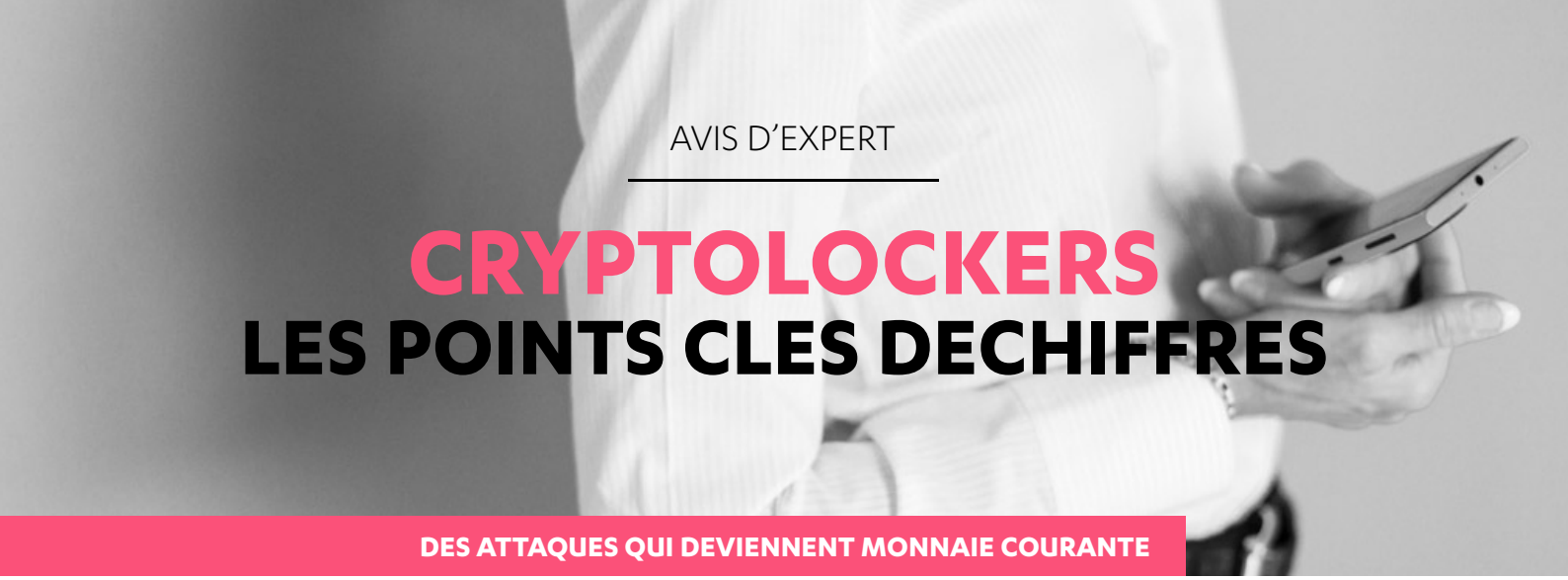


AVIS D'EXPERT

CRYPTOLOCKERS
LES POINTS CLES DECHIFFRES

DES ATTAQUES QUI DEVIENNENT MONNAIE COURANTE

En activité depuis 2013, les cryptolockers ou cryptovirus appartiennent à la famille des ransomware ou en français des rançongiciels.
Ce sont des **chevaux de Troie** spécialement conçus pour **bloquer vos appareils** : ordinateurs, portables Windows ou MAC, tablettes, smartphones, environnements de machines virtuelles (VDI). Une prise d'otage en somme pour vous demander, via une boîte de dialogue, une rançon en échange d'un déblocage.

LES RANSOMWARE

LES RANCONGICIELS POLICIERS

Ils utilisent des logos d'autorité policière, parfois même ceux du FBI ou de la CIA, pour réclamer le paiement d'une rançon.

LES BLOQUEURS PAR PUBLICITE

Il s'agit d'une variante plus récente qui invite l'utilisateur à **cliquer sur des publicités**, l'auteur du virus se rémunérant au nombre de clics.

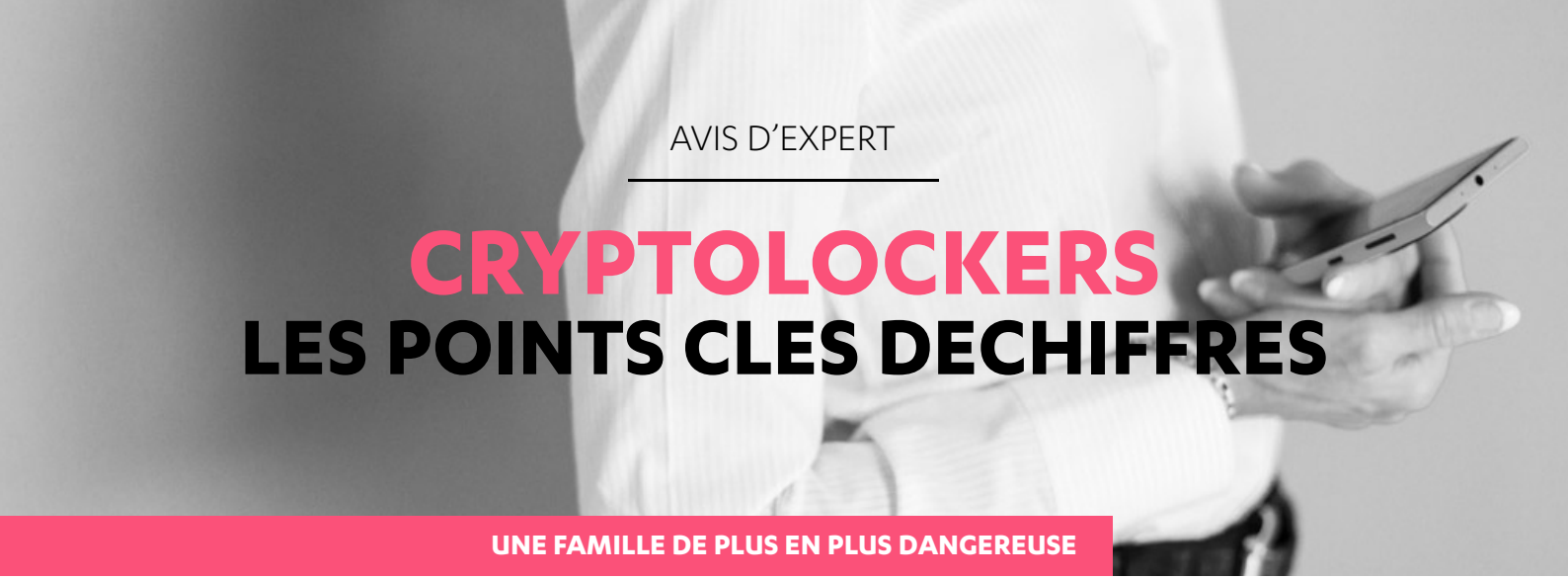
LES CRYPTOLOCKERS OU CRYPTOVIRUS

Ils procèdent quant à eux par le **chiffrement des données de vos appareils** et des fichiers partagés s'ils sont reliés à un lecteur réseau.
Une clé de déchiffrement est nécessaire pour les récupérer. Celle-ci, souvent unique, est générée pour chaque appareil infecté. Elle peut se trouver sur le support mais c'est aujourd'hui de plus en plus rare...

Ces cryptovirus s'introduisent de différentes manières :

- Attaque par **phishing ou hameçonnage** : l'infection se fait par l'ouverture d'une pièce jointe exécutable ou le clic vers un site malveillant.
- Attaque de type **«watering hole»** : le passage sur un site très fréquenté contamine l'appareil utilisé.

Si la majorité des attaques se font par spam, les failles applicatives seront très probablement exploitées à l'avenir.



AVIS D'EXPERT

CRYPTOLOCKERS
LES POINTS CLES DECHIFFRES

UNE FAMILLE DE PLUS EN PLUS DANGEREUSE

CryptoLocker, le grand frère éponyme qui fait des émules : il a infecté des dizaines de milliers de machines et généré des millions de dollars pour les criminels.

CryptoWall, le plus gourmand : il double souvent la demande de rançon si le paiement n'est pas effectué dans les temps.

TorLocker, le plus discret : il chiffre les données et utilise le réseau Tor pour effacer les traces de l'auteur.

SimpleLocker, le plus mobile : il s'agit d'une version déclinée spécialement pour Android.

CTB-Locker, le plus dangereux : il n'existe pas de solution de déchiffrement, les fichiers sont définitivement perdus à moins d'avoir une sauvegarde saine.

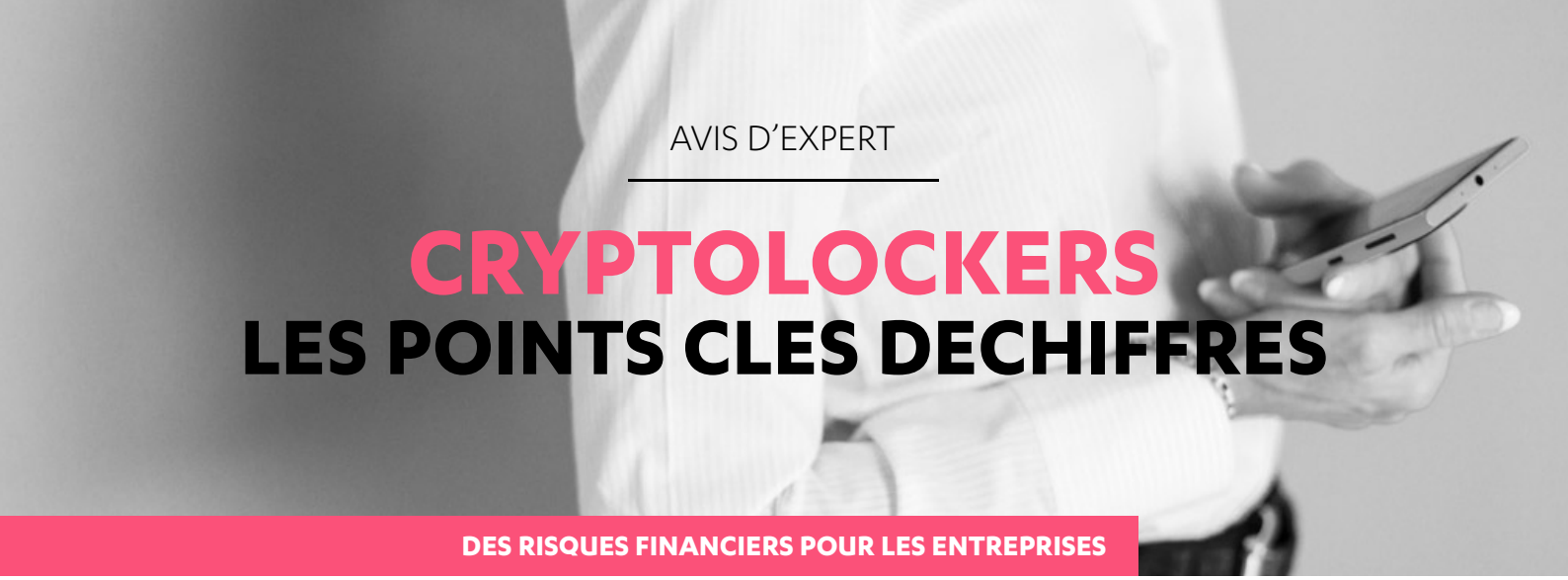
COMMENT PROCEDE CTB-LOCKER ?

L'utilisateur reçoit un email en français, a priori très bien écrit, **avec une pièce jointe** de type ZIP ou CAB. Le fichier archive contient un malware appelé **Dalexis** qui **télécharge** et **exécute CTB-Locker**. Si l'utilisateur ouvre l'archive et exécute son contenu, tous les fichiers des disques locaux et des partages seront chiffrés. CTB-Locker est un kit de malware développé pour opérer des **attaques multiples** : pour le moment le spam a été choisi comme vecteur d'attaque principal.

La sophistication de ces malware s'est généralisée avec des méthodes de chiffrement qui rendent la plupart du temps le déchiffrement impossible :

- La **combinaison des méthodes** RSA (chiffrement asymétrique) / AES (chiffrement symétrique) qui permet une grande vitesse de chiffrement de données, jusqu'à 256 bits à l'aide de l'algorithme AES, et qui chiffre ensuite la clé AES avec l'algorithme RSA.

- Les **algorithmes à courbes elliptiques**, qui procèdent à un chiffrement encore plus complexe et tout aussi rapide.



AVIS D'EXPERT

CRYPTOLOCKERS
LES POINTS CLES DECHIFFRES

DES RISQUES FINANCIERS POUR LES ENTREPRISES

LES COUTS DIRECTS

Puisque le principe de l'attaque est de demander de l'argent aux cibles, le premier risque est le coût de la rançon : **+ de 40% des victimes de cryptolockers auraient accepté de payer**. Si les demandes pour les particuliers oscillent entre 100 et 500 dollars, les montants demandés aux entreprises peuvent être beaucoup plus importants, jusqu'à 10 000 dollars. Les délais de paiement sont de 2 ou 3 jours et doivent s'effectuer par carte prépayée ou par bitcoins.
Passé ce délai, l'attaquant peut doubler la mise ou tout simplement supprimer la clé de déchiffrement. Certains cryptovirus utilisent des méthodes incitatives pour vous faire payer : crypter partiellement vos données pour vous faire croire que le pire est encore évité.

Dans tous les cas : Ne payez pas !

Et cela pour plusieurs raisons :

- L'attaquant n'a jamais eu l'intention de débloquer votre appareil.
- La clé de chiffrement risque de contenir des bugs.
- Le déchiffrement peut être provisoire : lorsque l'on a payé une fois , pourquoi pas deux ?

LES COUTS INDIRECTS

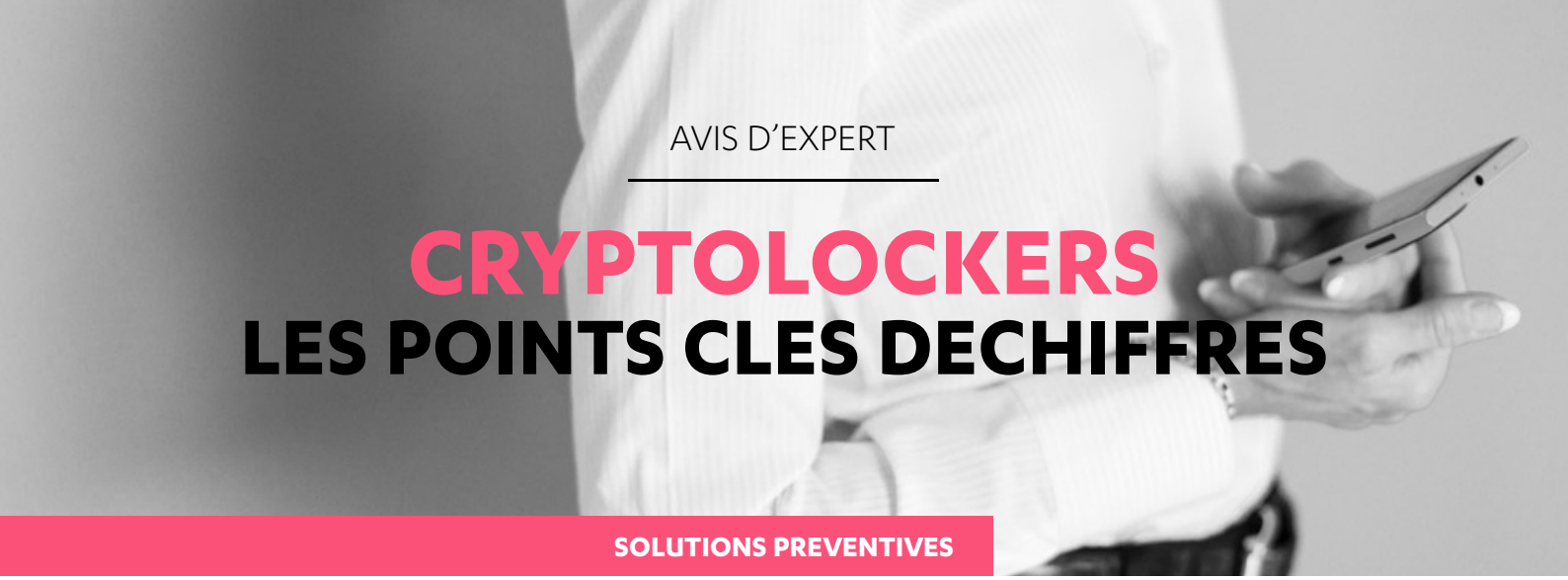
A la suite d'une attaque, l'entreprise doit s'attendre à faire face à :

- une **baisse de la productivité**,
- une **chute des ventes**,
- un **coût lié à la récupération** du système.

L'indisponibilité des données ou leur perte peuvent avoir de graves conséquences à plus long terme pour l'activité d'une entreprise et induire une baisse significative de chiffre d'affaires :

- **Perte de parts de marché :** les entreprises doivent être réactives, un simple ralentissement peut avoir un impact permanent.
- **Réputation ternie :** les données perdues peuvent impacter des particuliers ou des entreprises clientes qui perdront alors confiance vis-à-vis de l'organisation.
- **Développement ralenti :** ne plus avoir la main sur ses données de propriété intellectuelle ou industrielle représente un manque à gagner.

C'est l'existence même de l'organisation qui est en péril : si les données ne sont plus disponibles, comment maintenir l'activité ?



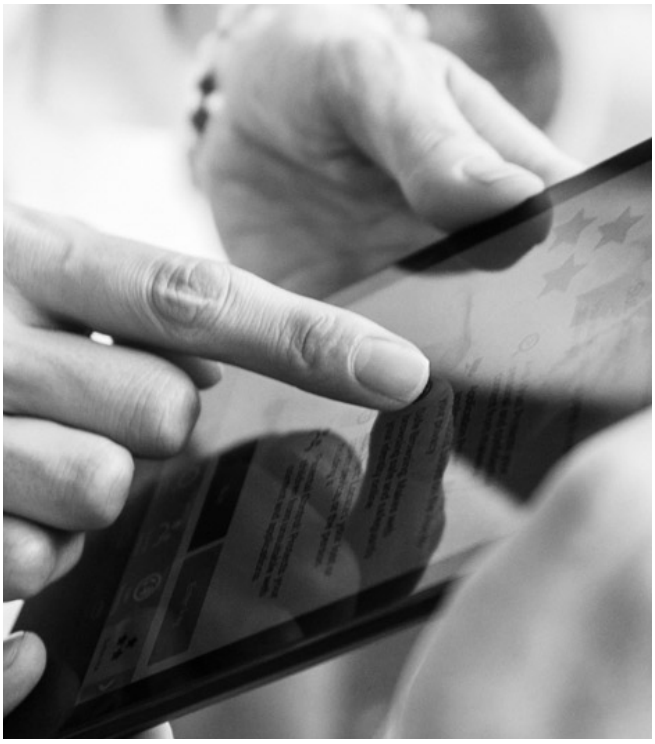
AVIS D'EXPERT

CRYPTOLOCKERS
LES POINTS CLES DECHIFFRES

SOLUTIONS PREVENTIVES

Les autorités prennent le sujet très au sérieux et recherchent activement les auteurs de ces cryptolockers. Mais en attendant le meilleur moyen est de **prévenir le danger et d'assurer ses défenses :**

- **Sensibilisez vos salariés** au risque de hameçonnage.
- **N'ouvrez jamais un lien dont vous ignorez l'origine**, d'autant plus s'il contient une pièce jointe ou un lien vers un site.
- Afin d'éviter l'ouverture de ces pièces jointes, **configurez vos solutions Antispam** pour supprimer les pièces jointes de type ZIP, CAB, SCR, TAR, GZ et plus globalement toutes les pièces jointes exécutables.
- **Etablissez une politique de sauvegarde**, sauvegardez régulièrement vos données sur un sous-système de sauvegarde hors ligne et vérifiez régulièrement la restauration de celles-ci.
- **Appliquez tous les patchs de sécurité critiques et importants** ou utilisez une solution de Patch Management, car demain les attaques pourraient se faire via des failles applicatives.



- **Bannissez XP, les applications Microsoft** et les applications tierces non supportées.
- Depuis Windows 7, la sécurité est renforcée avec **AppLocker et UAC : exploitez-les !**
- **Protégez tous vos appareils :** ordinateurs Windows et Mac, machines virtuelles et les appareils mobiles Android.
- **Votre antivirus et sa base de signatures doivent être à jour,** avec toutes les fonctionnalités de sécurité activées.
- Ne connectez pas vos partages en mode automatique ! **Restreignez leur accès en lecture seule.**

Comme nous l'avons vu, il est de plus en plus difficile de procéder au déchiffrement des données. Autrement dit, quand le mal est fait, il est souvent trop tard ! Le meilleur conseil que l'on puisse vous donner : protégez-vous et sensibilisez vos équipes en interne !