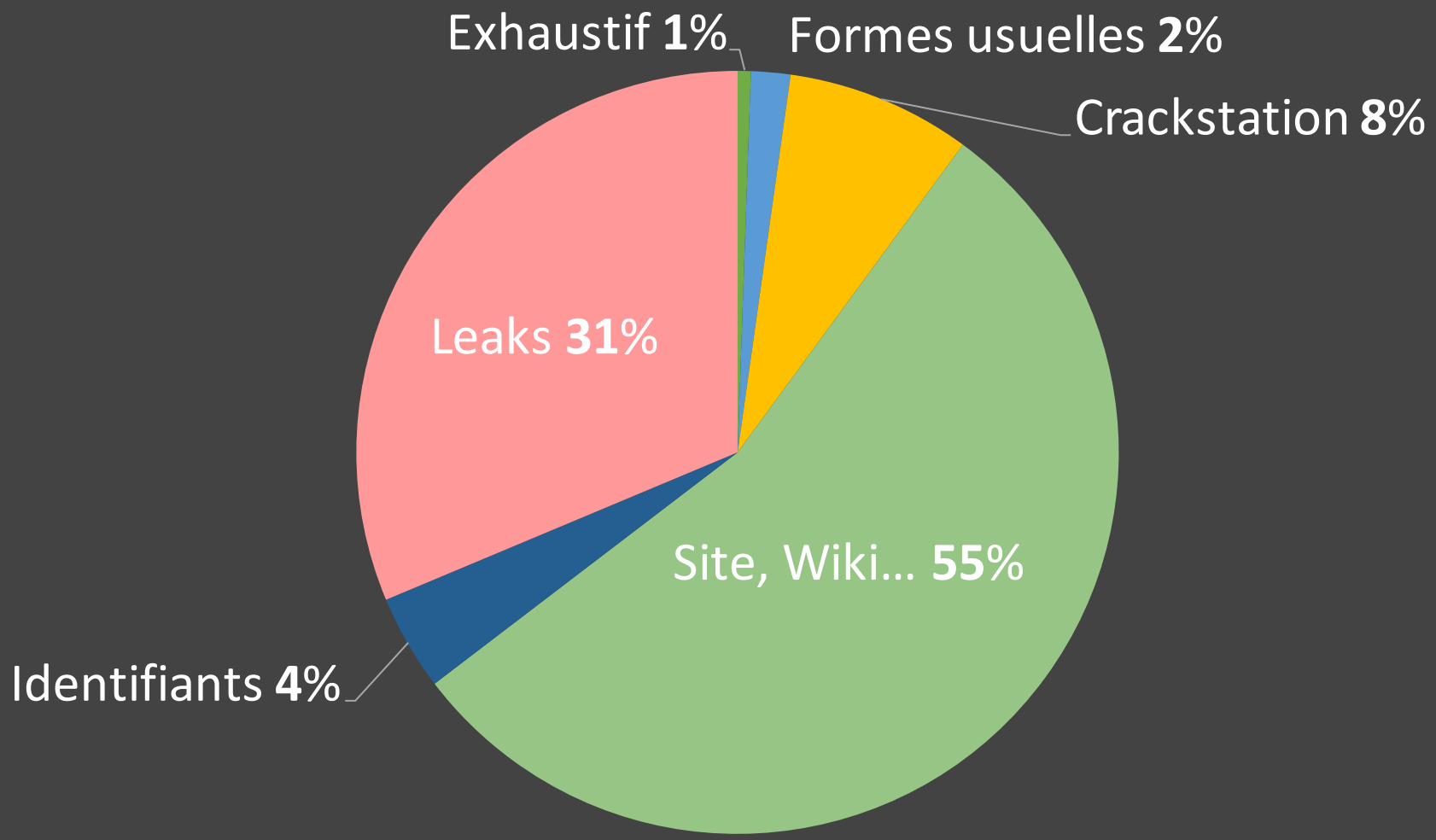
« Cassages » récents (2019)

Statistiques NTLM

		Stratégie de complexité	Longueur minimale	Expiration
Service / Energie	76%	✗	✗	✗
Pharmaceutique	71%	✗	✗	✗
Comp. Aérienne	65%	incomplète	✗	✗
Conseil	33%	✓	?	✗
Distribution	19%	✓	10 (puis 12)	6 mois

« Cassages » récents (2019)

Résultats par attaque

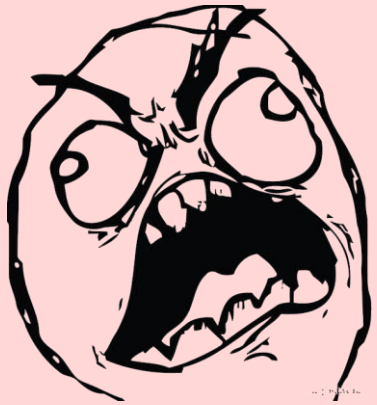


Statistiques totalement **arbitraires**

Les pires et les rigolos

Les pires

(Entreprise « Machin »)



Password01

Password10

Machin2018

MAC2018

M@C2018

Machin001

Machin1

Les rigolos

ChangeMe123!

ChangeMe123#!

CrackMe123

gogolito92!

PSGcdpd8

"Nom de produit/offre"

"Nom de molécule"

audit**hsc**_user: Herv%$chikh22301!

1. Pourquoi cette présentation ?

2. Casser des condensats ?

3. L'outillage

4. Les familles d’attaque

5. « Cassages » récents (2019)

6. Une conclusion

Les mots de passe c’est tout pourri

Alternatives et solution ?

Les mots de passe c'est tout pourri

Longueur et **entropie** limitées

Chaine de caractères **courte**
(longueur de 32 caractères < clef de 2048 bits)

Chaine de « **caractères** », même si unicode

Dualité **complexité / expiration**

Expiration **30** à **90j** ⇨ mots de passe **moisis** ou incrémentés

👍 Expiration de 6 à **12** mois
(avec une forte complexité et longueur importante)

Les mots de passe c’est tout pourri

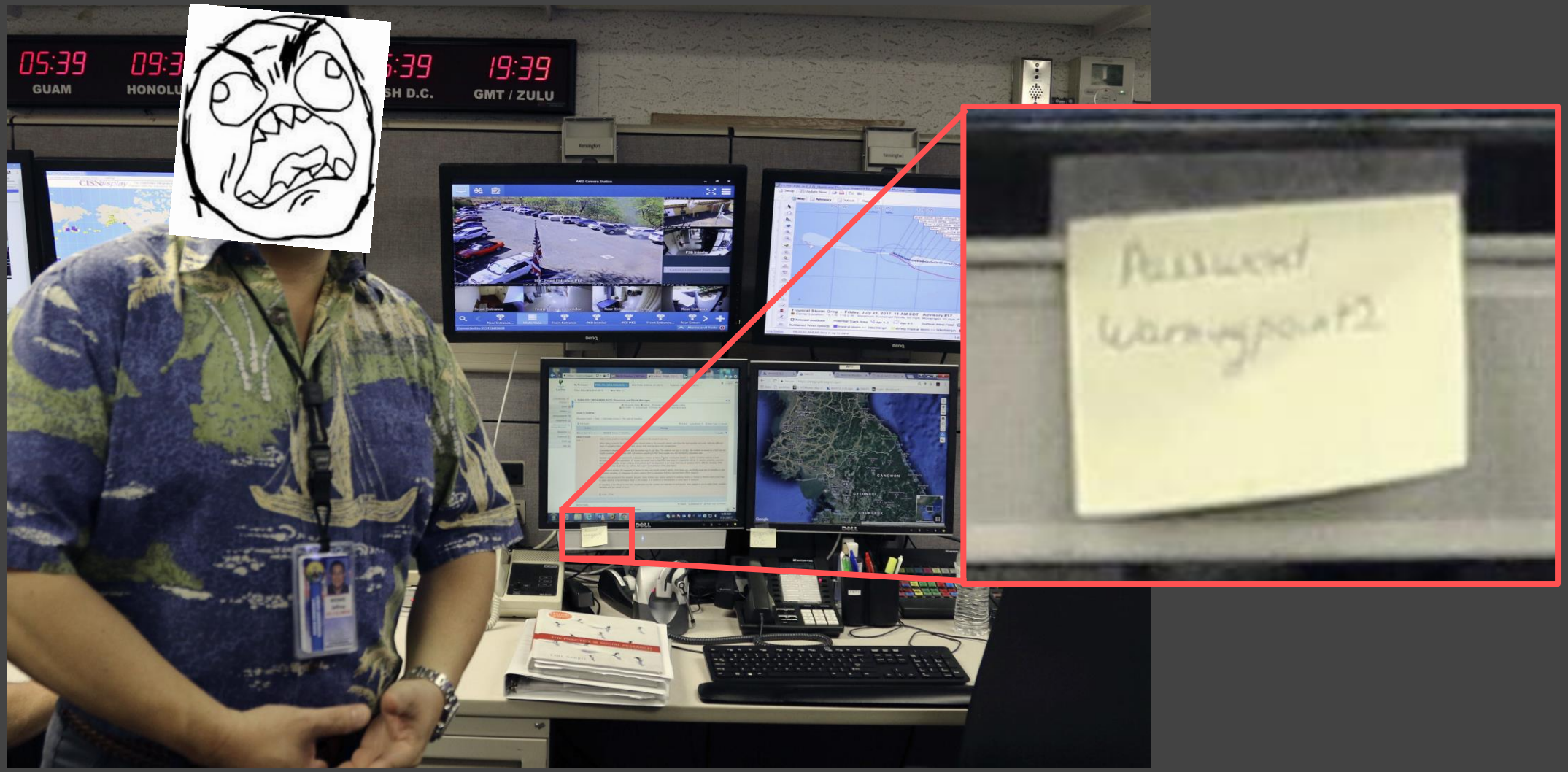
Humain = Capacités de mémorisation **limitées**

Impossible de **mémoriser** de **nombreux** mots de passe solides

👍 **Conteneurs** de mots de passe (hors ligne ou SaaS) mais :

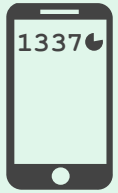
- Risque fort en cas de fuite de la base
- Peu (pas?) de solution changeant les mots de passe sur tous les composants

Les mots de passe c’est tout pourri



Alternatives et solution ?

Authentification forte à double facteurs, avec 2 facteurs parmi



Ce que je **possède**
(token, smartphone, pc…)

Ce que je **suis**
(carte d'identité, biométrie…)

Ce que je **connais**
(mot de passe)

Ce que je **sais faire**
(signature, dessin…)

L'endroit où je suis
(géolocalisation)

Alternatives et solution ?

Alternative
Mots de passe + Certificat
Mots de passe + TOTP/HOTP
Carte à puce + PIN
YubiKey « seule »
SSO avec SAMLv2, Open ID Connect)

« La » solution ?
WebAuthn
YubiKey (FIDO)
avec ou sans
Fédération d'identité (Délégation)

Reste la question du changement des secrets