

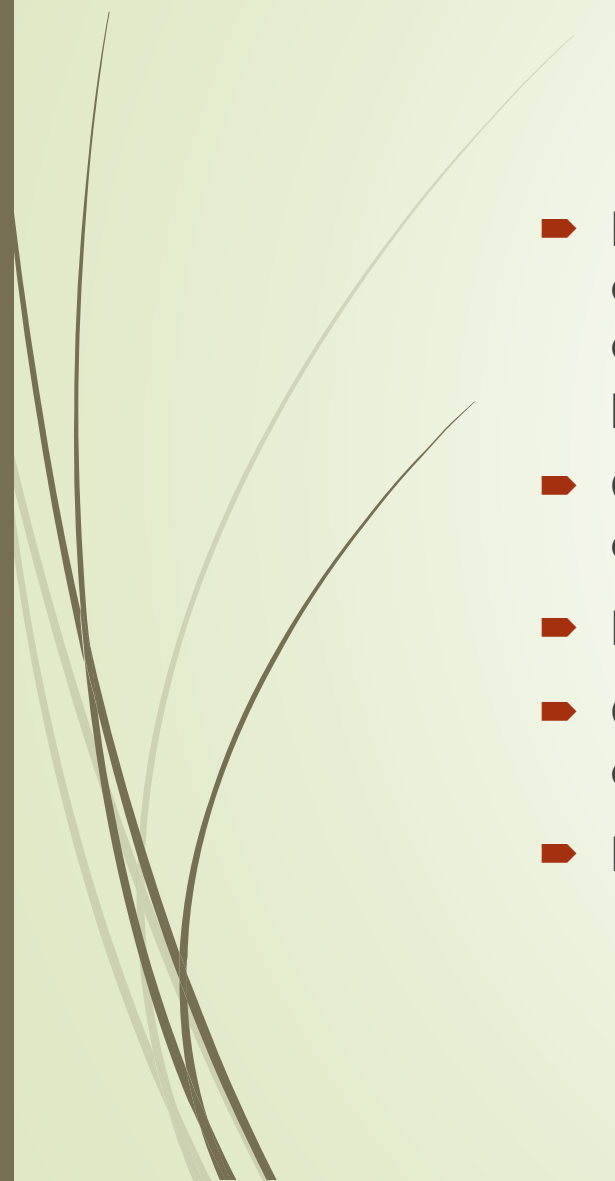


SKIMMERS

Jean-Louis Courteaud - Septembre 2014



SKIMMERS



- Dispositif placé en façade d'un distributeur de billets / distributeur automatique de carburant qui va lire la carte bancaire du consommateur avant le « vrai » lecteur et qui va enregistrer les données contenues dans la piste magnétique ISO.
- Ces distributeurs lisent la piste magnétique pour des raisons de compatibilité internationale (cartes étrangères sans puce).
- La vérification du code s'effectue par circuit dit « hybride ».
- On trouve en général des dispositifs qui permettent de capturer le code composé (caméras, surclaviers, ...).
- Les données volées sont stockées en local, télétransmises (BT).



SKIMMERS

- Les données volées sont recueillies sur un support (PC/TELEPHONE) avant d'être transmises (souvent via SKYPE) à l'étranger.
- OU
- Le matériel est rapatrié à l'étranger (Roumanie) (Vol low cost / Confiance dans les mules).

EXEMPLES DE SKIMMERS ET CLAVIERS



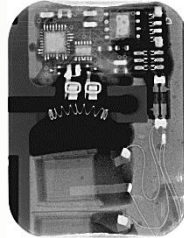


Affaire de skimming : On peut trouver

- Des skimmers.
- Des claviers.
- Des caméras.
- Des transmetteurs (essentiellement BT).
- Des PC.
- Des téléphones (essentiellement smartphones).

TRAITEMENT EXPERTAL

- Recherche documentaire sur les appareils (sites chinois).
- Radiographie .

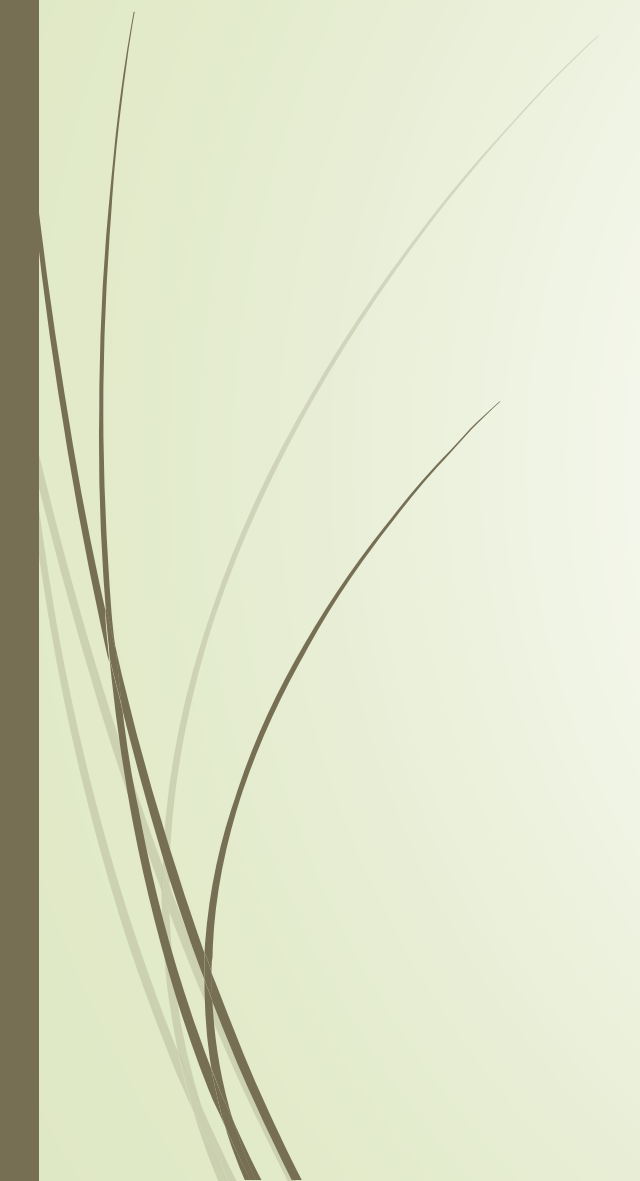


- **Cas 1** : Dessoudage du composant et lecture directe.
- **Cas 2** : Connexion sur un PC et extraction des données (attention au sens de lecture).
- **Cas 3** : Extraction des données du PC/Téléphone.
- Ensuite XWAYS est mon ami ou développement d'un bout de soft pour extraire les n° de carte du dump obtenu.
- Appairage pistes et codes.
- Contact GIE Cartes Bancaires pour recherche des points de compromission.



DIFFICULTES

- Casser la couche de protection sans casser les composants (Radios).
- Dessoudage.
- Disposer du bon socket (documentation) pour connexion.
- **Nouveauté** : Cryptage direct sur les composants d'où l'importance de disposer des collecteurs (PC/téléphones).
- Obtenir du Juge l'autorisation de rendre les scellés dans un état beaucoup moins présentable qu'au départ 😊.



MERCI DE VOTRE ATTENTION