SYNACKTIV
DIGITAL SECURITY

Cassage d'empreintes de mots de passe avec Kraqozorus

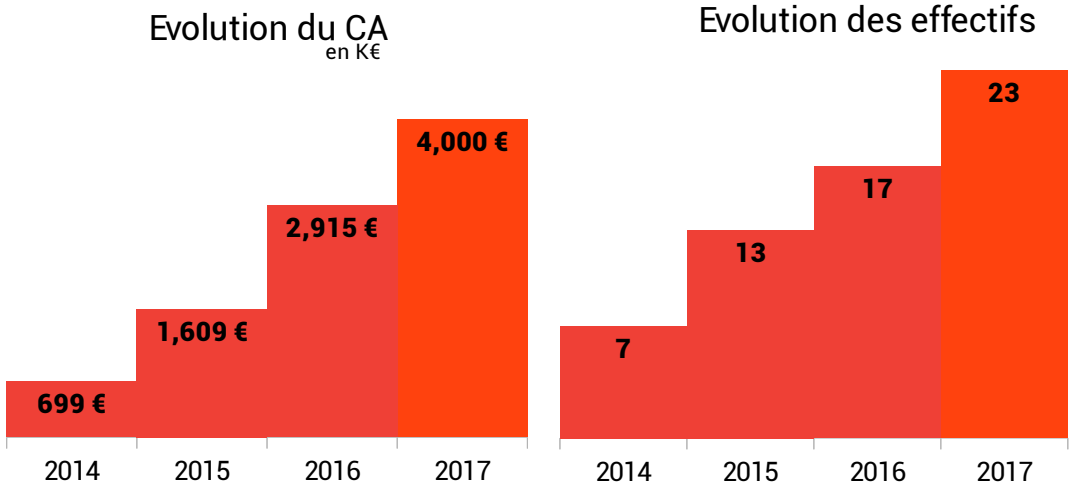
Présenté le 14/11/2017
Pour l'OSSIR Paris
Par Renaud Feil

Innovation | Expertise

Pertinence | Sécurité

Transparence | Passion

- **Avril 2012 : création de Synacktiv**
- **Expertise en sécurité des systèmes d'information**
- **2 associés fondateurs**
  - 12 ans d'expérience dans l'audit de sécurité
  - Membres de l'équipe francophone des *Routards*, finalistes du concours international d'intrusion DEFCON CTF (*Capture The Flag*)
- **Intervention en France et dans le monde entier**

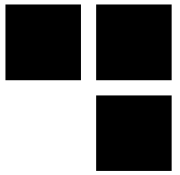


Ambition : Être une référence française en sécurité offensive

Le cassage d’empreintes de mots de passe

Pourquoi ? Comment ?

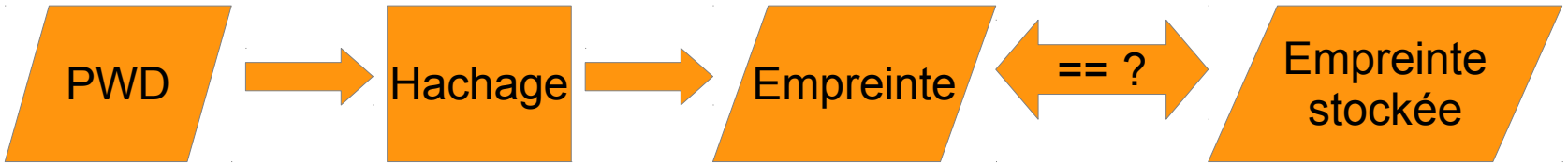
L'éternel problème des mots de passe faibles



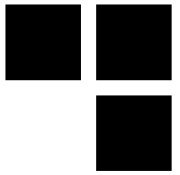
- **Faiblesse des mots de passe :**
  - Vulnérabilité grave
  - Toujours très répandue
- **Attaques en ligne et attaques hors-ligne :**
  - Qu'est-ce qu'un mot de passe « fort » ?
  - Avec les empreintes, il est possible selon l'algorithme de retrouver même des mots de passe « solides »
- **Agenda :**
  - Pourquoi casser les empreintes de mots de passe
  - Rappels théoriques
  - L'outil Kraqozorus
  - Contre-mesures et protection des empreintes

Stockage des mots de passe

- **Stockage en clair ou encodage**
- **Chiffrement :**
  - Permet de retrouver le mot de passe en connaissance la clé
- **Hachage :**
  - Fonction à sens unique
  - A partir d'une donnée arbitraire, génère une empreinte (ou hash, condensé, condensat, etc.)
  - Le système stocke une empreinte du mot de passe
  - Comparaison de l'empreinte du mot de passe soumis par l'utilisateur à l'empreinte stockée



Les fonctions de hachage

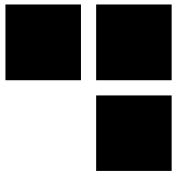


- **Effet avalanche de la fonction de hachage**

```
$ echo -n aaaa | md5sum
74b87337454200d4d33f80c4663dc5e5  -
$ echo -n aaab | md5sum
4c189b020ceb022e0ecc42482802e2b8  -
```

- **Fonction de hachage « idéale » :**
  - Résistance au calcul de la première préimage
  - (Résistance au calcul de la seconde préimage)
  - (Résistance aux collisions)
  - ~~Calcul rapide~~
- **Vulnérabilités dans les fonctions de hachage :**
  - Met souvent en cause son utilisation comme contrôle d'intégrité / signature
  - Pas toujours son utilisation pour le stockage de mots de passe

Pourquoi casser les empreintes ?



- **Avancer dans une intrusion :**
  - Accès aux fonctions d'administrations (ex : injection SQL dans commande SELECT)
  - Compromettre les systèmes sur lesquels le même mot de passe est réutilisé (ex : compte Administrateur Windows local)
  - Récupération d'un fichier de sauvegarde contenant les empreintes
  - Interception de l'empreinte sur le réseau (ex : *man-in-the-middle* lors de l'authentification d'un client légitime)
- **Recherche lors d'enquêtes forensiques :**
  - Documents Microsoft Office protégés, archives chiffrées, etc.
- **Parfois pas nécessaire :**
  - Mot de passe en clair (sur disque ou en mémoire)

```
Authorization: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==
$ echo QWxhZGRpbjpvcGVuIHNlc2FtZQ== |base64 -d
Aladdin:open sesame
```

  - Mécanisme d'authentification vulnérable au *pass-the-hash* : utilisation directe de l'empreinte pour s'authentifier

Attaque des fonctions de hachage

- **Collisions**
  - Vulnérabilités quand la fonction de hachage est mal conçue (ensemble d'arrivée trop petit)
  - Paradoxe des anniversaires
- **Attaque par force-brute sur les mots de passe candidats**
  - Protection par *Key Stretching*

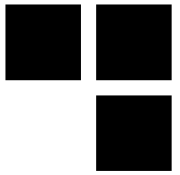
```
for 1 to 65536 do
  key = hash(key + password + salt)
```

- **Génération de tables précalculées**
  - Utilisation d'un sel (*salt*)

Les enjeux actuels

- **Des algorithmes de plus en plus solides**
- **Mais des techniques de cassage de mots de passe de plus en plus puissantes :**
  - CPU
  - Tables précalculées (rainbow tables)
  - GPU
  - FPGA (ex : COPACOBANA)
  - ASIC (ex : Deep Crack)
  - Répartition multi-noeud, cloud (CPU, GPU, etc.)
- **Quelques outils clés :**
  - John the Ripper (JtR) jumbo patch
  - hashcat
  - RainbowCrack et Ophcrack

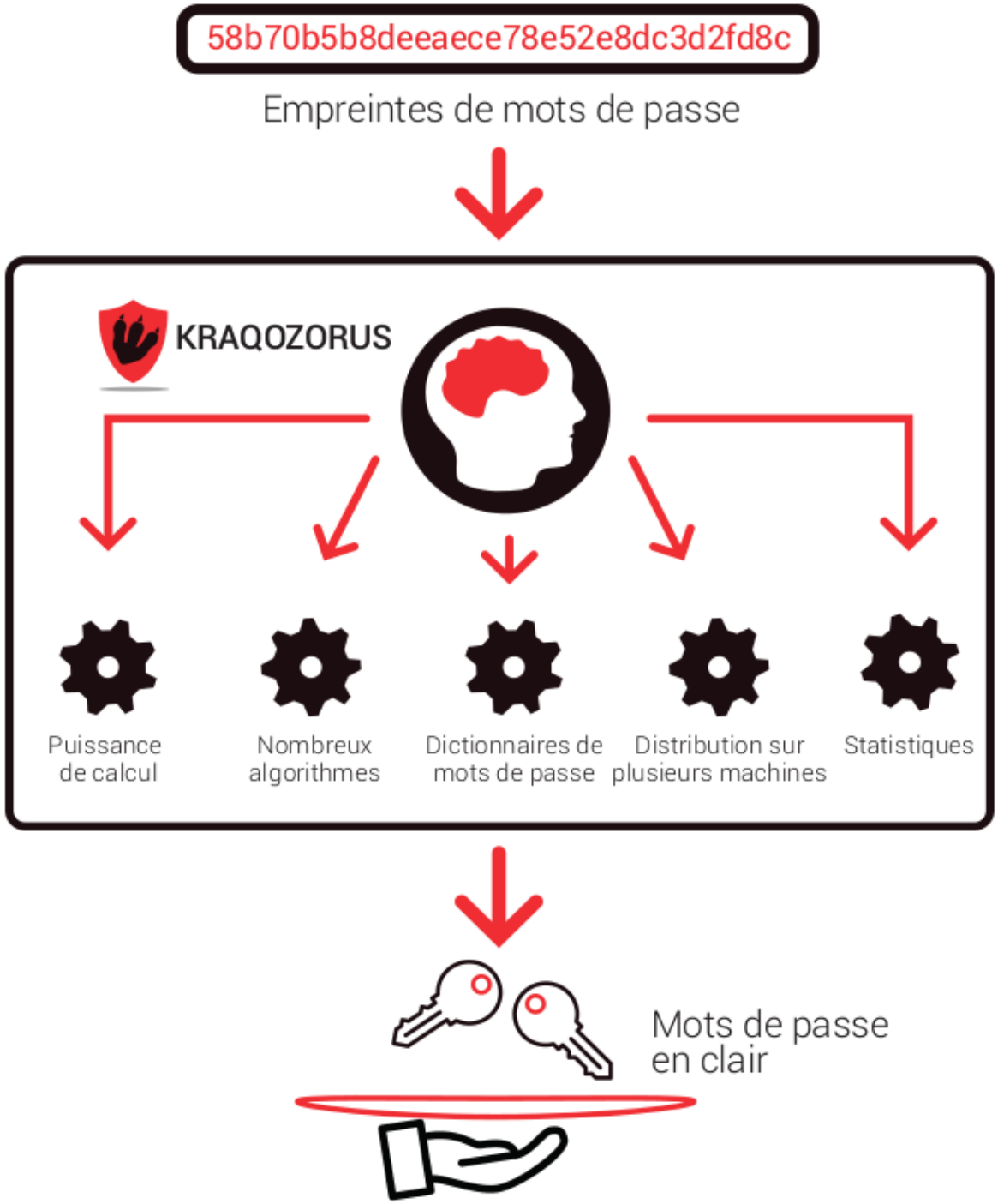
Génération des mots de passe candidats



- **Force brute**
- **Masque**
- **Dictionnaires**
  - Très efficace
  - Outils complémentaires comme WyD
- **Chaînes de Markov**
- **Règles de dérivation**
- **Prince processor**
  - Combinaisons de mots d'un dictionnaire

Kraqozorus

Plateforme de cassage d'empreintes de mots de passe

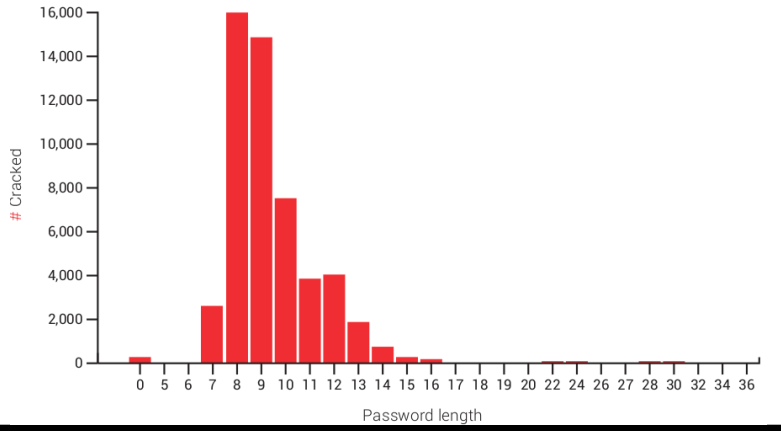

58b70b5b8deeaece78e52e8dc3d2fd8c
Empreintes de mots de passe
KRAQOZORUS
Puissance de calcul
Nombreux algorithmes
Dictionnaires de mots de passe
Distribution sur plusieurs machines
Statistiques
Mots de passe en clair

Kraqozorus : fonctionnalités

- **Puissance de calcul**
  - Jusqu'à 8 cartes graphiques par machine
  - 99% des empreintes de mots de passe cassées sur des fuites publiques
  - Plus de 300 milliards de mots de passe testés par seconde (algorithme Windows)

- **Personnalisation des campagnes de cassage**
  - Création de stratégies
  - Sélection de dictionnaires
  - Configuration de la politique de mots de passe
  - Choix de la priorité des tâches

- ***Dashboard***
  - Statistiques sur les mots de passe trouvés



Kraqozorus : spécifications

- **Matériel :**
  - 8 cartes GPU Nvidia GTX 1080Ti
  - Bi-processeur Xeon E5-2600 series
  - 128 Go de RAM DDR4
  - 2 disques SSD de 500 Go
  - 4U Rackmount – TYAN
  - Prises C13 EU + US
  - 2 alimentations (total 3200 W) – 3 prises électriques


GEFORCE GTX
GEFORCE GTX
GEFORCE GTX
GEFORCE GTX
GEFORCE GTX
GEFORCE GTX
GEFORCE GTX
GEFORCE GTX
REAR
REAR
REAR
REAR
REAR
REAR

Kraqozorus : fonctionnalités

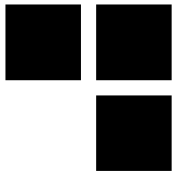
- **Supports des types d'empreintes**
  - Plus de 60 formats d'empreintes testés
  - Supporte tous les formats *John* et *Hashcat*
  - Possibilité d'ajouter des nouveaux formats, y compris développements sur mesure

- **Nombreux dictionnaires**
  - Plus de 100 Go de dictionnaires
  - Intégration des dictionnaires provenant de fuites publiques
  - Recyclage automatique des mots de passe cassés pour trouver des dérivations

Protections

Plateforme de cassage d'empreintes de mots de passe

Protéger les empreintes



- **Protéger les empreintes**
  - Corriger les injections SQL et autres vulnérabilités permettant d'accéder aux empreintes de mots de passe
  - Empêcher les accès privilégiés sur les machines
  - Chiffrer les disques pour éviter les accès hors-ligne aux disques
  - Attention aux fichiers de sauvegarde
- **Ne pas réutiliser le même mot de passe**
- **Définir une politique de mot de passe solide**
  - Passphrases
  - Changement régulier (en cas d'indiscrétion)
  - Audit régulier des empreintes
- **Utiliser un deuxième facteur d'authentification**

AVEZ-VOUS DES QUESTIONS ?

MERCI DE VOTRE ATTENTION,

SYNACKTIV
DIGITAL SECURITY