CHIP

mars 2006 Vol. 22, No. 7

Club informatique Mont-Bruno — Mount Bruno Computer Club

La Saint-Patrick, WOW! le printemps RE WOW!

Calendrier des prochaines activités

mercredi **1** mars	**Windows, Internet — (niveau facile)** **Windows:** Le téléchargement, l'installation et l'utilisation de l'anti-espion Ad-Aware. **Internet Explorer:** Les témoins (cookies) et les fichiers Internet temporaires. **Site Internet:** Quelques sites de bons dictionnaires.	**Michel Gagné** **(19h30)**
mercredi **8** mars	**Les Graveurs — (niveau intermédiaire)** Gravure d'un CD avec « Nero 6 ». Les différences entre graver un CD-R et un CD-RW. Création d'un CD de démarrage avec les principales commandes de DOS. La comparaison entre la vitesse [1X] pour le CD et [1X] pour le DVD.	**Pierre St-Aubin** **(19h30)**
mercredi **15** mars	**La Sécurité sur Internet — (niveau intermédiaire)** Le vol d'information et le sabotage informatique a pris beaucoup d'ampleur ces dernières années avec, parfois, des conséquences désastreuses. Nous allons exposer les principales menaces auxquelles font face ceux qui utilisent Internet pour fins personnels et les mesures de base à prendre pour se protéger.	**André Archambault, Pierre Geoffroy** **(19h30)**
Vendredi **17** mars	**Windows, Internet Réunion de l'après-midi — (niveau facile)** **Windows:** Le téléchargement, l'installation et l'utilisation de l'anti-virus AVG. **Internet Explorer:** Outlook Express (3 de 4). **Site Internet:** LESPAC	**Réjean Coté** **(13h30)**
mercredi **22** mars	**MS Word « Le Tableau » — (niveau intermédiaire)** La création d'un tableau et les modifications possibles des cellules, des rangées et des colonnes. La mise en forme du texte inclus. Démonstration d'exemples de tableaux simples qui peuvent vous servir dans vos documents.	**Robert Paradis** **(19h30)**

Toutes les soirées du Club ont lieu au Centre Communautaire.
53 Rabastalière est, Saint-Bruno, Qc

CHIP est le bulletin officiel du Club informatique Mont-Bruno. Les articles présentés dans ce bulletin sont le reflet des opinions des personnes les ayant rédigés. Les articles qui nous sont expédiés pour publication doivent être signés.

CHIP is the official newsletter of the Mount Bruno Computer Club. The opinions presented in this newsletter are those of the authors and not necessarily the views of the Club. Articles submitted for publication must be signed.

CHIP est un acronyme qui signifie « Computer Hackers Information Pamphlet ».

CHIP est édité avec le logiciel Microsoft Office 2000 et Microsoft Publisher 2000. Également une imprimante Brother MFC-8500.

Le Club informatique possède une adresse courriel (e-mail address):
cimbcc@cimbcc.ca

Visitez la page d'accueil du Club sur Internet à l'adresse suivante:
Visit our WEB site and find out about the Club activities:
http://www.cimbcc.ca

Sommaire

Carnet d'adresses Internet

Par Albert Richard

Email/Courriel: albertri@videotron.ca
Mon site à http://pages.infinit.net/alber

Dictionnaire d'argot en ligne - French slang dictionary online
(ABC de la langue française)
http://www.languefrancaise.net/glossaire/

Les Oiseaux du Québec
www.oiseauxqc.org

How to Perform a Windows XP Repair Install
http://www.michaelstevenstech.com/XPrepairinstall.htm

Fondé en 1983, le Club informatique Mont-Bruno est une société incorporée sans but lucratif. Ses administrateurs et ses animateurs déclinent donc toute responsabilité envers les participants aux soirées d'information verbale ou écrite. De plus, nous déclinons toute responsabilité sur les conséquences possibles de vos expériences que vous seriez tentés de faire, suite à ce que vous auriez entendu ou discuté entre membres du Club, aux soirées ou ailleurs.

Founded in 1983 by M. Gordon Craig, minister of the United Church in St-Bruno, Mount Bruno Computer Club is incorporated as a non-profit organization. All responsabilities are declined as described in the French text above.

Adresse postale: **Club informatique Mont-Bruno**
a/s Service de la Récréation
1585 rue Montarville
Saint-Bruno de Montarville, Qc. J3V 3T8

Message du président

Réjean Côté,

Soupir de soulagement pour la plupart d'entre nous, le mois de mars arrive, cela veut dire que le printemps est à nos portes et que nous pouvons commencer à rêver à la pose de nos fleurs et à la planification de notre potager.

Il y aura beaucoup d'activités au Club pour le mois de mars, six présentations de sujets différents sont au programme.

Les espions dans nos ordinateurs sont de plus en plus présents et c'est pourquoi il est important d'installer un anti-espion et de faire une recherche des espions environ une fois par semaine pour les éliminer de votre ordinateur. Le 1er mars, Michel Gagné vous montrera comment télécharger, installer et utiliser l'anti-espion gratuit Ad-Aware. De plus il vous parlera des fonctions des (cookies) et des fichiers temporaires. Pour finir il vous montrera comment trouver des sites de dictionnaires.

Le mercredi 8 mars, soirée sur la gravure avec Pierre St-Aubin. Vous verrez comment graver un CD avec Nero 6, faire une multi session de gravure, les options sur la gravure et aussi comment faire les copies de sécurité de votre ordinateur. Il vous montrera aussi comment faire un CD de démarrage, chose particulièrement importante aujourd'hui, car avec la plupart des nouveaux ordinateurs, on ne peut plus utiliser de disquette pour le démarrage de son ordinateur.

Mercredi 15 mars, soirée importante sur la sécurité présentée par André Archambault. La sécurité prend une place de plus en plus grande aujourd'hui. Avec les virus, les espions, les vers etc… qui peuvent envahir nos ordinateurs, il faut être de plus en plus prudent face à tous ces envahisseurs malveillants.

Le vendredi après midi à 13h30, suite à la soirée sur la sécurité**,** nous verrons comment installer l'antivirus AVG dans sa version gratuite mais disponible en anglais seulement. La deuxième partie avec Outlook Express portera sur l'envoi de messages et de son contenu comme: mettre une couleur de fond, ajouter un GIF animé et aussi comment y inclure une pièce jointe, un diaporama par exemple. Nous verrons aussi comment gérer notre carnet d'adresses. En dernière partie nous apprendrons comment faire une recherche sur le site LESPAC pour y acheter certains articles et aussi comment placer une annonce sur le site pour y vendre son auto par exemple. La popularité des vendredis après-midi semble se confirmer, car même avec une mauvaise température et des vents très violents, 53 personnes ont assisté à la présentation du 17 février.

Vous aimeriez savoir comment faire un tableau? Venez assister à la présentation du 22 mars de Robert Paradis, qui continue avec sa 3ième soirée sur Word. Le sujet portera sur la création de tableaux avec les modifications des cellules, des rangées et des colonnes et aussi une démonstration d'exemples de tableaux qui vous serviront dans vos documents Word.

Au plaisir de vous revoir,
Réjean Côté

LE COIN DU CURIEUX

(par Michel Gagné)

N.D.L.R. Michel Gagné termine ses vacances près du Tropique du Cancer, *Le Coin du Curieux* reviendra dans le CHIP d'Avril. Merci !

Malware

By Don Druce

Right up front, I am going to tell you that this is not an article about Malware, but rather an Anecdote. OK, I am cheating a bit, but really it is meant to be an anecdote, I just got carried away.

If you have been paying attention lately, you have most probably heard the term Malware. Some make lightly of it, some ignore it, some are concerned, some realize the dangers and some do not. My personal opinion is that the Good Guys vs. Bad Guys exchange is continuing to escalate and is now at a position where the casual user cannot follow the evolution. Even the more advanced users are having a difficult time in keeping up.

So, on to my anecdote.

There is a rather popular program on TV - **"Call For Help TV"** -out of Toronto - that has or is starting to get world wide distribution. It is distributed in Australia, so we could even say it goes around the world. No, it is not distributed in all countries in between, but it has wide ranging appeal.

The show is hosted by **Leo Laporte**, one of the co-hosts up to about six months ago was Andy Walker. [www.cyberwalker.com]. *Andy Walker* according to the back leaf of his recent book on "**Security, Spam, Spy ware & Viruses"** is one of North America's top technology journalists. [ISBN 0-7897-3459-1]. OK, so his credentials are well established.

To continue with the back leaf, he " now lives in Toronto with two cats and a really secure personal computer."

If you have been following the Malware evolution, you have heard of the term **Rootkit** and **DRM**. Sony did their best to make a mess of things by distributing about 50 CDs protected by DRM and containing Rootkit technology which ended up being installed on users computer, if they happened to play one of the infected CDs on their computer and were not in the know. I mentioned this, and the dangers involved - which are considerable, at one of our meetings earlier on in the year. Sony are not the only distributors of Rootkits, but their bad judgment in using one on their CDs brought world wide attention - and lawsuits from various groups and even from some state governments. So, to say the least it is a serious business.

Well, on one of the more recent Call For Help TV shows Leo Laporte explained that there is now a Rootkit detector available for download on the Net. The difficulties in detecting a Rootkit and why is is a problem, I will leave for some other time. Just understand that because of it very nature, a Rootkit is most difficult to detect than the Malware we are used to dealing with. To detect if you have the Sony Rootkit in your computer is rather simple because its functioning has been determined/documented and you can therefore determine that it is there by a simple test. The functioning of other Rootkits have not been documented and their detection is therefore difficult. Your **AntiVirus** software, **AdWare** and **SpyWare** tools will not see them. (my spellings to get attention) and most certainly will not remove them.

Back to the anecdote. On the show, Leo Laporte gave the URL where you can download the Rootkit detector. One of the assistants in the background - on the spot - downloaded the detector and ran it on the portable previously used on the show by Andy Walker. Now you see why I brought up his name above. I am sure you have already guessed what I am going to say next. Andy Walker's portable was hiding a Rootkit.

So, on a TV show dedicated to computers, where Malware has been explained again and again, where one of the co-hosts has written a book on the subject, his computer is infected.

I am going to leave it at that for the moment. I clearly realize that I have left some open questions here. The club is having a session on Malware on Wednesday March 15th and you might want to save your questions for that presentation.

I do have to make one comment regarding recent articles on our Web site that also appeared in Le Journal. This is just being said to clear the air so to speak. The only known way to remove a Rootkit - other than the Sony Rootkit for which removal tools have been developed - is to reformat your hard drive and install a new OS. So, the threats should not be taken lightly.

Today, as I write this article, I just took a quick look, and Microsoft have released 6 (six) new critical updates. ***(See Table above right…)***

Summary

It is becoming more and more difficult to protect your computer. Malware is becoming more and more sophisticated and protection methods are lagging more and more behind are becoming less effective. With approximately 100 new Viruses being release each week, some becoming more and more sophisticated, do you need to question why.

There are Viruses out there that:

1. attack other viruses.
2. attack Anti-Malware programs.
3. have payloads that do nothing, all the way up to literally destroying all your data.
4. there are free and "commercial" anti-Malware programs on the Net that are Malware themselves (Yes, some people pay for Malware).
5. anyone can be hit.
6. removing some spyware programs will disable other programs or your computer.
7. some recent Virus programs destroy data and are designed so as to be able to destroy data in your backups.
8. our club needs to cover the subject in more detail than in the past, distribute more - and more accurate - information to members.
9. I could go on, but I am sure that you get the point.

Last but not least, you are responsible for protecting your computer, so take heed and I hope we will see you on Wednesday March 15th. - Check the club Web site calendar to see why.

Till next month ….

UNC (*Universal Naming Convention*)

Web definitions for UNC

A standard for identifying servers, printers and other resources in a network, which originated in the Unix community. A *UNC* path uses double slashes or backslashes to precede the name of the computer. The path (disk and directories) within the computer are separated with a single slash or backslash, as in the following examples.

Note that in the DOS/Windows example, drive letters (C:, D:, etc.) are not used in UNC names.

\\Server_Name\Shared_Folder

Don Druce

Robert Paradis

Big Bobby's Corner

Selon vous, pour un internaute, existe-t-il pires menaces qu'un virus, un Cheval de Troie, un ver informatique ? — Pas plus tard que l'an dernier (2005), effectivement, il y avait pire : les espions, les zombies. Cette année, pour 2006, une nouvelle menace s'ajoute à cette longue liste de cochonneries et c'est « *La réalité artificielle.* »

Notez bien que les virus et compagnies étaient et sont toujours aussi dangereux. Mais les espions eux, ont cette manie de voler votre identité, vos secrets les plus intimes…BRR…Et si un ou des espions réussissent à voler votre identité, soyez bien conscients qu'une fois qu'ils auront vos coordonnées, vous ne saurez ce qu'ils ont fait avec... que trop tard.

Cette année encore (2006), on nous annonce une nouvelle menace qui pourrait s'avérer encore pire… ***Trend Micro*** appelle cela **« La réalité artificielle »,** une nouvelle technique de vol d'informations personnelles. Selon un des représentants de Trend, la réalité artificielle consistera à faire passer pour réelles des informations qui ne le sont pas via l'écran de l'ordinateur d'un utilisateur, une version évoluée de l'hameçonnage (*phishing)*, en quelque sorte.

On donne l'exemple d'un utilisateur qui, pensant consulter son compte bancaire en ligne, visualisera en fait des pages falsifiées, lesquelles lui présenteront un compte créditeur alors que, dans la réalité, son compte aura été vidé depuis longtemps. On imagine le dialogue qui pourrait s'ensuivre avec la banque appelant son client pour l'inviter à renflouer ses finances…

Autre exemple : faire croire à l'utilisateur qu'il est bien à jour dans ses correctifs de sécurité (système d'exploitation, navigateur, etc.) alors que son système sera, dans la réalité, complètement troué. Ceci constitue une situation en or pour les pirates qui pourront exploiter les vulnérabilités de la machine pour installer logiciels espions et autres applications de contrôle à distance. Avec le consentement indirect de la victime qui aura, de fait, toute confiance dans son système.

Cette *réalité artificielle* passera notamment par l'exploitation des **rootkits**, ces applications qui simplifient l'accès au système et permettent du coup d'automatiser la mise en place d'une porte dérobée (*backdoor*) ou d'un cheval de Troie. Des programmes seront également capables de modifier le noyau (kernell) du système d'exploitation afin de cacher fichiers et processus. Du fait même de leur nature, les rootkits sont difficilement détectables et également difficiles à désinstaller.

LES ROOTKITS

Ainsi, dans les mains d'un esprit malveillant, l'installation d'un rootkit permettrait de modifier en profondeur nombres de processus de votre machine, à commencer par vos requêtes Web. Certes, l'installation d'un rootkit nécessite des droits d'administrateur, qui peuvent être obtenus par l'intermédiaire d'une faille du système. L'affaire de Sony BMG, qui utilisait un rootkit pour mettre en oeuvre des outils anticopies sur ses CD de musique, est éloquente. Évidemment, depuis cette découverte, Sony a émis un correctif à cette lacune grave de votre sécurité. A défaut d'avoir porté ses fruits, l'affaire du rootkit de Sony BMG aura au moins permis d'aborder un domaine de la sécurité informatique jusque-là ignoré de la plupart des éditeurs de solution de sécurité.

Ce serait donc à dire que **si votre système est à jour** avec tous ces correctifs, celui de Sony comme de tous les autres, vous seriez à l'abri de ces menaces ? Tant mieux pour les optimistes. Il ne faut jamais oublier que c'est l'utilisateur lui-même (vous) qui, sans porter attention la majeure partie du temps, installe ces outils de contrôle à distance. On a donc tout avantage à les reconnaître du moins essayer de les reconnaître, n'est-ce-pas ?

À la décharge de toute* cette *mauvaise publicité, il faut quand même mentionner qu'un rootkit n'a rien de dangereux en soi. Il s'agit d'un outil d'administration qui permet notamment de modifier les règles de fonctionnement de l'environnement en toute discrétion vis-à-vis de l'utilisateur. Du coup, il reste invisible aux yeux ***des antivirus et pare-feu traditionnels — Mais sa discrétion en fait une arme de choix pour les pirates qui tentent de l'utiliser pour dissimuler leurs propres virus et autres codes malveillants. Malheureusement, XCP, le rootkit développé par la société First4Internet pour le compte de Sony, s'est révélé être une véritable aubaine pour les individus aux agissements douteux ou criminels.***

Un autre danger, parfaitement complémentaire de l'exploitation des rootkits, menace directement les réseaux : le détournement des requêtes Web par l'intermédiaire de certains protocoles de routage qui forment notamment le cœur d'Internet. Un de ces protocoles entr'autre se charge des échanges d'informations sur la disponibilité des réseaux selon le principe que chaque routeur du réseau ne connaît directement que ses voisins proches et non l'ensemble du réseau.

« *Comme l'architecture du réseau n'est pas centralisée, il n'y a aucun moyen de confirmer le bon routage d'une adresse* », explique un représentant de Trend Micro, *« et* comme *l'information de routage ne peut être garantie, le système est sujet à des attaques. »*. N'importe quel internaute véreux pourrait ainsi compromettre un routeur du réseau et détourner les requêtes qui passent par là.

En conséquence, une adresse Web pourtant correctement saisie dans votre navigateur pourrait vous amener à un site frauduleux sans que vous en ayez conscience, surtout si les pages falsifiées sont similaires aux vraies.

Les internautes, conscients du danger, peuvent se demander comment se protéger ? Dans de telles conditions, toujours selon Trend Micro, il n'existe pas encore de solution fiable à 100 % pour garantir qu'on se connecte bien au bon endroit. La sécurité concerne autant le particulier, responsable de sa machine, que les entreprises qui évaluent le coût des protections face aux risques de fuites d'information.

Les rootkits peuvent donc poser de sérieux problèmes de sécurité. Les éditeurs de solutions antivirales ne sont plus les seuls à s'intéresser au phénomène. A part les personnes honnêtes, qui d'autres pensez-vous s'y intéressent ? Poser la question, c'est y répondre.

LA SOLUTION D'INTEL POUR LES ROOTKITS

La solution préconisée par Intel pour contrer les esprits malveillants est purement matérielle. Il s'agirait d'une puce qui, placée sur la carte mère, surveillerait en temps réel les changements qui surviendraient dans les codes des programmes résidant en mémoire. En cas de modification suspecte, le système pourrait bloquer la manœuvre le temps que l'utilisateur prenne la décision de valider ou non l'opération, mais pourrait également isoler l'ordinateur du reste du réseau afin de restreindre l'infection ou encore donner une alerte. La puce fonctionnerait quel que soit l'environnement d'exploitation (Windows, Mac OS, Linux...).

L'approche anti-rootkit d'Intel n'est pas sans rappeler une autre puce : ***LaGrande*** (chargée notamment d'isoler les processus d'exécution en mémoire afin d'éviter les infections) qu'Intel devrait introduire en 2006 dans les *chipsets de ses motherboards*.

Or, toutes ces manœuvres ne seront pas complétées avant deux ou trois ans. Aussi, cette solution ne devrait pas s'opposer aux solutions des logiciels d'antivirus. Au contraire, en surveillant certaines parties du système, cette protection pourrait prévenir les désactivations d'antivirus que parviennent à réaliser certains agents malveillants actuels. Du succès de *LaGrande* dépendra probablement l'avenir de cette solution d'Intel.

Albert Einstein

Albert Einstein a été nommé le personne la plus marquante du 20ième siècle par *Time Magazine.* C'était un grand physicien et une des marques de commerce d'un physicien est d'énoncer des *théories*. En voici quelques unes.

- La théorie, c'est lorsqu'on sait tout et que rien ne fonctionne. La pratique, c'est lorsque tout fonctionne et que personne ne sait pourquoi.
- Le monde ne sera pas détruit par ceux qui font le mal, mais par ceux qui les regardent agir et qui refusent d'intervenir.
- La science sans la sagesse est comme une mise à la loterie. On risque de perdre tout ce qu'on a investi.
- La vie, c'est comme une bicyclette: il faut sans cesse avancer, sans s'arrêter, pour ne pas perdre l'équilibre.
- Aucune découverte, aucun progrès, aucune science ne comptent aussi longtemps qu'il existe quelque part un enfant malheureux.
- L'imagination est plus importante que le savoir. On peut tout savoir et ne rien faire tandis qu'avec l'imagination on peut tout faire.
- Il n'existe que deux choses infinies, l'univers et la bêtise humaine…mais pour l'univers, je n'ai pas la certitude absolue.
- Il y a davantage de perfection dans une simple goutte d'eau que dans toutes les machines inventées par les hommes.
- S'il fallait un jour que les forêts disparaissent, l'homme n'aurait plus que son arbre généalogique pour pleurer.
- Je crois que la chose la plus difficile à comprendre au monde est la manière de calculer ses impôts sur un formulaire du fisc.
- Il est plus difficile de détruire un préjugé qu'un atome.
- Le plus important pour un homme de science n'est pas ses diplômes, ni le nombre de ses années d'étude, ni même son expérience, mais tout simplement son intuition.
- Malheureusement, les progrès de la science sont souvent comme une hache dans les mains d'un criminel pathologique.
- L'éducation c'est ce qui reste lorsqu'une personne a oublié tout ce qu'elle a appris à l'école.
- J'ignore quelle seront les armes de la troisième guerre mondiale, mais je suis sûr que celles de la quatrième guerre mondiale seront des frondes et des cailloux.
- Tout homme qui prétend pouvoir interpréter et enseigner les choses de l'au-delà doit être la risée des dieux.

Commentaires - Suggestions - Questions ?

L'Équipe de direction du Club informatique Mont-Bruno vous invite à communiquer vos commentaires, suggestions ou interrogations, que ce soit par courriel, téléphone ou cette note que vous pouvez apporter lors de votre prochaine visite à une soirée du Club. L'anonymat sera respecté si vous le désirez.

De plus, l'éditeur du CHIP apprécierait grandement recevoir soit un article, un texte court, une image ou même quelques expériences personnelles pour inclure dans un prochain CHIP, avec votre permission bien sûr. Merci.