AfterWorkShop

de La Mêlée Adour

Les entreprises sous la menace des pirates

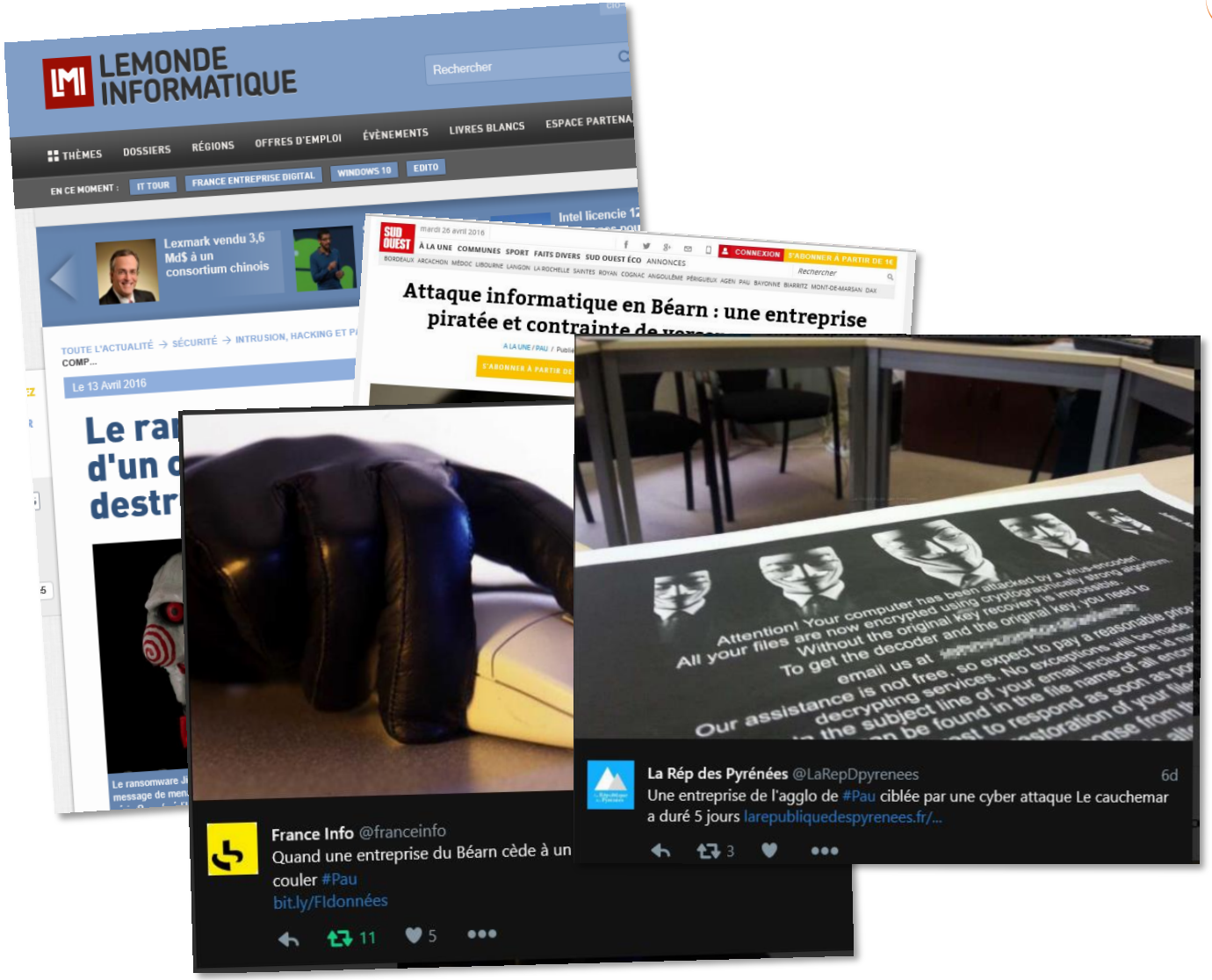
Crypto virus, ransomware, peut-on s'en protéger ?

Fin avril, la presse locale indiquait que des entreprises béarnaises ont été la cible de cyber attaques et avaient dû payer une rançon.

A la lumière de ces faits divers, il semble intéressant de revenir sur les bases de la sécurité informatique pour les entreprises.

Comment faire face à ces demandes de rançon?
Comment se protéger ?
Que faire une fois infecté ?
Faut-il obligatoirement payer les pirates ?
Existe-t-il des « Best Practices » ?

Fin avril 2016: la fiction rattrape la réalité dans les médias



Les premières questions

Ce type d'attaque marque les esprits parce qu'il met en évidence brutalement des choses que personne n'a vraiment envie d'entendre:

- La cible est une PME, une entreprise du coin, pas une obscure firme internationale ou un quelconque organe d'état
- Le dommage subit apparaît comme principalement financier
- L'entreprise attaquée avait elle vraiment d'autres choix?
- Comment cela se passerait il chez vous, dans votre entreprise?

Un peu de vocabulaire

- Chiffrage ou cryptage: c’est le fait de convertir en langage codé. Il faut avoir la clé pour pouvoir décrypter ou déchiffrer.

- TOR : c’est un réseau mondial qui permet de rendre anonyme son utilisation d’internet.

- BitCoin: c’est une crypto-monnaie qui permet de réaliser des paiements de manière « totalement » anonyme.

- Cookie: c’est un fichier texte qui rend notre navigation beaucoup plus conviviale et qui est régulièrement décrié comme portant atteinte à notre vie privée.

Un peu de vocabulaire

- Ransomware: catégorie de codes malveillants dont l'objectif est de vous empêcher d'utiliser vos ressources et/ou vos fichiers tant que vous n'avez pas payé une rançon.

- Malware ou Badware: c'est le nom générique donné aux programmes malveillants: virus, vers, cheval de Troie,…

- Spyware: c'est un petit logiciel installé à votre insu pour espionner votre activité en ligne (en vue de publicité ciblée)

Macro-chronologie

- 1989: 30 virus « in the wild » (aujourd'hui, plus de 8,5 millions)

- Avant les années 2000, les coûts matériels de l'informatiques et la faible interconnexion ont fait que le risque viral était pris très au sérieux par les entreprises (ex.: Jerusalem)

- Début des années 2000, la démocratisation de l'Internet a fait exploser les risques en particuliers avec « Melissa », « Sircam », « Code Red »,…

- Milieu de la décennie, l'ADSL aidant au risque viral traditionnel, il a fallu prendre en compte tous les nouveaux outils de marketing: les fameux spywares. Les pirates ont basculé dans la cybercriminalité organisée tant l'activité est lucrative.

- Depuis 2010, La monétisation du Net rend finalement très acceptable les logiciels espions. Le risque informatique n'étant plus destructeur, il est peu à peu banalisé et souvent ignoré. La question de savoir s'il est toujours utile d'avoir un antivirus est posée régulièrement sur les forums

- Aujourd'hui, les virus prennent en otage nos PME !

Le cas particulier des ransomwares

Les ransomwares existent depuis un moment sur la toile et touchent toutes les plateformes aujourd'hui: Android comme MacOS, Windows comme Linux.

Ils représentent une grandes familles qui va de la page un peu ridicule au code vraiment méchant, de l'utilisation de cartes prépayées aux crypto monnaies

1. Le « virus Gendarmerie »
2. Principe de fonctionnement d'un ransomware
3. Ce que peuvent faire ces ransomwares aujourd'hui
4. Quelques chiffres

Le « virus Gendarmerie »

Les ransomwares existent depuis un moment sur la toile et touchent toutes les plateformes aujourd'hui : Android comme MacOs, Windows comme Linux.

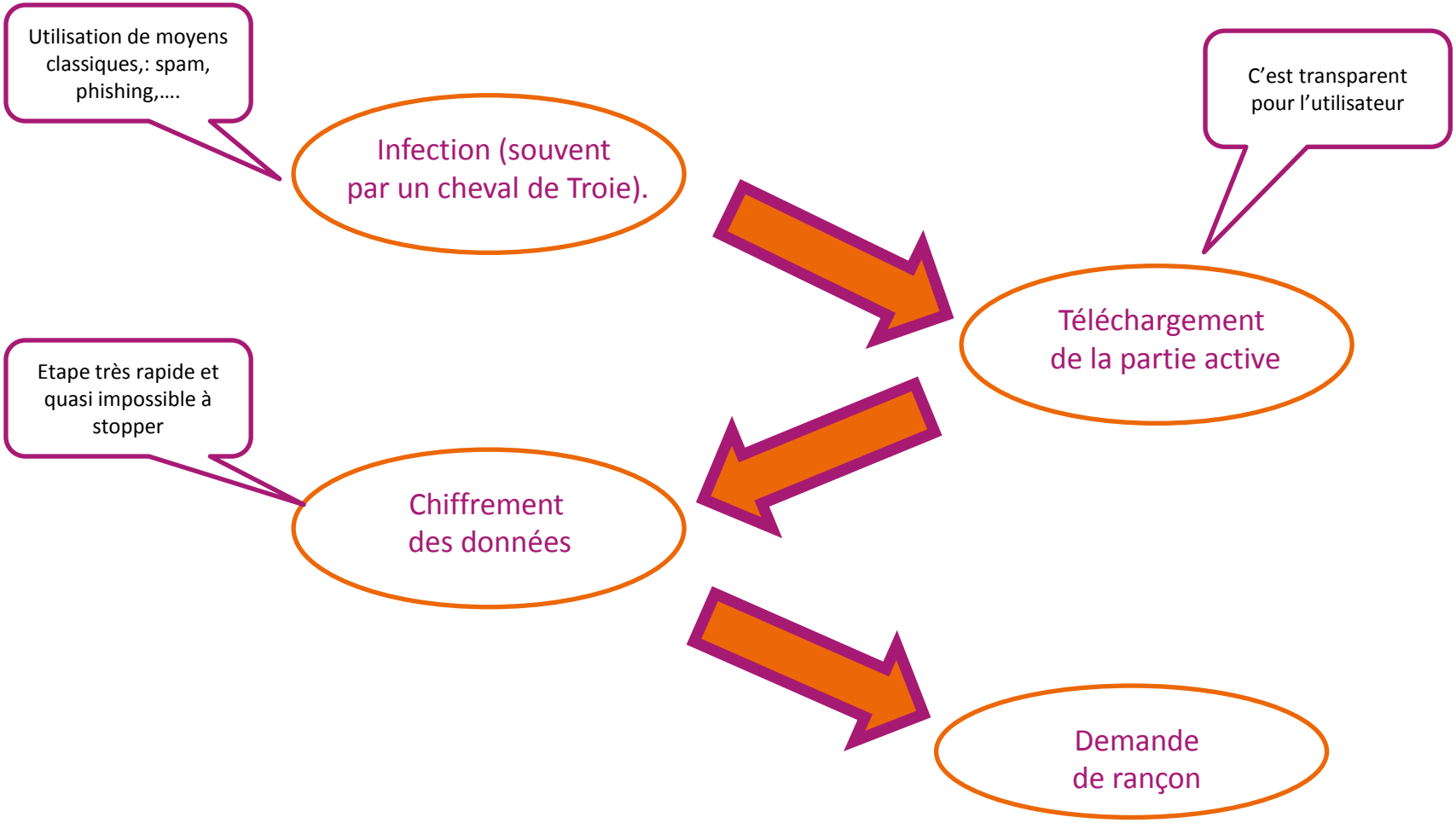
Le premier ransomware remarquable (et assez répandu) affichait une fenêtre de ce genre :

Source: forum de commentcamarche.com

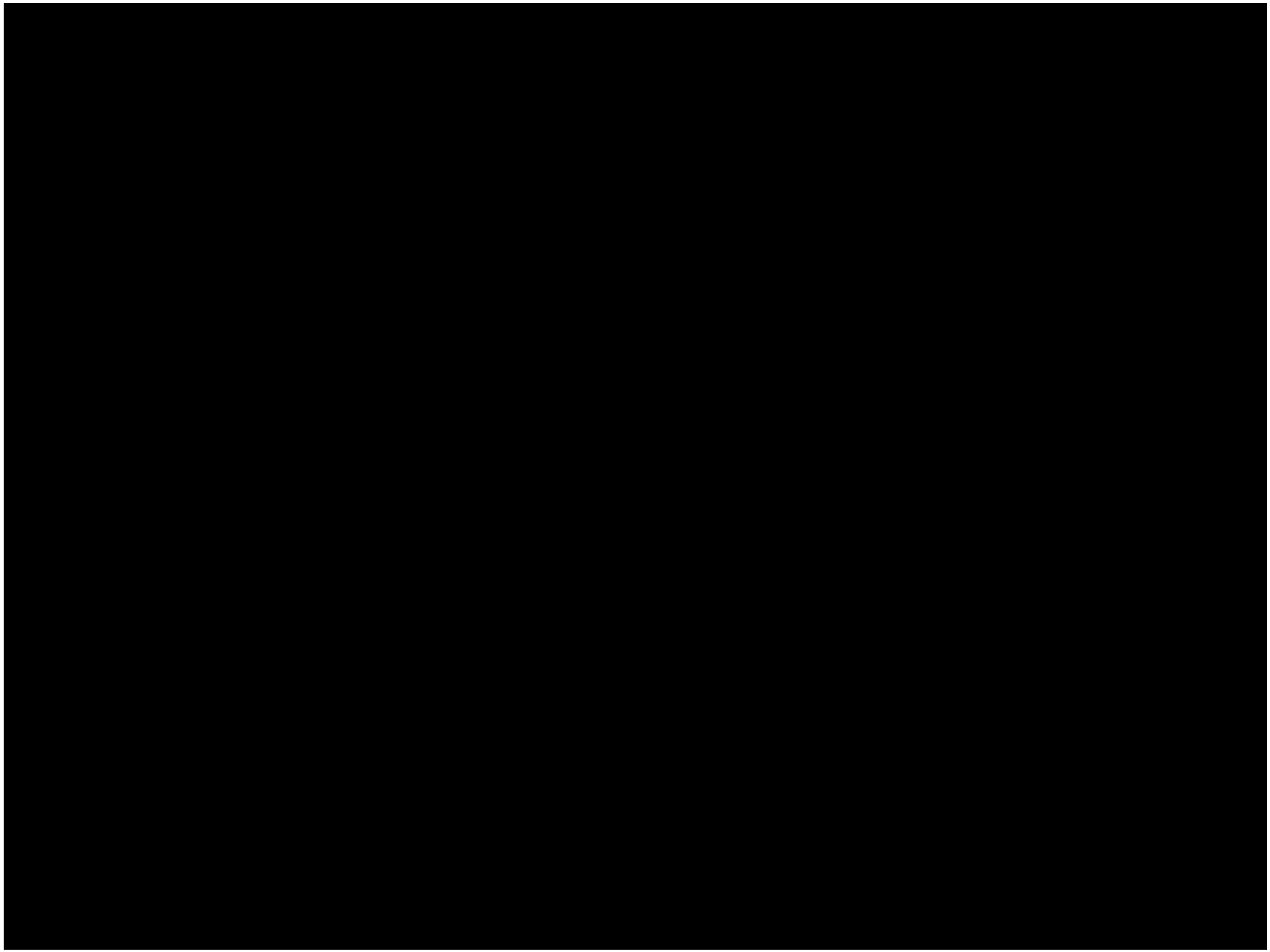
Ce type de rançonneur est assez simple à gérer et pourtant des entreprises ont payé… plusieurs fois…

Principe de fonctionnement d'un ransomware

Il s'agit d'un schéma simplifié pour faciliter la compréhension. La variété des cas est telle qu'il est difficile d'être exhaustif



Petite démo d’une infection: Vidéo Youtube de Malekal



Quelques explications

La vidéo étant sans bande son et surtout un peu technique, voici quelques explications pour mieux comprendre.
L'auteur de la démonstration (malekal.com) utilise une machine virtuelle et propose de voir l'impact d'un ransomware sur un dossier contenant des images dans des conditions quasi-réelles.

- Au préalable, il a reçu par mail un fichier zip (kl.zip)

- Au départ, nous avons 2 fenêtres ouvertes, le dossier contenant les images et un outil monitorant les processus exécutés par le système.

- Il fait ce qu'on fait tous avec un fichier zip, on regarde son contenu et on extrait un fichier contenant le script le fichier invoice_SCAN_46U3s.js

Quelques explications (suite…)

- En doublant cliquant sur ce fichier, l'UAC demande une confirmation avant d'exécuter le script.
- En cliquant sur OK, le script est exécuté
- Processus Explorer se ferme
- Les extensions des fichiers images changent (*.micro)
- La demande de rançon apparait (fenêtre bleu turquoise)

Vous pouvez noter que cela va très vite !!

Beaucoup d'autres explications sont disponibles sur le site malekal.com

Exemples de mails infectés

Source: securlist

FW: Payment ACCEPTED M-267689 - Message (Plain Text)

Message

Reply | Reply to All | Forward | Delete | Move to Folder | Other Actions | Junk E-mail | Categorize | Follow Up | Mark as Unread | Find

Respond | Actions | Options

From: Tracey Hoover [HooverTracey74635@pawluk.org] Sent: Wed 3/16/2016 2:46 AM
To: info
Cc:
Subject: FW: Payment ACCEPTED M-267689

Message | payment_document_267689.zip

```
Dear info,

Please check the payment confirmation attached to this email.
The Transaction should appear on your bank in 2 days.

Thank you.

Tracey Hoover
Financial CEO
```

Invoice 2016-74583971 - Message (Plain Text)

Message

Reply | Reply to All | Forward | Delete | Move to Folder | Other Actions | Block Sender | Safe Lists | Not Junk | Categorize | Follow Up | Mark as Unread | Find | Related | Select

Respond | Actions | Junk E-mail | Options | Find

From: Elbert Massey [MasseyElbert43716@hsi14.unitymediagroup.de] Sent: Wed 2/17/2016 10:58 AM
To: [redacted]
Cc:
Subject: Invoice 2016-74583971

Message | SCAN_INVOICE_2016_74583971.doc

```
Hi [redacted]

Here's invoice 2016-74583971 for 157,30 USD for last weeks delivery.

The amount outstanding of 490,34 USD is due on 23 Feb 2016.

If you have any questions, please let us know.

Thanks,
Elbert Massey
First Data Corporation  www.firstdata.com
```

Ce que peuvent faire ces ransomwares aujourd'hui

Nous l'avons vu sur la vidéo, les environnements Microsoft sont des cibles de choix. Ne croyez pas que Windows est moins sûr que les autres systèmes. Il est surtout beaucoup plus populaire et utilisé que les autres.

- Chez Apple, la dernière attaque découverte date de mars dernier avec un code infectant un programme légitime: lien *(paloaltonetworks.com)*

- Sur Androïd, le nombre de malwares expose depuis 2013 en exploitant les mêmes vecteurs que les micro ordinateur: lien *(welivesecurity.com)*. 17% des attaques visent des terminaux Androïd.

- Côté Linux, ce sont surtout les serveurs web qui sont menacés aujourd'hui en particulier en exploitant les failles des CMS les plus populaires : lien *(blog.kaspersky.fr)*

Ce que peuvent faire ces ransomwares aujourd'hui

Les experts prévoient une extension aux objets connectés, smart TV, etc…

En terme de dégâts, ils peuvent chiffrer vos documents, vos disques, s’attaquer aux partages réseaux, détruire vos fichiers,… y compris sur certains services Cloud.

Les rançons sont payables suivant les cas par cartes prépayées, BitCoin, mais aussi par cartes cadeaux Amazon.

Les ransomwares en chiffres

- Les ransomwares ciblent les pays occidentaux,
  → la France est dans le TOP 5 des pays visés

- En 2015, Kaspersky Lab. estime le nombre de victimes à plus de 750 000, soit une hausse de près de 50 %

- En moyenne la rançon serait de 300 $. Un hôpital américain a déboursé 17 000 $ en février dernier *(Forbes)*

- En 2015, 2 453 attaques auraient rapportés plus de 24 millions de dollars *(FBI Internet Crime Complaint Center)*

Les ransomwares en chiffres

- On trouverait des « tutos » en ligne pour 20 $ *(secureworks)*

- On peut trouver des kits complets pour faire son propre ransomware avec un manuel et une assistance gratuite pour 2 700 € *(Bitdefender)*

- Un seul ransomware peut rapporter près d'1 millions € par campagne

- Les campagnes sont teintées d'ingénierie sociale et sont ciblées :
  - ✓ Les abonnés Free,
  - ✓ Les hôpitaux,
  - ✓ Les écoles,
  - ✓ Les administrations, …

Quizz 1/3 Vrai ou faux?

- Les virus et autres malwares n'infectent que les PC

Tous les terminaux sont visés ainsi que les serveurs, mais aussi les systèmes industriels (et même les centrales nucléaires « Stuxnet »). La démonstration de la vulnérabilité des objets connectés a été faite des TV aux voitures en passant par les pacemakers

- les réseaux sociaux populaires sont sûrs

On ne compte plus les cas d'ingénierie sociale et de scams exploitant ces réseaux

- Les produits Apple ne sont pas visés par les pirates

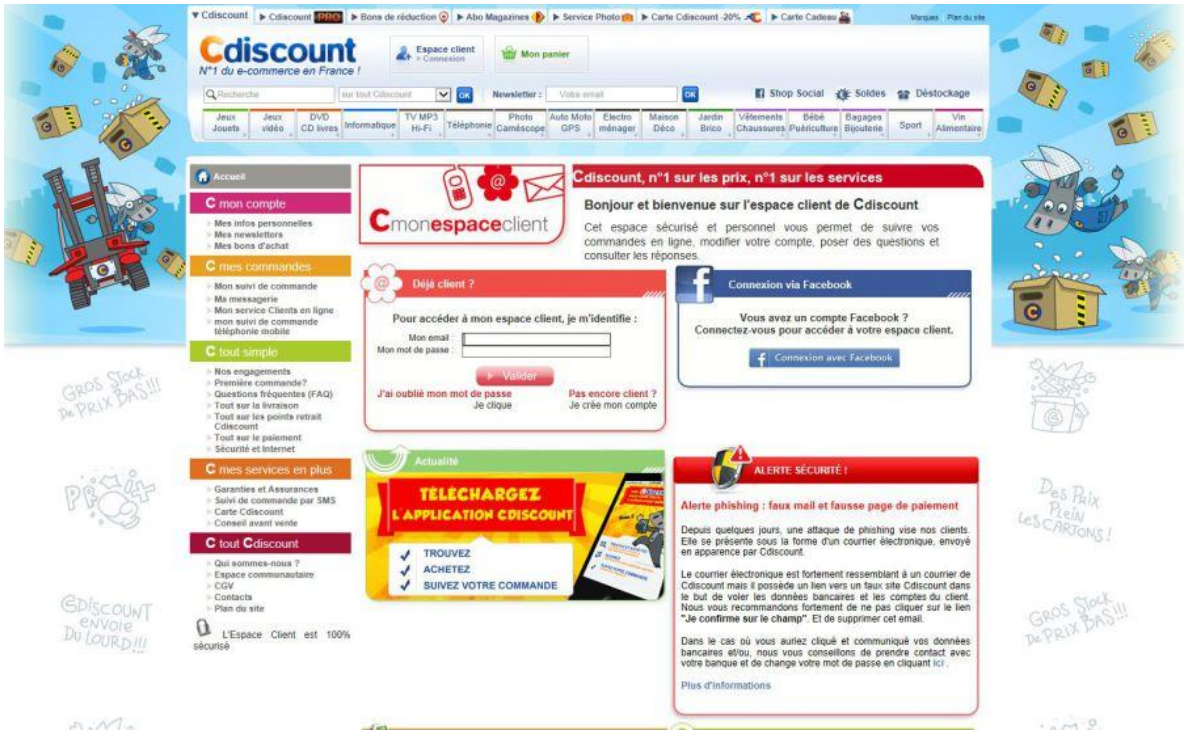
En Avril 2013, plus 600 000 Mac ont été infectés en une seule attaque

- Les antivirus gratuits sont suffisants pour protéger mes données.

A priori, je n'en sais rien ça dépend un peu de vos données.
Mais il vaut mieux avoir un antivirus gratuit et savoir s'en servir, que d'investir dans une solution payante et croire qu'elle va marcher toute seule

Quizz 2/3

➢Il est facile de reconnaître un site web contrefait : ils sont plein de coquilles reconnaissables.



C’est plutôt ressemblant et il y a même une alerte de sécurité

Quizz 3/3

- Je ne vais pas sur des sites douteux, je ne risque rien

Aujourd'hui, de nombreux sites et blogs sont compromis de façon « industrielle » et servent de relais aux pirates pour infecter des postes et lancer des attaques de masse.
Une autre menace est née avec la monétisation du web, l'explosion de la publicité en ligne a conduit les pirates à utiliser les régies publicitaires comme vecteur.
La notion de « site de confiance » est devenue discutable

- Je sais immédiatement si mon pc est infecté

Il existe bien des signes symptomatiques (mon PC « rame ») mais ils sont souvent un peu… tardif.
Les pirates cherchent à être le plus discret possible et la plupart des machines infectées ne sont que des cibles intermédiaires en prévisions d'attaques coordonnées plus importantes ou pour collecter des informations personnelles.
Pour un Cybercriminel, collecter des données est beaucoup plus rentable que de ralentir votre machine.

Comment cela se passerait il dans votre entreprise?

C’est la question légitime à se poser. Sommes nous capable de faire face à cette menace ? Très difficile de répondre même avec un audit… Mais cela ne veut pas dire que les entreprises sont sans défense et seront obligées de payer les demandes de rançon.

1. L’arsenal de protection des entreprises
2. L’individu est au centre de la sécurité
3. Quelques cas d’école
4. Le recours aux autorités
5. Quelques conseils

L’arsenal de protection des entreprises

Malgré l’évolution et la multiplication des risques, l’entreprise a toujours au moins 2 moyens de protection qui ont fait leurs preuves :

- L’antivirus pour anticiper sur les soucis
- La sauvegarde pour redémarrer en cas de sinistre

Il existe de nombreux autres dispositifs de sécurité (Firewall, chiffrement, IDS, sondes, ….) mais maitriser son antivirus et sa sauvegarde, c’est déjà beaucoup.

Les pirates exploitent le plus souvent des failles techniques non corrigées

Il est important d’appliquer les correctifs fournis par les éditeurs, en particulier:

- Les mises à jour « système »
- Les correctif applicatifs (Acrobat, Flash, Office, navigateurs web,…)
- Les CMS, leurs extensions, thèmes

L'antivirus

C'est l'outil qui va essayer de bloquer notamment le cheval de Troie ou le téléchargement du ransomware.

C'est un équipement indispensable :

- il doit être installé sur tous vos terminaux et serveurs
- il doit être mis à jour régulièrement
- il doit être correctement paramétré
- chacun doit savoir s'en servir
- son fonctionnement doit être contrôlé régulièrement

Gratuit ou payant?

Mon avis personnel: il me semble difficile de prétendre garantir le même niveau de service quand il est gratuit.

Attention, vérifier que votre version gratuite est bien utilisable dans un cadre professionnel = <u>risque juridique</u>

La sauvegarde

Il y a beaucoup de bruits autour des sauvegardes, il y a beaucoup de solutions « miracles » proposées et il faut revenir aux fondamentaux:

Une sauvegarde est un dispositif qui permet de se protéger contre le risque de perte de données suite à un sinistre (panne, vol, incendie,…)

- Ce n'est pas une archive, mais un élément possédant un cycle de vie complet
- Les supports de sauvegarde ne doivent pas rester au même endroit que les données sauvegardée
- En cas de sauvegardes « réseaux », les connexions doivent être chiffrées et non permanentes
- Pour avoir des sauvegardes efficaces, il faut impérativement:
  - ✓S'assurer de son bon fonctionnement au jour le jour
  - ✓S'assurer que l'on est en capacité de réaliser une restauration
- Multiplier les copies de données est mieux que rien mais attention au risque juridique

Certaines entreprises auditent la stratégie de sauvegarde de leurs sous-traitants

L’individu est au centre de la sécurité

L’individu a rôle important à jouer dans la protection du « patrimoine informationnel » en particulier parce qu’il est le maillon faible.

- un premier lieu en tant qu’utilisateur des ressources de l’entreprise :
  - ✓ il doit accepter l’idée qu’il ne peut pas tout faire sur son poste de travail
  - ✓ il doit connaître des actes techniques de base sur l’utilisation de son antivirus pour vérifier un fichier ou une clé USB
  - ✓ il doit avoir accès au strict minimum de données

La sécurité informatique est comme la sécurité routière ou incendie: **c’est l’affaire de tous !**

L'individu est au centre de la sécurité

- Mais aussi personnellement en tant qu'individu :

  - ✓ Il doit communiquer sur tous les événements suspects rencontrés
  - ✓ Il doit s'interroger sur la légitimité des mails qu'il reçoit
  - ✓ En cas d'imprudence, il faut alerter du risque de compromission *(sic)*
  - ✓ Il doit comprendre que sur Internet (comme ailleurs) il faut se méfier de se qui est trop beau

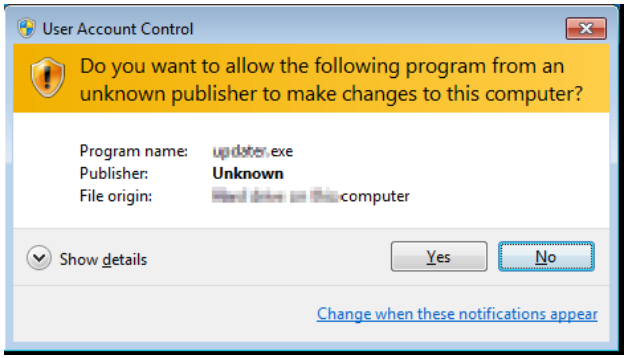
La sécurité informatique est comme la sécurité routière ou incendie: **c'est l'affaire de tous !**

Quelques cas d'école 1/4

- vous recevez un mail avec une PJ douteuse
  - ✓ vous contrôlez la PJ avec votre anti-virus (à jour) ou avec un service en ligne
  - ✓ vous en parlez autour de vous
  - ✓ **Vous ne l'ouvrez pas pour voir ce que ça fait**

Quelques cas d'école 2/4

- En ouvrant un document bureautique ou une archive, la fenêtre suivante s'affiche:



- ✓ vous cliquez sur **No** parce que ce n'est pas habituel
- ✓ vous recherchez d'où vient ce fichier
- ✓ vous en parlez autour de vous
- ✓ vous n'oubliez pas de supprimer ce fichier

Evitez de désactiver l'UAC : c'est un très bon signal d'alarme !

Quelques cas d'école 3/4

➢ Malgré toutes vos précautions, un poste est infecté, les données sont cryptées et une demande de rançon s'affiche

- ✓ vous isolez le poste du reste de votre réseau et d'Internet
- ✓ vous réinstallez votre poste « from scratch »
- ✓ vous restaurez les données depuis votre dernière sauvegarde valide

Ne cherchez pas de trucs ou astuces sur Internet,
vous ne feriez qu'alourdir la facture !

Lorsque vos données sont cryptées, il faut considérer l'incident comme un sinistre.
A l'instar d'un incendie, repartir de la sauvegarde est la méthode la plus rapide et la plus fiable.

✓Pour les bidouilleurs optimistes et les entreprises sans sauvegarde, on peut tenter

- ❖ l'utilisation de « VSS » (sans garantie que les clichés ne soient pas également corrompus)
- ❖ l'utilisation de logiciels type Photorec (permet de recouvrer parfois des fichiers effacés)

Quelques cas d'école 4/4

- Si vous payez la rançon, il sera indispensable de:

  - ✓ faire des copies des données recouvrées avec la clé fournie par le pirates
  - ✓ réinstaller l'ensemble des machines qui ont pu être compromises
  - ✓ revoir votre politique de sauvegarde
  - ✓ revoir votre politique antivirus
  - ✓ changer tous vos mots de passe

Le danger serait de croire que le paiement effectué, vous pouvez reprendre votre vie comme avant.

En payant le pirate, vous retrouvez (au mieux) l'accès à vos données, votre informatique reste toujours compromise et vous risquez d'être à nouveau rançonné dans quelques semaines

Le recours aux autorités

Vous pouvez déposer une plainte en cas de cybercriminalité auprès de votre commissariat de Police, brigade de Gendarmerie ou du Procureur de la République

Sous-direction de Lutte contre la Cybercriminalité (SDLC)
SDLC/OCLCTIC
101, rue des 3 Fontanots
92 000 Nanterre
Tél. : 01 47 44 97 55
Site Internet
Services de signalements en ligne de contenus illégaux sur l'Internet
Plateforme téléphonique « Info-escroqueries » : 0811 02 02 17

Centre de lutte contre les criminalités numériques (C3N) du Service Central du Renseignement Criminel (SCRC) de la gendarmerie nationale
SCRC/C3N
5, Boulevard de l'Hautil – TSA 36810
95037 CERGY PONTOISE CEDEX
Tél. : 01 78 47 36 52
contact : cyber@gendarmerie.interieur.gouv.fr

Quelques conseils …

- En cas d'attaque, il est indispensable de trouver de comprendre comment vous avez été touché.

- La communication interne est important pour maintenir une certaine vigilance

- Quand une machine est compromise, il ne faut pas faire de détails et la réinstaller intégralement .C'est comme une panne ou un vol

- Avoir des sauvegardes sans être certains de pouvoir les restaurer ne sert à rien

- Savoir reconnaître les messages légitimes du système et de l'anti-virus permet d'éviter beaucoup de piège

- Il faut faire toutes les mises à jour proposées par les éditeurs au plus tôt

- Si vous ne savez plus quoi faire, fermer avec la croix ou avec le gestionnaire de tâches

Tous les analystes sont d'accord, les ransomwares sont trop rentables pour être un simple épisode.
Il faut apprendre à vivre avec cette menace.

AfterWorkShop

de La Mêlée Adour

N’hésitez pas à nous faire des propositions de sujets !

Merci de votre attention

Contact:

pascal@pwojciec.info @borbhal

Le blog de la commission SI et sécurité

borbhal.org