LAVI

Cybercriminalité: préservation des preuves et prévention

Romain Roubaty, 6 septembre 2018

Infractions informatiques

Soustraction de données

Accès indu à un système informatique

Détérioration de données

Portrait du cyberdélinquant

Motivations

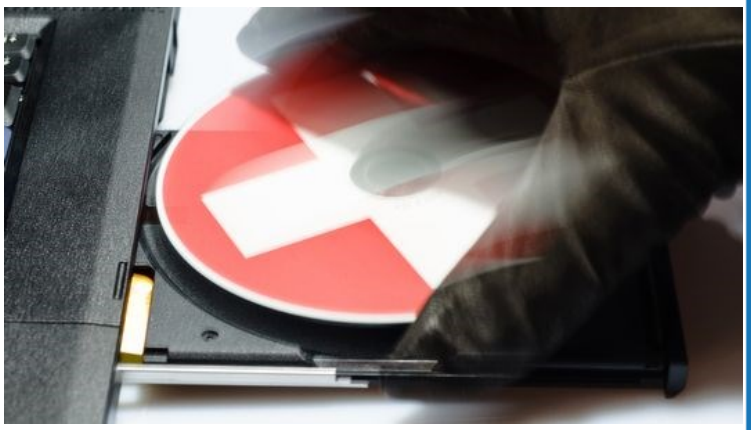
- Sociale
  - Besoin de reconnaissance (immaturité), Vengeance
- Technique
  - Limite de la technologie
- Politique
  - Forcer une prise de conscience, Idéologie, Terrorisme
- Financière
  - Cupidité, Terrorisme
- Gouvernementale
  - Caractère stratégique, Idéologie

Soustraction de données

Illustration

Vols de données bancaires

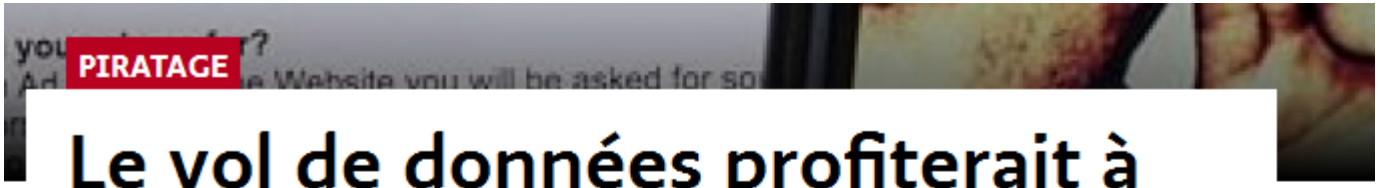
SR Suisse



[Christian Loose - Fotolia]

[Martin Ruetschi - Keystone]

Ashley Madison



Le vol de données profiterait à Ashley Madison

La société canadienne Avid Life Media, propriétaire du site de rencontres extraconjugales, dit n'avoir jamais enregistré autant de nouveaux membres depuis le piratage spectaculaire et la publication de sa base de données utilisateurs

Vol de données

Le **vol de données** clients d'Orange révèle une menace
7 mai 2014 ... *Données* personnelles : Contraint à la transparence sur le *vol* de ses *données* clients, Orange figure parmi les

Vol de données : attention aux salariés mécontents -
20 juin 2012 ... Toute l'actualité Sécurité *Vol de données* : attention aux sala... Le coût moyen d'une violation de données

800 000 clients touchés par un **vol de données** chez
3 févr. 2014 ... Intrusion, Hacking et Pare-feu : En fin de semaine dernière, l'opérateur a informé certaines personnes d'une intrusion

Les hôtels Hilton victimes d'un **vol** massif de **données**
25 nov. 2015 ... Après les hôtels Starwood, c'est au tour du groupe Hilton d'avouer le *vol* de *données* de cartes bancaires de

La base de **données** du service RH du gouvernement
22 juin 2015 ... Intrusion, Hacking et Pare-feu : Après le *vol* début juin de plus de 4 millions de *données* d'employés fédéraux aux

Les **données** privées de 22 175 employés du FBI
9 févr. 2016 ... Alors que pour le précédent hack de données personnelles des ... Mark Giuliano, le *vol de données* opéré par le mystérieux DotGovs a été ...
www.lemondeinformatique.fr/.../lire-les-**donnees**-privees-de-22-175- employes-du-fbi-piratees-63860.html

Vol de données

06 OCTOBRE 2016 / SÉCURITÉ

Un sous-traitant de la NSA arrêté pour vol de données classifiées

Le FBI a arrêté un consultant du gouvernement américain. L'homme, originaire du Maryland, est accusé d'avoir volé des documents administratifs, dont des informations

19 OCTOBRE 2016 / SÉCURITÉ

6 000 sites web Magento visés par des vols de données bancaires

Les attaques ciblant les boutiques en ligne pour voler les données des cartes de paiement des clients se multiplient et sont de plus en plus sophistiquées. La dernière technique consiste à cacher le...

19 AOUT 2016 / DONNÉES PERSONNELLES

Eddie Bauer, HEI Hotels touchés par un vol de données clients

Après l'intrusion subie par Oracle dans sa division Micros, spécialisée sur les terminaux point de vente, il est apparu que plusieurs autres fournisseurs de TPV avaient été infiltrés ces derniers...

Vol de données

27 JUIN 2016 / SÉCURITÉ

Des chercheurs volent des données en utilisant le bruit des ventilateurs d'un PC

Créé par des chercheurs en sécurité israéliens, le malware Fansmitter exploite les ventilateurs d'un ordinateur pour transmettre des données.

10 JUIN 2016 / DONNÉES PERSONNELLES

Twitter ferme des comptes suite au possible vol de ses données

Suite aux dizaines de millions d'utilisateurs potentiellement touchés par le vol de leurs identifiants, Twitter a pris la décision de fermer certains comptes qui auraient piratés directement sur les...

14 NOVEMBRE 2016 / INTRUSION, HACKING ET PARE-FEU

Piratage FriendFinder Networks : 412M de comptes exposés

Le groupe FriendFinder Network, comprenant notamment le site de rencontre adultfriendfinder.com, a été victime d'un nouveau piratage. Plus de 412 millions de comptes utilisateurs sont exposés à du...

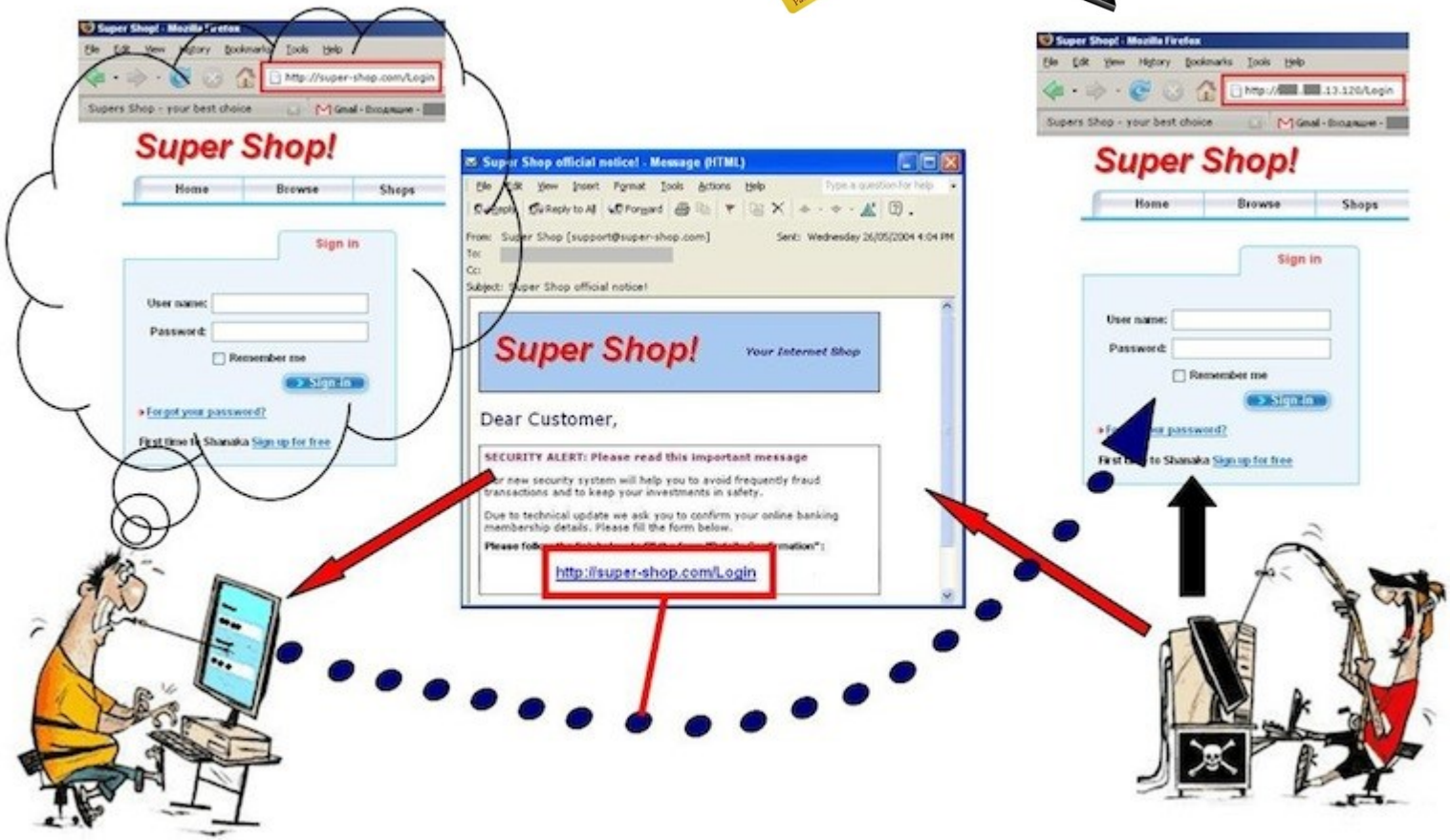
Spyware (logiciel espion)

Spywares commerciaux

Mouchards

Hack Academy

Phishing (hameçonnage)



Phishing (hameçonnage)

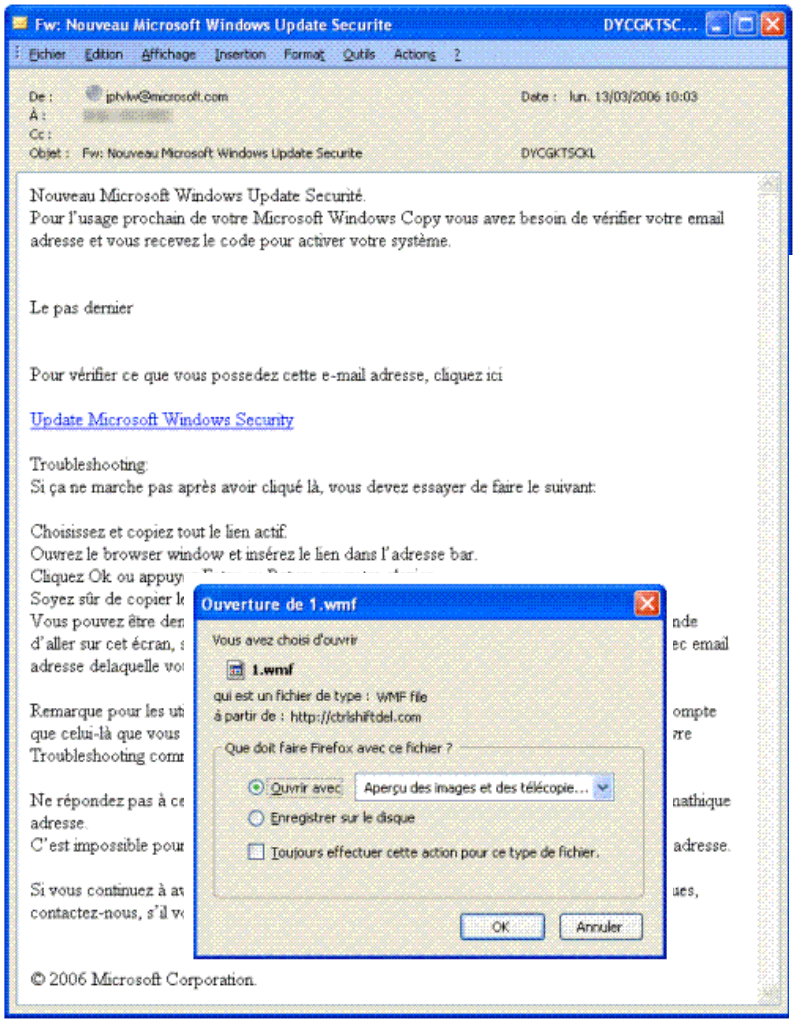
Dear PostFinance Customer

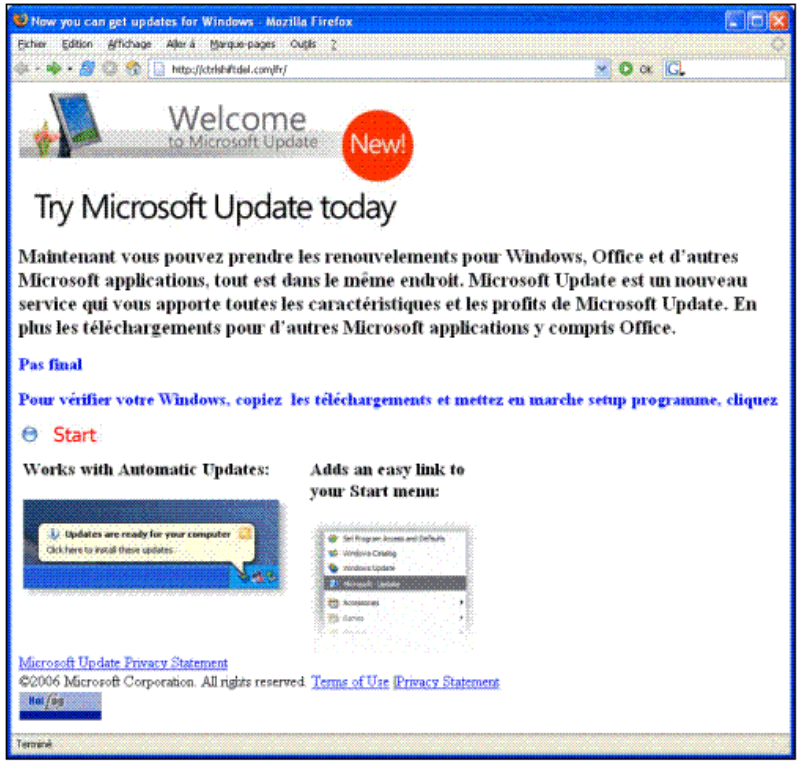
This email was sent by the Post Finance server to verify your e-mail address. You must complete this process by clicking on the link below and entering in the small window your Post Finance online access details. This is done for your protection - because some of our members no longer have access to their e-mail addresses and we must verify it.

To verify your e-mail address, click on the link below:

http://www.postfinance.ch/Jh0XH7MHiHaT1eY1OWqnvBZvKpNsWl2nnJwnXYwIOfOjg4QeWi7z0yum4fs02ut

Phishing (hameçonnage)





Phishing (hameçonnage)

Hallo lieber Kunde,
der Zustelltermin für Ihr Paket hat sich auf Dienstag, 14:00-19:00 Uhr geändert.

Klicken Sie dazu einfach auf den folgenden Link, der Sie zum Sendungsinformat
http://elsisart.com/qjsls283528mk/
Cliquez ou appuyez pour suivre le lien.
https://nolb.dhl.ch/ne
time=202501&report=JavaScript&email=Romain.Roubaty@he-arc.ch. (JavaScript Report)

Bitte beachten Sie, dass es einige Stunden dauern kann, bis die Informationen zu Ihrem Paket zur Verfügung stehen.

Patri
[ca] {S
Grou

Serç
[ca] {Spam?} Votre adh&#xfffd;sion &#xfffd; l'AFSIN mar. 04.04
Groupes AFSIN

DHL.ch
Ihr DHL Paket kommt am Dienstag, 14:00-19:00 Uhr. **mar. 04.04**
HallolieberKunde,

MSAB
Taking mobile forensics to the next level. mar. 04.04
Taking mobile forensics to the next level. View this email in your browser The new XAMN Spotlight 2.0 – Get your

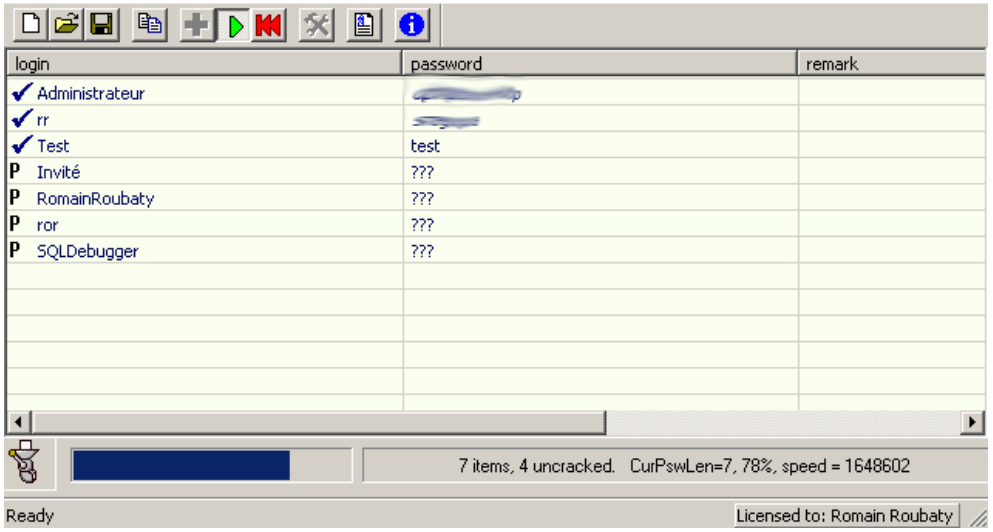
Accès indu à un système informatique

Usurpation de mots de passe

Un leurre énorme mais qui fonctionne

- E-mail
- Téléphone

Outils



Usurpation de mots de passe

Message De: Stephane Dolt <stephane.dolt@hews.ch>

Fichier Éditer Afficher Opérations Outils Fenêtre Aide PGP

Fermer Répondre Faire suiv

Message | Propriétés | Personnaliser

De : Stephane Dolt <stephane.dolt@hews.ch>
Vers : <romain.roubaty@hevs.ch>
Objet : probl*me technique

Salut

Je dois faire une mise * jour pour un de nos serveurs.
Il faut que tu me donnes le mot de passe de ta zone FTP par retour de mail.
C'est urgent, merci

St*phane

Usurpation de mots de passe

Failles techniques

LE 22 FÉVRIER 2017 / SÉCURITÉ

Microsoft corrige en urgence une faille du lecteur Flash d'Adobe

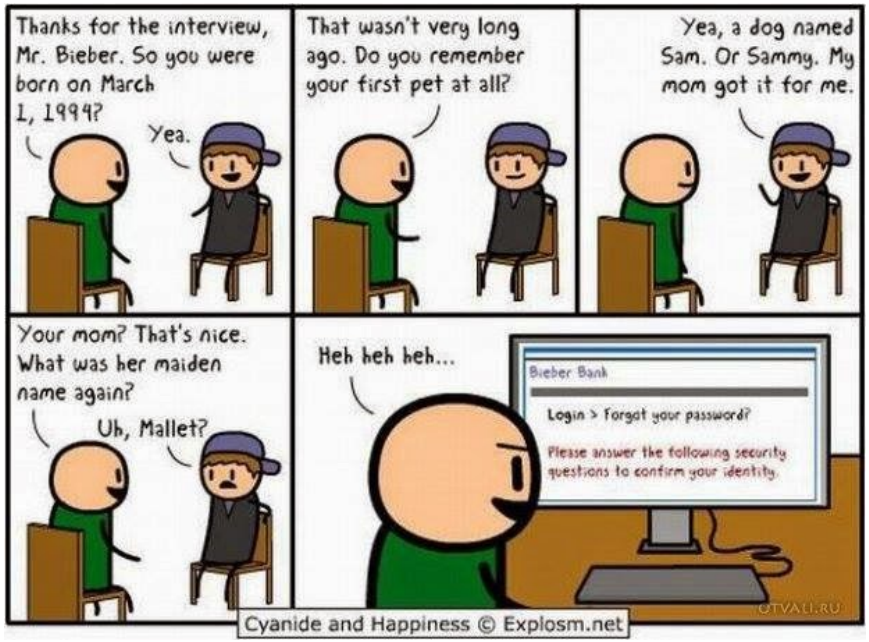
Microsoft a annoncé la disponibilité d'un correctif pour le lecteur Flash d'Adobe installé notamment sur Windows 10 et Windows Server 2016. La publication du patch tuesday a par...

LE 22 FÉVRIER 2017 / INTRUSION, HACKING ET PARE-FEU

Les clients FTP Java et Python, trappes à vulnérabilités XXE

Le chercheur en sécurité Alexander Klink a découvert que des pirates pourraient tromper les applications Java et Python pour exécuter des commandes FTP et ouvrir des ports dans...

Social Engineering / Ingénierie sociale



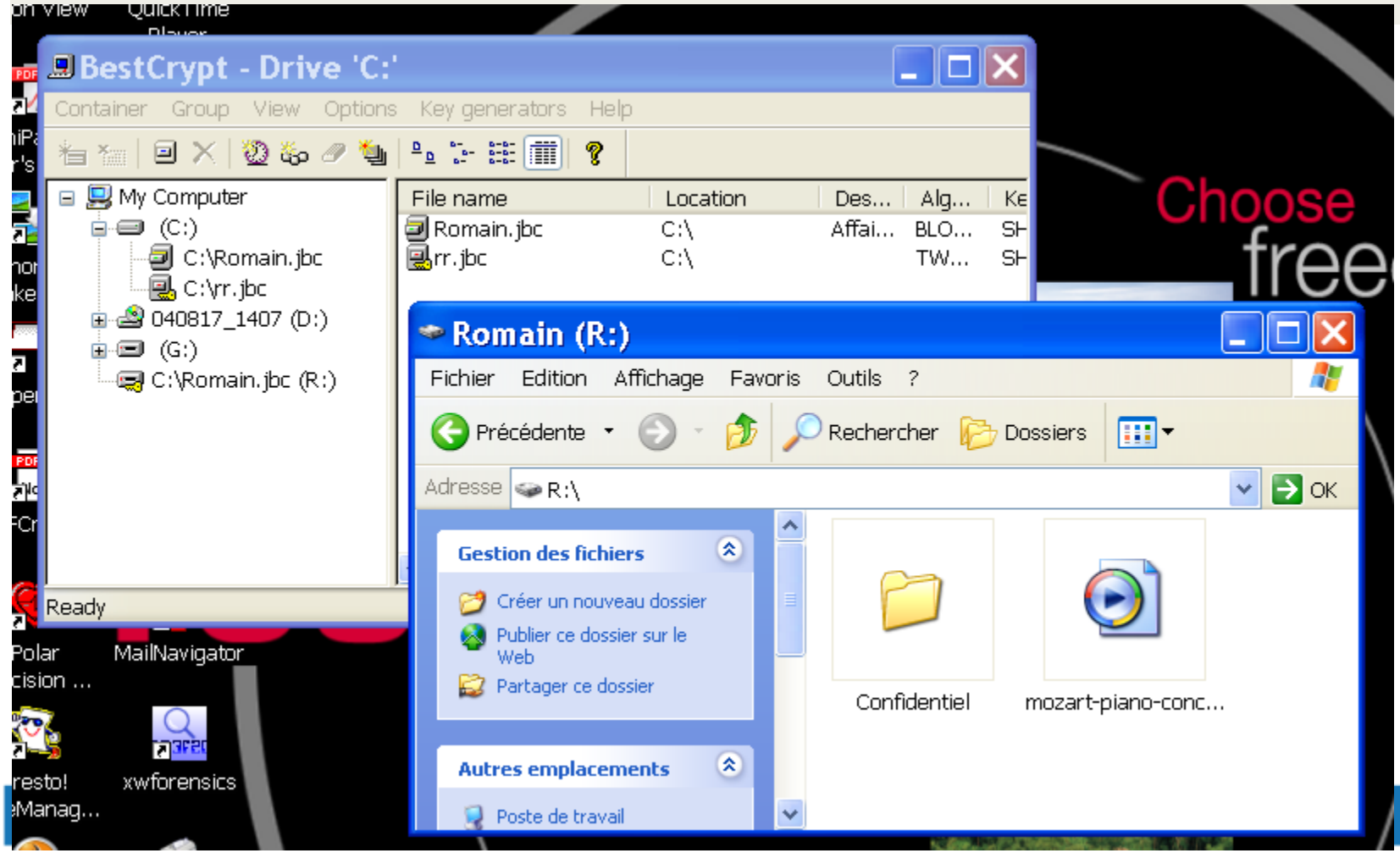
Plus d'un million !

15 fév. 2017 LA CHAUX-DE-FONDS - Une entreprise victime d'une escroquerie informatique.

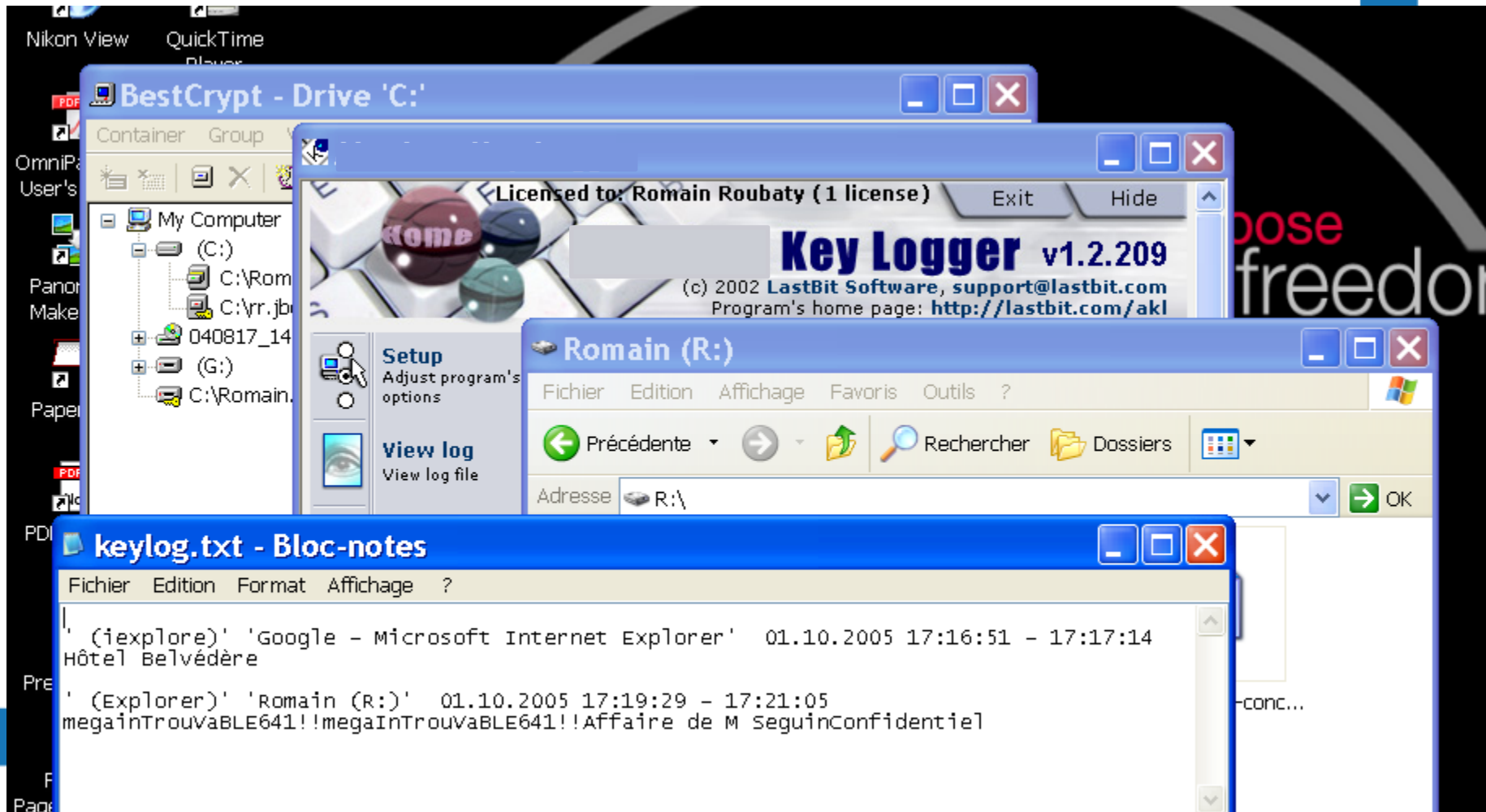
«Nous sommes très bien protégés sur le plan informatique. La faille est clairement humaine. Peut-être qu'en Suisse, on reste un peu trop naïf...»

Hack Academy

Renifleur de clavier



Renifleur de clavier



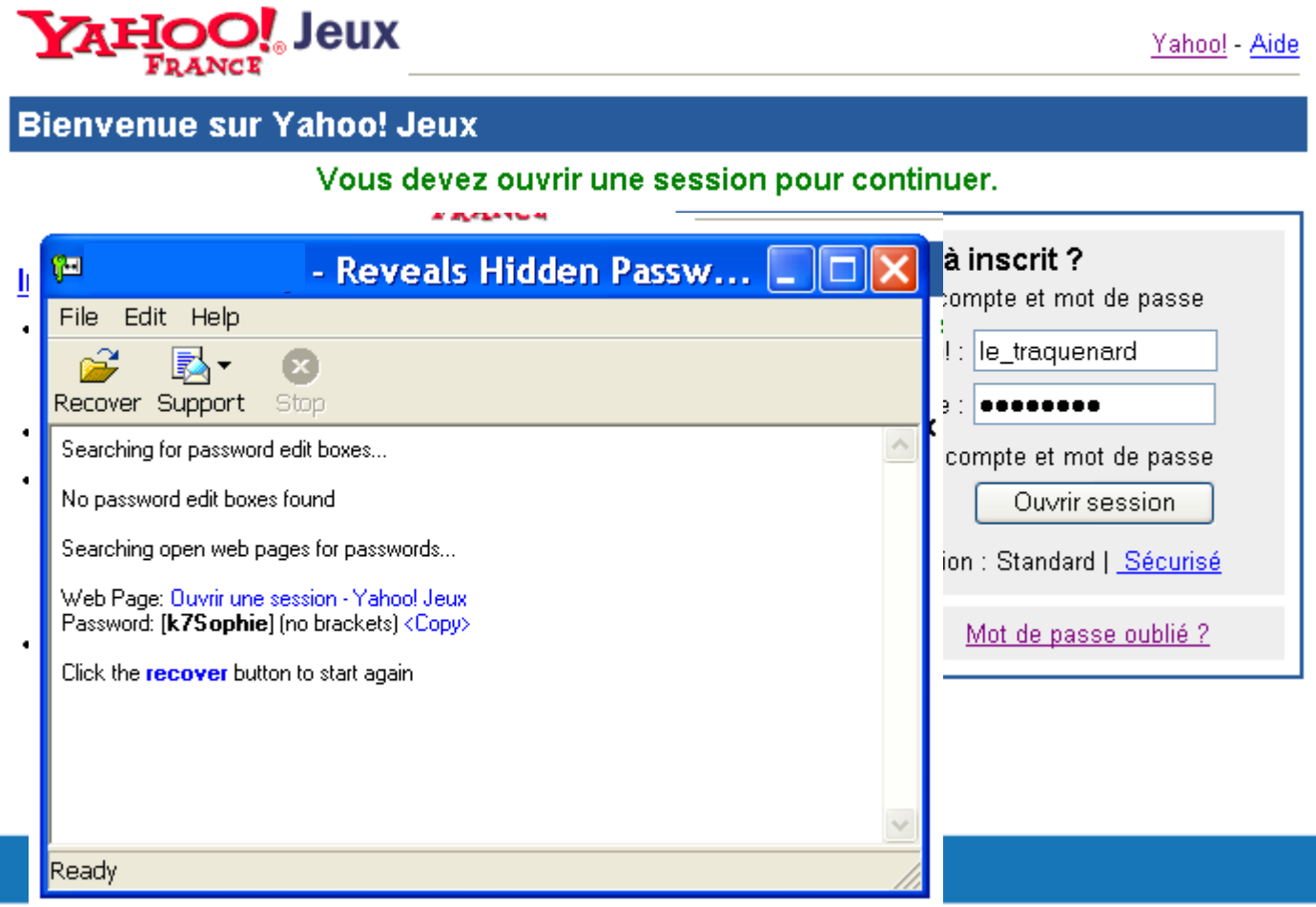
cinc - centre d'investigation numérique et de cryptologie

ILCE Institut de lutte contre la criminalité économique

Certifié ISO 9001

L'espion

Le démasquage



DOS Denial of service attack

Rendre indisponible un service

Botnets

Réseau d'agents logiciels qui suivent les instructions d'un serveur

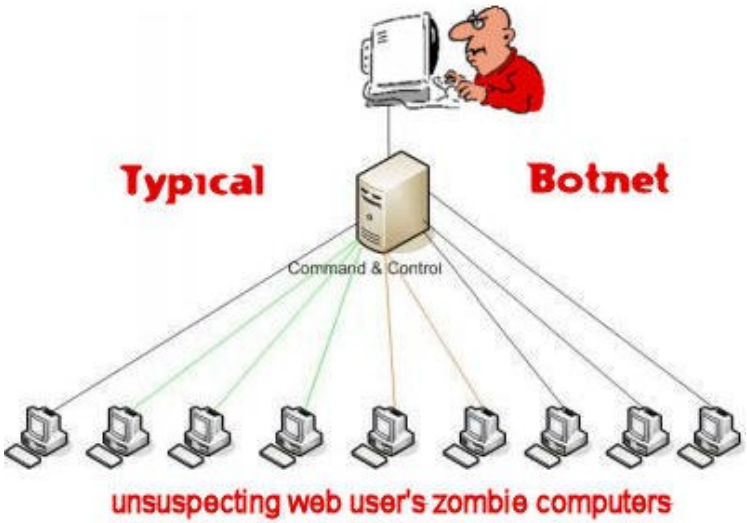
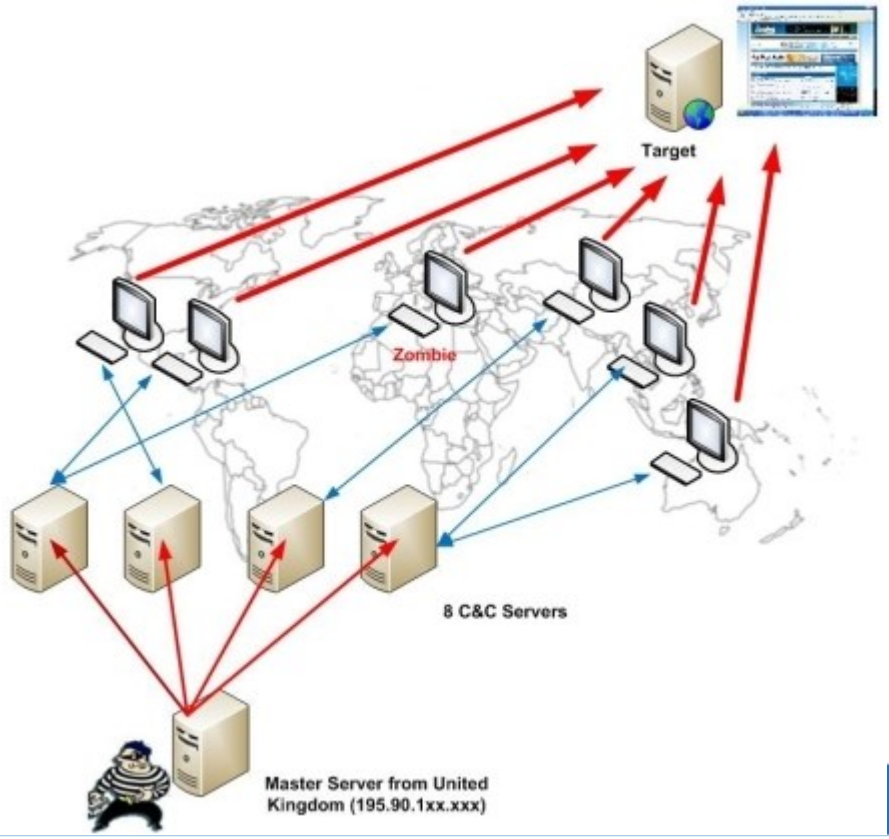


Schéma d'une attaque DDOS (Distribued Denial of Service)

Attaque via un réseau de zombies



Botnet

Un Britannique de 29 ans soupçonné d'être à l'origine du botnet qui a perturbé les routeurs d'un million de clients Deutsche Telekom en novembre 2016 a été arrêté à Londres. Le suspect pourrait écoper de 6 mois à 10 ans d'emprisonnement.

Un britannique de 29 ans serait à l'origine du mallware Mirai qui a bloqué les routeurs de plus d'un million de clients Deutsche Telekom en novembre 2016. CRédit: D.R.

Malware Mirai

Le Liberia a été victime d'une violente attaque DDoS qui a provoqué des coupures d'accès dans tout le pays et rendu les sites internet locaux inaccessibles. Réalisée grâce au malware Mirai impliqué dans la défaillance du prestataire DNS Dyn aux Etats-Unis le mois dernier, cette attaque a eu des conséquences désastreux sur l'économie de ce pays d'Afrique de l'Ouest.

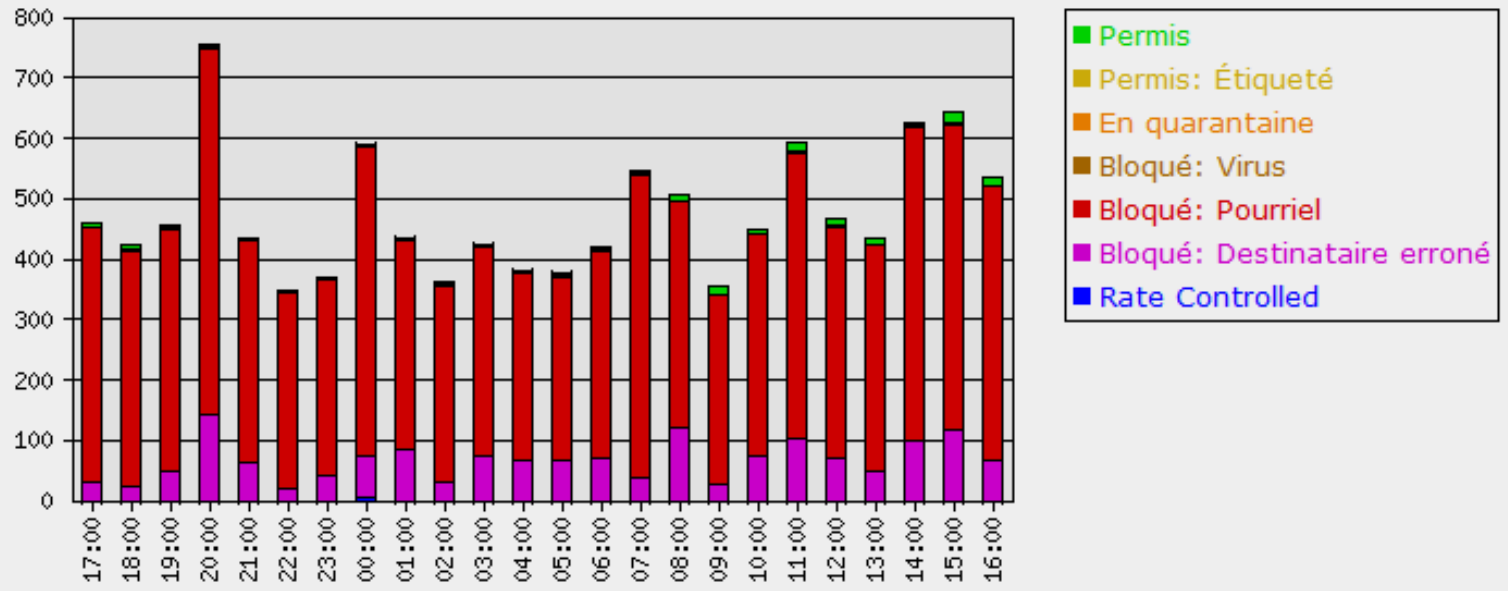
Le Liberia a été victime d'une attaque par déni de service du même type que celle lancée par le botnet Mirai qui a bloqué les serveurs DNS de l'entreprise Dyn aux Etats-Unis. Crédit : D.R.

Le chercheur renommé en sécurité Brian Krebs a mené une enquête de longue haleine pour tenter de découvrir l'auteur qui se cache derrière le pseudonyme Anna-Senpai à l'origine du malware Mirai. Ce dernier a été utilisé pour créer des botnets ayant permis de mener des attaques DDoS de grande ampleur.

Le chercheur en sécurité Brian Krebs a mené des investigations pour découvrir l'identité de l'auteur du malware Mirai qui serait Jha Paras (en photo), président de ProTraf Solutions spécialisé dans les solutions anti-DDoS. (crédit : D.R.)

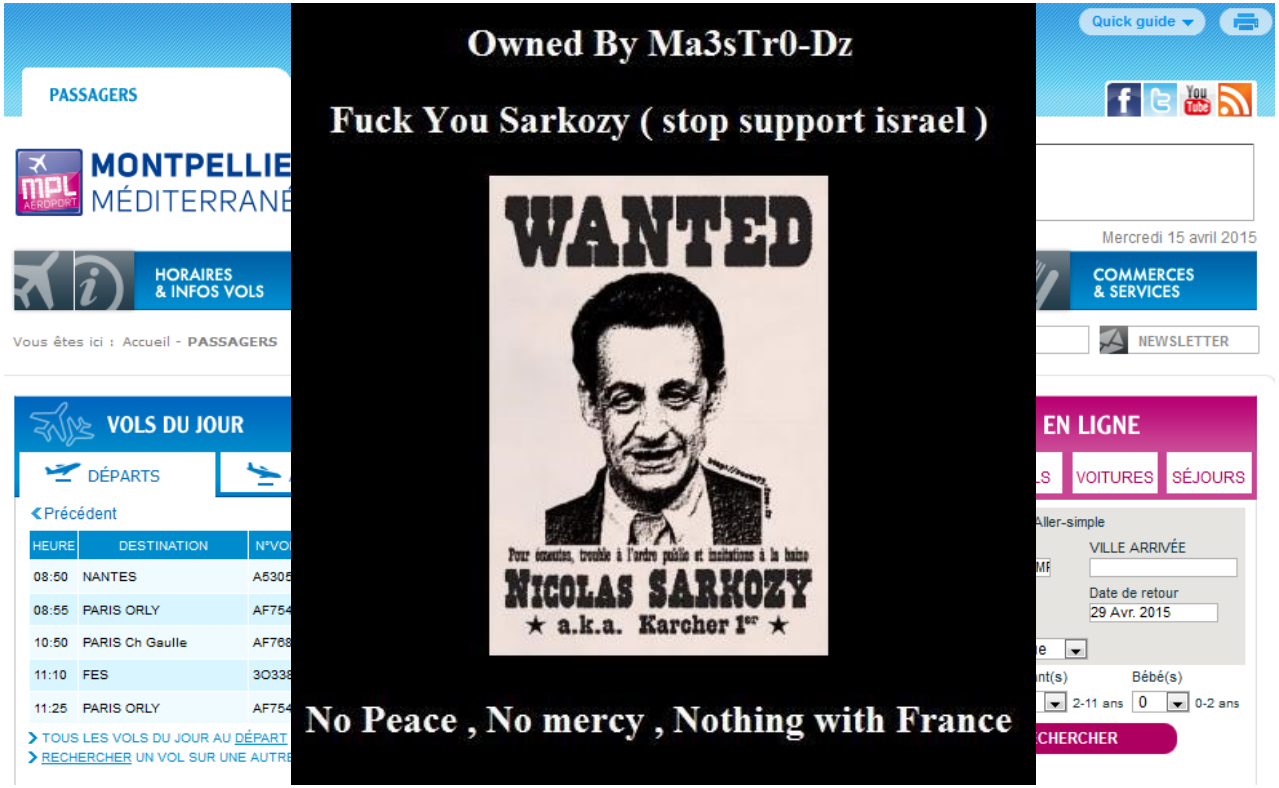
Pourriel

Statistiques de messagerie horaire



Détérioration de données

Le défaçage



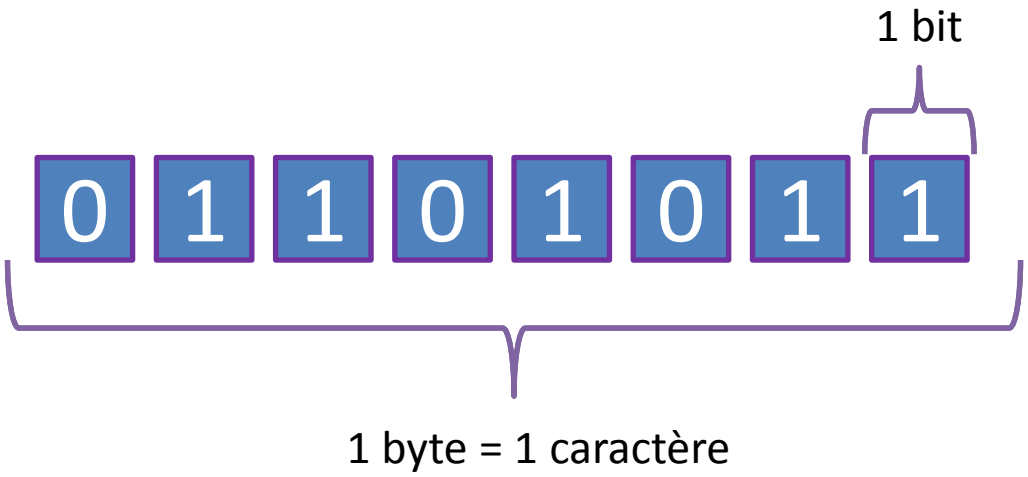
La page Facebook de TV5 Monde

La page Facebook de TV5Monde détournée par un groupe se réclamant de Daesh. - CAPTURE D'ECRAN

Poubelle

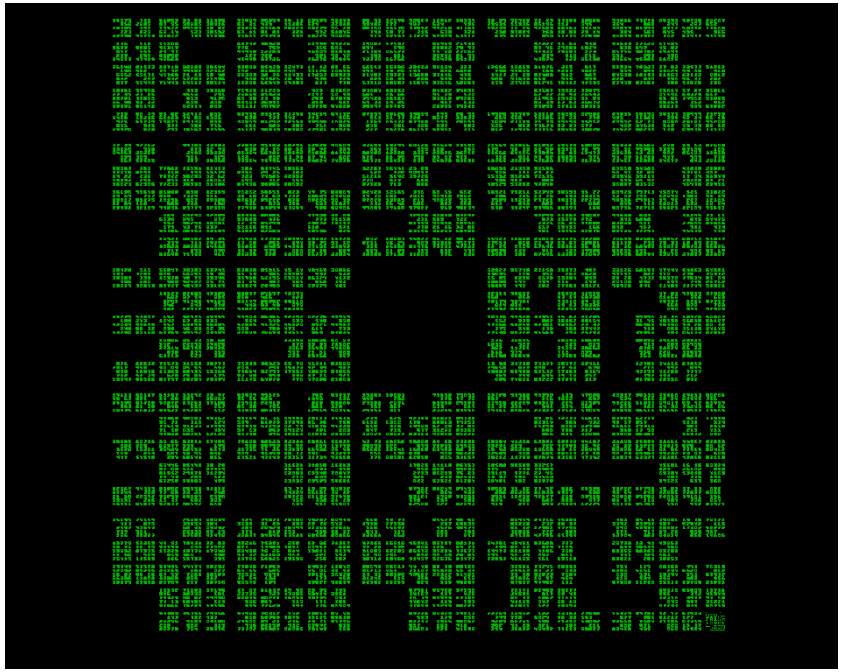
Détérioration des données

Changer quelques bits dans un fichier de base de données



Déterioration des données

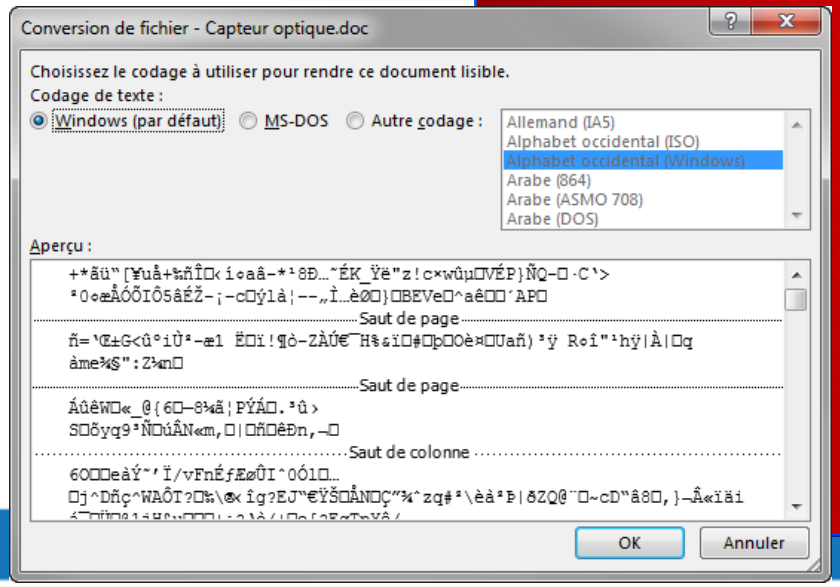
Réaction d'un utilisateur ayant fait une bêtise…



Déterioration des données

Attaques extérieures…

Ransomware



Ransomware

Le 12 Décembre 2016

Ransomware : une attaque toutes les 40 secondes contre les PME

On assiste à un triplement des attaques de ransomware contre les PME en 2016. (Crédit D.R.)

Entre janvier et septembre 2016, le nombre d'attaques de ransomware contre les entreprises a triplé. En septembre, Kaspersky Lab enregistrait une attaque de ce type toutes les 40 secondes contre une toutes les 2 minutes en début d'année. Une entreprise sur cinq dans le monde est concernée.

Selon un rapport de l'entreprise de sécurité Kaspersky Lab, entre janvier et septembre 2016, la fréquence des attaques de ransomware contre les entreprises est passée de deux minutes à 40 secondes. Pour le grand public, la situation est encore pire : en septembre, la fréquence des attaques est passée à 10 secondes. Au cours du troisième trimestre de l'année, Kaspersky Lab a détecté 32 091 nouvelles versions de ransomware contre seulement 2 900 au cours du premier trimestre. « Au total, nous avons comptabilisé 62 nouvelles familles de malwares de

Ransomware

Le 17 Février 2016

Le ransomware Locky propagé par des macros Word fait des ravages

Le ransomware Locky permet à des pirates de chiffrer des données qui ne délivrent une clé de chiffrement qu'une fois la rançon versée. (crédit : D.R.)

Utilisant la même technique de vol de données que le cheval de Troie Dridex, de sinistre mémoire, le ransomware Locky est actuellement massivement poussé sur des ordinateurs cibles. Une rançon de 3,6 millions de dollars a été demandée à un centre hospitalier américain pour remettre en marche son système d'information.

Un nouveau type de ransomware utilisant les mêmes modalités d'attaque que le fameux malware bancaire Dridex, fait des ravages sur les machines de certains utilisateurs. En général, les victimes reçoivent par courrier électronique une facture incluant une macro sous forme de document Microsoft Word, ou une petite application, qu'elles ouvrent sans trop de méfiance. Un seul conseil : attention aux documents Microsoft Word contenant des

Ransomware

23 FÉVRIER 2017 / MALWARE

Un ransomware piège les Mac

Le plus gros souci de ce malware concerne la façon dont il chiffre les fichiers. Il génère une clé de chiffrement unique pour tous les fichiers et les chiffre dans des archives zippées. Cependant, le malware ne semble pas être capable de communiquer avec un serveur externe, empêchant toute possibilité d'envoi de la clé à l'attaquant avant d'être détruit.

Ransomware

06 JANVIER 2017 / SÉCURITÉ

Le malware Killdisk évolue en ransomware

Le malware Killdisk est maintenant capable de crypter des fichiers sur les systèmes Windows et Linux et demande 216 000 dollars pour les restaurer.

Juin 2016

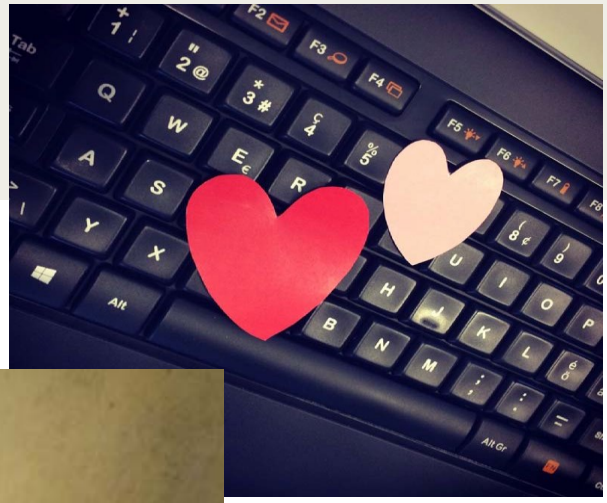
Alerte: Nouvelle vague du ransomware policier au nom de fedpol / SCOCI

fedpol met en garde contre un ransomware policier usurpant l'identité de fedpol / du SCOCI.

Hack Academy

Avec un ordinateur…

Nigériane & Cie



Sextorsion

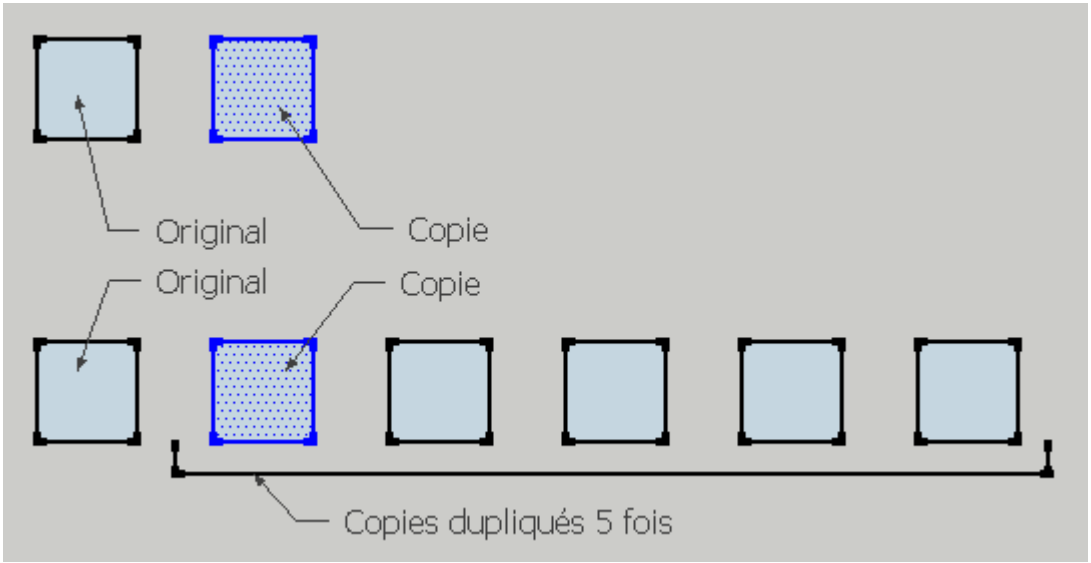
Arnaque au président

En trois ans, 360 entreprises françaises ont été les cibles de gangs internationaux, pour un préjudice global de 300 millions d'euros. La Direction centrale de la police judiciaire et le Medef vont signer mercredi un partenariat pour mieux protéger le tissu économique francais.

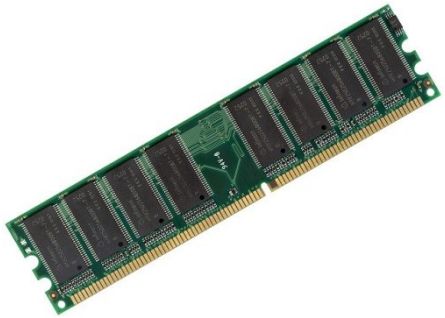
Différences entre le monde physique et le monde numérique

Monde du papier

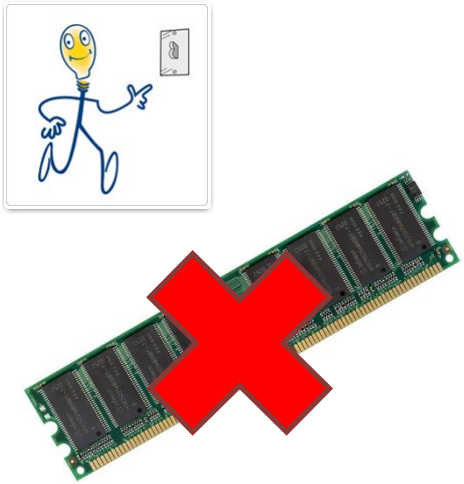
Document original / copies



Monde numérique



Ne reste que des copies…



Exemple de conséquence:

Effacer un fichier

combien de copies ?

où ?

C'est vous qui le dites...

Bonnes manières de faire et d'agir

Règles fondamentales

Faire des sauvegardes

Trop beau pour être vrai

Ne pas être curieux

Se renseigner

Avoir fait les mises à jour nécessaires

Mots de passe forts

- Plusieurs alphabets (lettres, chiffres, &%*-,.)
- Longueur convenable
- Pas toujours le même
- Pas facile à trouver

Virus, botnets, chevaux de Troie

- Ne téléchargez pas des programmes d'origine douteuse
- Ne téléchargez pas des programmes connus sur des sites douteux ou des sites peu fiables
- Méfiez-vous des fichiers joints aux messages que vous recevez
- Fuyez les disquettes ou les clés d'origine douteuse
- Créez dès maintenant, si ce n'est pas déjà fait, une disquette de boot saine contenant un antivirus
- Procédez régulièrement à des sauvegardes du contenu important de votre disque dur après avoir vérifié l'absence de virus tenez-vous au courant des apparitions de nouveaux virus.

Règles face au Hammeçonnage

Vérifier l'orthographe du nom de domaine

Pas de @ dans les URL

Attention au jeu de caractère

- Latin, unicode

Vérifier les certificats électroniques

Ecrire manuellement les URL

Et s'il ne faut qu'en garder une, …

Photo: Shutterstock

En cas de problèmes

Préserver la preuve…

affaire de spécialistes

Prendre contact avec la police

Preuve numérique

Une particularité très importante du monde numérique :

Volatilité

Mots clés

Non-altération

Tracabilité

Préservation de la preuve

Changement des données

Perte de données

Effacement des données (virus, ver, etc…)

Illustration

conseil Boîte de réception

de **st-christophe@paradis.com** <st-christophe@paradis.com> masquer les détails 09:38 (il y a 7 minutes) Répondre

à undisclosed-recipients <>

date 6 déc. 2007 09:38

objet conseil

roule moins vite, chauffard !!!

Répondre Répondre à tous Transférer Inviter st-christophe@paradis.com sur Gmail

Questions ?

- Merci de votre attention
- Avez-vous des questions?

Hack Academy