PASSION AFFAIRES et technologies

NOUS AIDONS LES ENTREPRISES À TRANSFORMER LEURS TI EN LEVIER D'AFFAIRES

ARSolutions 25 ans

Vol. 3 nº 9. Novembre 2016

ÉDITION SPÉCIALE

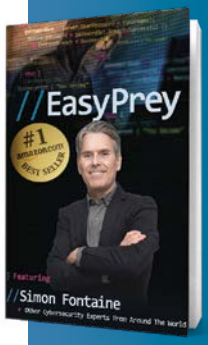
ARTICLES COUPS DE CŒUR DE NOS LECTEURS

DÉCOUVREZ LES ARTICLES LES PLUS LUS EN 2016 !

EN PRIMEUR!

OPPORTUNITÉ PRÉ-LANCEMENT POUR NOS LECTEURS

Obtenez en **EXCLUSIVITÉ** une copie du second livre de **Simon Fontaine, président et co-fondateur d'ARS Solutions.**



Sélectionné à nouveau par *CelebrityPress,* un leader dans le domaine des publications TI, il a co-écrit le livre *«Easy Prey»* en collaboration avec des entrepreneurs de partout en Amérique du Nord.

Contactez-nous au **418 872-4744 pour demander votre exemplaire SANS FRAIS.**

Suivez-nous

2 ÉTAPES SIMPLES pour récupérer 691 heures de productivité par année

TEMPS DE LECTURE 3:00

Dans les entreprises, il existe de nombreuses sources de perte de temps. Saviez-vous que la recherche de documents en est l'une des principales? Non seulement la recherche de fichiers, mais la duplication des versions ainsi que la mauvaise gestion des dossiers peuvent vous coûter cher...

Une étude de l'IDC (International Data Corporation) a révélé que les travailleurs passent environ **36 % de leur temps à la recherche de documents**. Sceptique? Amusez-vous à faire l'exercice dans votre propre entreprise et constatez les résultats par vous-même... Par employé, cela correspond à environ 14,4 heures par semaine, 57,6 heures par mois et 691 heures par année – gaspillées à rechercher de l'information que vous détenez déjà! Même si vous avez une petite compagnie d'une dizaine d'employés, cela représente 6 910 heures par année. Imaginez ce que votre entreprise pourrait faire avec autant d'heures de plus par année!

Par ailleurs, **39 % des utilisateurs corporatifs ne peuvent trouver l'information nécessaire pour accomplir leur travail quotidien**. Non seulement perdent-ils leur temps à essayer de la trouver, mais au final, ils ne la trouvent tout simplement pas.

Voici 2 étapes simples afin de vous aider à éliminer le temps perdu.

ÉTAPE 1 : ÉTABLIR UN STANDARD DE NOMMAGE POUR VOS FICHIERS

Créez un organigramme faisant état de qui se rapporte à qui et incluez une brève description des tâches de chacun. Ensuite, considérez tous les types de documents que les utilisateurs travaillent.

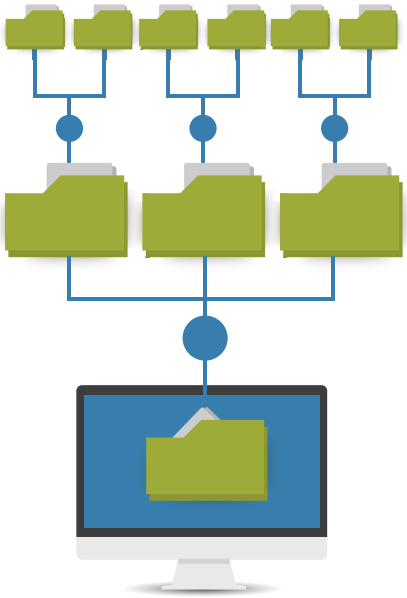
Pourquoi un standard de nommage? Parce que c'est la clé du repérage facile de vos fichiers. Si vous n'avez pas standardisé la façon dont vous nommez vos fichiers, chaque employé va utiliser la méthode qu'il croit être la meilleure.

SUITE À LA PAGE 2 ▼

Affaires et techno

SUITE DE LA PAGE 1 ▲

Les bonnes intentions peuvent vite dégénérer... Modifier à tour de rôle le titre d'un fichier et l'enregistrer à un autre endroit créera de nombreux doublons et au final, vous ne saurez plus identifier la bonne version. Dans quelques mois, trouver ce document pourrait être impossible. Vous allez devoir le retracer, le renvoyer, ou encore pire, avoir à le redemander et le refaire acheminer. Vous venez de perdre trois heures de productivité sur un simple document.



CONCEVOIR LE SCHÉMA DE NOMMAGE

Bien sûr, il en existe d'autres, mais voici quelques exemples de règles à suivre pour que vos documents soient faciles à trouver :

1 Choisissez bien vos caractères;
2 Utilisez une convention de nommage courte pour vos clients réguliers;
3 Utilisez un format de date facilement repérable par ordre chronologique.

ÉTAPE 2 : ÉTABLIR UNE STRUCTURE DE DOSSIERS POUR ACCUEILLIR VOS FICHIERS

Pour la version intégrale de cet article, rendez-vous au www.ars-solutions.ca/blogue

Simon Fontaine, Président
simon.fontaine@ars-solutions.ca

Sécurité des données

#2

Les mots de passe les plus prisés des *hackers*

TEMPS DE LECTURE 2:00

Rapid7 - une entreprise spécialisée en sécurité informatique, est à la tête du projet Heisenberg qui s'appuie sur plusieurs *honeypots* déployés à travers le monde. Ces derniers permettent de collecter différentes informations sur les hackers, notamment sur la manière dont ils procèdent pour attaquer certaines infrastructures.

Ces stratégies utilisées par les sociétés de sécurité informatique fonctionnent comme des leurres et sont donc spécialement conçues pour attirer les pirates. En gros, les *honeypots* permettent d'identifier et de suivre toutes les activités des cybercriminels en vue de se protéger contre d'éventuelles attaques.

Depuis un an, l'entreprise a pu analyser plus de 220 000 tentatives de connexions enregistrées, dont plus de 5 000 adresses IP situées dans 119 pays différents, principalement en provenance de la Chine (39.9 %) et des États-Unis (24.9 %).

Selon les données recueillies, voici les tops 10 des noms d'utilisateur et des mots de passe les plus utilisés par les pirates :

TOP 10 DES NOMS D'UTILISATEUR:

- administrator (34,9%)
- Administrator (24,2%)
- user1 (3,9%)
- admin (2,2%)
- alex (1,8%)
- pos (1%)
- demo (0,9%)
- db2admin 0,8%)
- Admin (0,6%)
- sql (0,6%)

TOP 10 DES MOTS DE PASSE:

- x (5,36%)
- Zz (4,79%)
- St@rt123 (3,62%)
- 1 (2,57%)
- P@ssw0rd (2,55%)
- bl4ck4ndwhite (2,32%)
- admin (2,32%)
- alex (1,82%)
- ..... (1,21%)
- administrator (1,01%)

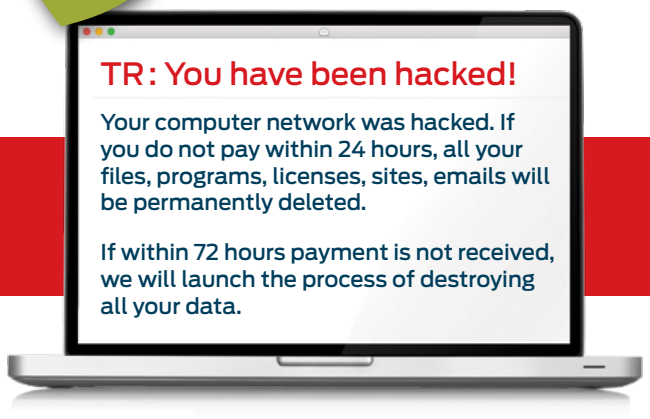
**Fondée à Boston en 2000, Rapid7 est une entreprise qui offre des solutions de sécurité informatique. Elle compte plus de 550 employés et possède un chiffre d'affaires évalué à plus de 105 millions $.*

Nous rendons les entreprises plus efficaces et performantes en transforma

LE RANÇONNAGE : un problème de sécurité majeur pour les entreprises

#3

TEMPS DE LECTURE 3:30



Si vous receviez ce message en ouvrant votre ordinateur, sauriez-vous quoi faire ?

L'hameçonnage (où la fraude par courriel) n'arrive pas qu'aux autres et le fait de demander une somme d'argent en échange de vos données s'appelle le rançonnage. Selon une étude menée par l'Université de Kent en février 2014, plus de 40 % des gens qui ont été victime de *CryptoLocker*[1] ont payé la rançon demandée. Le rapport *SecureWorks* de Dell indique que le même *malware* coûte plus de 30 M$ tous les 100 jours.

Mais comment savoir si la menace est sérieuse ou non ? **Le contenu d'un courriel ou d'un message texte hameçon vise à déclencher une réaction impulsive de votre part.**

Il peut se présenter sous différentes formes : *Cher titulaire de compte en ligne… Votre compte n'est pas accessible à l'heure actuelle… Nous vous prions de vérifier les renseignements de la transaction ci-dessous…* On vous demande alors une réponse immédiate sous un faux prétexte. Dans tous les cas, il n'y a pas de chance à prendre.

SI CELA VOUS ARRIVE, PAR OÙ DEVEZ-VOUS COMMENCER ?

- Soyez vigilant : prenez l'habitude de vérifier la barre d'adresse du site Web afin de voir si elle est différente de celle inscrite dans le courriel;
- Ne répondez pas à ces courriels ou messages textes;
- Ne cliquez jamais sur les hyperliens;
- Ne fournissez l'information demandée sous aucun prétexte.

Si vous avez malencontreusement répondu aux courriels, agissez rapidement et faites vérifier votre réseau.

Les programmes malveillants sont à toutes fins pratiques invisibles. Ils sont difficiles à détecter, car généralement ils n'apparaissent pas dans la liste des programmes installés et peuvent se réactiver à tout moment.

Un diagnostic révèlera s'il s'agit d'une vraie menace et vous permettra de savoir quoi faire. Vous pourrez ainsi évaluer la situation et serez en mesure de prendre la meilleure décision. ***N'hésitez pas à nous contacter si vous avez besoin d'aide.***

Cet exemple est tiré d'un cas réel vécu par l'un de nos clients qui, heureusement, n'a pas subi de conséquence grave puisque ses données étaient bien sécurisées. Par contre, **la vérification lors du diagnostic a révélé que la menace était bien réelle**. Les outils mis en place pour assurer la sécurité ont fait une partie du travail. Toutefois, il a quand même été nécessaire de faire une mise à niveau de la sécurité de l'environnement.

[1]CryptoLocker est un logiciel malveillant de type cheval de Troie et qui tourne sous Windows. Le programme se diffuse principalement via des mails infectés, déguisés en factures UPS, FedEx ou de banque. Une fois activé, il chiffre les données personnelles de l'utilisateur et demande une rançon pour les déverrouiller. Le message d'alerte s'accompagne d'un compte à rebours de 72 ou 100 heures, qui menace de supprimer les données si la rançon n'est pas payée. Une fois arrivé à zéro, il augmente en réalité fortement le montant de cette dernière (source : Wikipédia).

Pour plus d'informations sur…

- **Comment se présente l'hameçonnage**
- **Quels sont les signes précurseurs**
- **Comment s'en prémunir**

Consultez l'article intégral au www.ars-solutions.ca/blogue

Notre groupe a maintenant un gain en efficacité de près de 100 heures par semaine!

Avant qu'on rencontre ARS, les frustrations et les pertes de temps s'accumulaient. Nous avions des problèmes de lenteur au niveau du réseau et des problèmes récurrents qui nuisaient à nos usagers. On avait besoin de gens compétents sur qui se fier et en mesure de répondre rapidement à nos demandes.

Nous faisons affaires avec ARS depuis moins d'un an et nous notons déjà un gain en efficacité de près de 100 heures par semaine pour les 10 entreprises du DIX54 et une qualité de vie au travail supérieure. Notre environnement est stable, performant et les problèmes se règlent plus vite. On a l'esprit tranquille parce que nos systèmes sont sécurisés.

Julie Pilote
Les Constructions Bé-Con
Administratrice et propriétaire

TEMPS DE LECTURE 2:30

Vérifiez auprès de 165 sites Web et plus dont LinkedIn, Dropbox, Adobe, etc.

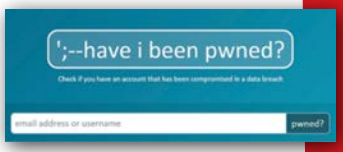
Les arnaques, la fraude en ligne et le vol d'identité ne sont que quelques exemples d'enjeux devenus très préoccupants dans le cyberespace. Naviguer sur le Web tout en évitant ces menaces peut représenter un défi de taille. En effet, des millions de personnes sont régulièrement victimes de cyberattaques sans même le savoir. Dans cet article, vous découvrirez si vos identifiants ont été volés parmi plus de 165 sites répertoriés.

DROPBOX – L'UN DES PLUS GRANDS CAS DE CYBERATTAQUE AU MONDE

On annonçait dernièrement que Dropbox - *plateforme américaine de stockage de documents en ligne* - avait subi une **brèche de données en 2012 et que près de 70 millions d'identifiants (noms d'utilisateurs et mots de passe) avaient été volés. Et ce n'est qu'il y a quelques semaines, soit 4 ans plus tard, qu'elle a admis que les informations de ses clients avaient été publiées en ligne...** Dropbox a rapporté que les adresses courriel ont été rendues publiques. Elle a mis en garde ses utilisateurs que s'ils ont utilisé le même mot de passe pour d'autres services, qu'il serait préférable de le changer immédiatement.

VOS IDENTIFIANTS ONT-ILS ÉTÉ PIRATÉS ?

Rassurez-vous, il existe un outil gratuit fort simple et sécuritaire pour le savoir !



La page Web « **Have I been pwned** » (Est-ce que je me suis fait avoir?) répertorie l'ensemble des sites piratés et dont les informations personnelles ont été divulguées.

Simplement en entrant votre adresse courriel, vous pourrez savoir si vous avez été impliqué par l'une des cyberattaques recensées par le site. Attention! Même si le site affiche "**Good news – no pwnage found!**, cela ne veut pas dire pour autant qu'il n'y a aucun risque, puisqu'il se peut que vous ayez été impliqué dans une brèche qui n'a pas encore été révélée...

Il est donc urgent que vous vérifiiez vos comptes et rehaussiez leur sécurité.

À ce jour, ***Have I been pwned*** prend en compte plus de 165 sites et applications et 1 925 000 000 comptes compromis, provenant entre autres des sites suivants :

myspace	359 420 698
in	164 611 595
Adobe	152 445 165
	68 648 009
vtech	4 833 678
	4 609 615
Forbes	1 057 819
YAHOO!	453 427
	116 465
Bell	20 902
SONY	37 103

Sources : Have I been pnwed : https://haveibeenpwned.com
Times : http://time.com/4474986/dropbox-hack

ARS solutions affaires et technologies
6655, boul. Pierre-Bertrand, bureau 301, Québec (Québec) G2K 1M1
www.ars-solutions.ca | info@ars-solutions.ca | 418 872-4744