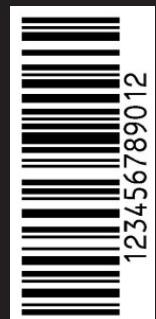


# INFORMAG



## EDITION CYBERATTAQUES

5 DÉCEMBRE 2019





- 6 Attention aux ransomwares
- 8 Le saviez vous ? Spécial ver informatique  
Quelques chiffres sur les cyberattaques

- 8 L'interview du hacker Robin des Bois



- 9 Top 5 meilleurs hackers

10 Protection des données privées :  
Quels sont les outils des criminels ?



20 3 cyberattaques hors normes  
Jeu : Le labyrinthe



# SOMMAIRE

## #56



LES PRODUCTIONS DU POSSIBLE PRÉSENTENT

**THE HACKER  
LOUISAHHH  
MR MAGNETIX  
DRAMA**

SAM 7 DEC - LE BIKINI

# LE BIKINI

Les prochaines soirées  
Décembre 2019  
Toulouse



x

**LeBikini**  
IN BIKINI DURA ROCK



**House  
to  
Techno.**

7€

**JEU. 12 DEC.**

23h-5h30

**Navettes  
au départ  
du centre ville**



# Le nouveau MacBook

Le plus fin, le plus léger et le plus sophistiqué des ordinateurs portables Mac. En or, argent et gris sidéral.  
À partir de 1449 € TTC.

# ATTENTION AUX RANSOMWARE

## Qu'est ce qu'est un ransomware ?

Cela se traduirait en anglais 20% ne reverraient jamais leur données. On estime que toutes les 20 secondes une victime se fait attaquer par ce genre de logiciel malveillant. Généralement, ces virus sont envoyés dans un mail directement en pièce jointe, et il suffit d'ouvrir cette dernière pour que le virus soit instantanément libéré.

Donc un conseil, n'ouvrez jamais une pièce jointe d'un mail dont vous ne connaissez pas l'expéditeur. Ni même un sms, notre smartphone n'est pas à l'abri. Mais ne paniquez pas ! Ce genre de virus ne s'attaque généralement pas aux particuliers mais plutôt aux grandes entreprises où plus d'argent y est en jeu.

Cela se traduirait en anglais 20% ne reverraient jamais leur données. On estime que toutes les 20 secondes une victime se fait attaquer par ce genre de logiciel malveillant. Généralement, ces virus sont envoyés dans un mail directement en pièce jointe, et il suffit d'ouvrir cette dernière pour que le virus soit instantanément libéré.

Donc un conseil, n'ouvrez jamais une pièce jointe d'un mail dont vous ne connaissez pas l'expéditeur. Ni même un sms, notre smartphone n'est pas à l'abri. Mais ne paniquez pas ! Ce genre de virus ne s'attaque généralement pas aux particuliers mais plutôt aux grandes entreprises où plus d'argent y est en jeu.

Cependant, d'après une étude menée par Kaspersky, sur toutes les personnes payant la rançon,

Par Camélia Zahí

## LE SAVIEZ-VOUS ?

Un ver informatique est un programme malveillant qui s'autopropage tout seul. Il fait des copies de lui-même et infeste les programmes qui doivent être infestés. Comme pour les ransomware, les vers se trouvent généralement dans les mails, alors prenez garde !



## QUELQUES CHIFFRES SUR LES CYBERATTAKES

Une cyberattaque se traduit par la mise en place d'un acte de malveillance envers des systèmes informatiques. C'est un fléau de plus en plus présent dans notre société.

Saviez vous qu'au tout début d'Internet, on estimait qu'un virus était créé toutes les heures. A partir de 2006 ce nombre a augmenté pour devenir un par minute, et il était même de un par seconde en 2011. Aujourd'hui, ce serait 3/4 virus par secondes qui seraient créés, ce qui représente tout de même plus de 30 000 par jour. Voilà pourquoi c'est important de faire attention à ce qu'on fait sur internet et d'avoir un antivirus plutôt efficace.

Un virus, on sait rarement d'où ça vient et quelles sont ses intentions. Le meilleur moyen de s'en protéger reste donc de l'éviter. Mais ce n'est pas toujours très évident, et même les très grandes entreprises ne sont pas à l'abri.

Par Camélia Zahí

# L'interview

## du hacker Rabbins des Bois

Par Théo Merenciano



**Vous décrivez un univers de la cyber criminalité très organisé qui rapporte beaucoup, beaucoup d'argent. Ça correspond vraiment à la réalité ?**

"Franchement j'ai essayé d'être un émissaire de là où je viens, de mon propre monde, et j'ai essayé de relater avec le plus de netteté possible ce monde-là. La criminalité aujourd'hui est en train d'évoluer, les criminels sont en train de réaliser qu'il y a bien plus à gagner et bien moins de risques en étant derrière un ordinateur que dans la rue par exemple. Je pense que d'ici 5 à 10 ans il y aura véritablement une transformation et que ça va se voir de plus en plus. Pour vous donner un petit chiffre, en 2018, la cybercriminalité c'était 400 milliards d'euros, d'ici 2020 l'addition sera en trilliard en fait, donc on est vraiment sur une expansion évidente du cybercrime."

**Vous nous expliquez étape par étape comment, en toute discréction, vous êtes devenu riche depuis votre chambre d'ado et derrière votre ordinateur.**

"Ouais voilà c'est ça, c'est à dire que à la base j'ai essayé d'avoir une intégration sociale par l'excellence académique, donc j'ai visé des écoles importantes comme science po comme HEC ou comme polytechnique. En revanche, j'ai jamais été accepté mais j'ai toujours su trouver ma place devant l'écran, ou plutôt derrière l'écran en essayant de gagner de l'argent et dans ma chambre. Donc comme ça s'est plutôt bien passé de ce côté là, j'ai eu tendance à persévirer et j'ai eu plus ou moins de la chance l'année dernière lorsque j'ai pu faire la connexion entre mes deux vies."

**Vous vous positionnez un peu comme un lanceur d'alerte, en tout cas vous dites écrire un livre parce que vous voulez prévenir le public de ce qui se passe en terme de cybercrime, mais vous avez vous même mené cette vie de cybercriminel, c'est pas un peu hypocrite ?**

"Justement c'est pas véritablement par rapport au cybercrime, même si le cybercrime est un constat, c'est avant tout par rapport à la protection des données, les données qui vous appartiennent chers auditeurs, et qui se doivent d'être protégées car c'est votre droit. Actuellement il n'y a plus de vie privée sur Internet, c'est une illusion, on a fait un amalgame et on a totalement confondu vie privée, intimité et réseaux sociaux. Je veux dire, maintenant la ligne n'existe plus. Facebook et Instagram connaissent toute votre vie et vous leur avez donné toutes les clés de votre intimité. J'ai choisi mon anonymat aussi pour pouvoir parler honnêtement, pour pouvoir m'exprimer honnêtement et pouvoir apporter le message le plus clair et lucide.

**Merci beaucoup pour cette interview.**

Par Théo Merenciano



# TOP 5 MEILLEURS HACKEURS

Par Théo Merenciano



5

## KEVIN POULSEN

Dans les années 80 une station de radio organise un jeu concours dans lequel le prix à gagner est une Porsche. Kevin Poulsen va donc pirater toutes les lignes téléphoniques et gagner le prix. Il sera arrêté par le FBI en avril 1991 où il passera 4 ans et 3 mois en prison.

4

## ADRIAN LAMO

Ce hacker s'est fait connaître pour avoir introduit plusieurs réseaux informatiques comme Microsoft, Yahoo! et New York Times. Il est finalement arrêté en 2003.



**3****KEVIN MITNICK**

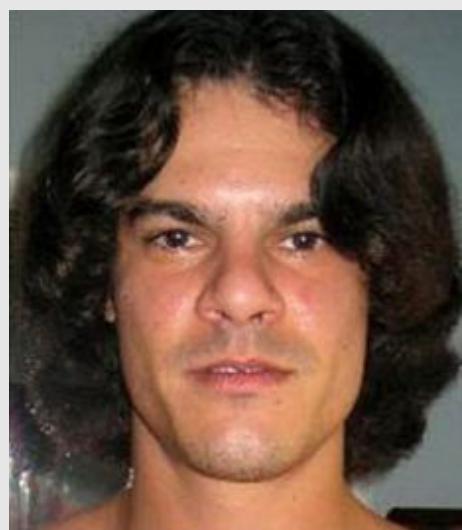
Il est le premier hacker à figurer sur la liste des 10 criminels les plus recherchés par le FBI. Il s'est introduit dans les bases de données de Pacific Bell, Fujitsu, Motorola, Nokia et Sun Microsystems. En 1995 il sera condamné à 5 ans de prison.

**2****GARY MCKINNON**

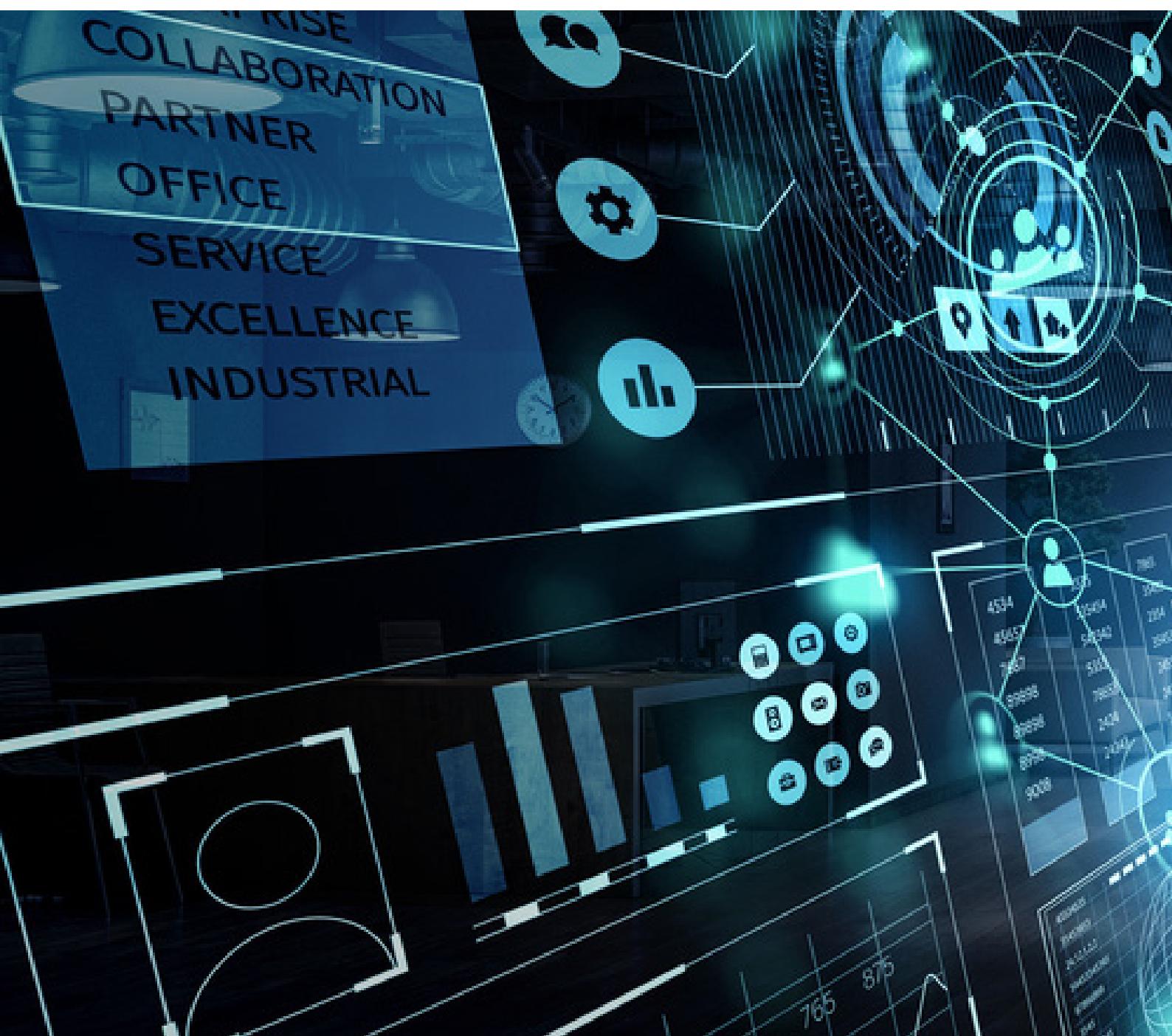
Ce pirate informatique britannique est considéré comme le hacker qui a réussi le "plus grand piratage informatique militaire de tous les temps". Il est en effet accusé d'avoir infiltré 97 ordinateurs appartenant à l'US Army et à la NASA entre 2001 et 2002. Il était fasciné par les OVNI et voulait à tout prix avoir la preuve de leur existence. Si il avait été extradé aux États-Unis il aurait écoper de 70 ans de prison. En 2012 la ministre britannique déclare qu'il ne sera pas extradé en raison de soucis de santé : il souffre en effet du syndrome d'Asperger.

**1****Albert Gonzales**

Entre 2005 et 2007, Albert Gonzales qui était à la tête d'un groupe de hacker a réussi à revendre plus de 170 000 000 numéros de cartes de crédit en installant des logiciels renifleurs sur des réseaux d'entreprises. En 2010 il sera condamné à 20 ans de prison.



# PROTECTION DE DONNÉES PRIVÉES



# Quels sont les outils des cybercriminels ?

Pour commencer, il faut savoir qu'il n'y a que 3 moyens pour porter atteinte à votre ordinateur personnel



# LES ATTAQUES DIRECTES

C'est la plus simple des attaques. Le hacker attaque directement sa victime à partir de son ordinateur. La plupart des «script kiddies» utilisent cette technique. En effet, les programmes de hack qu'ils utilisent ne sont que faiblement paramétrables, et un grand nombre de ces logiciels envoient directement les paquets à la victime.

# LES ATTAQUES INDIRECTES PAR REBOND

Cette attaque est très prisée des hackers. En effet, le rebond a deux avantages :

- Masquer l'identité (l'adresse IP) du hacker.
- Éventuellement, utiliser les ressources de l'ordinateur intermédiaire car il est plus puissant (CPU, bande passante...) pour attaquer. Le principe en lui-même, est simple : Les paquets d'attaque sont envoyés à l'ordinateur intermédiaire, qui répercute l'attaque vers la victime. D'où le terme de rebond.

# LES ATTAQUES INDIRECTES PAR RÉPONSES

Cette attaque est un dérivé de l'attaque par rebond. Elle offre les même avantages, du point de vue du hacker. Mais au lieu d'envoyer une attaque à l'ordinateur intermédiaire pour qu'il la répercute, l'attaquant va lui envoyer une requête. Et c'est cette réponse à la requête qui va être envoyée à l'ordinateur victime.



Ces explications introduisent le sujet globalement. Mais, malheureusement, les hackers sont très inventifs sur la manière de vous faire du mal. Une multitude d'attaques peuvent être menées par des pirates informatiques pour infecter votre système. Voici un tour d'horizon non exhaustif des différentes attaques informatiques actuelles.

## Le crypto jacking, minage de cryptomonnaie malveillant

Quand vous installez un logiciel suspect, il s'y cache pour la plupart du temps des petits logiciels de crypto jacking. Ces logiciels consistent à miner une monnaie virtuelle appelée Bitcoin en arrière-plan sans que vous ne vous en apercevez. C'est pour cela qu'il faut faire attention si votre ordinateur paraît lent après l'installation d'un ou de plusieurs logiciels, c'est probablement dû à un logiciel de crypto jacking.

## Les ransomwares

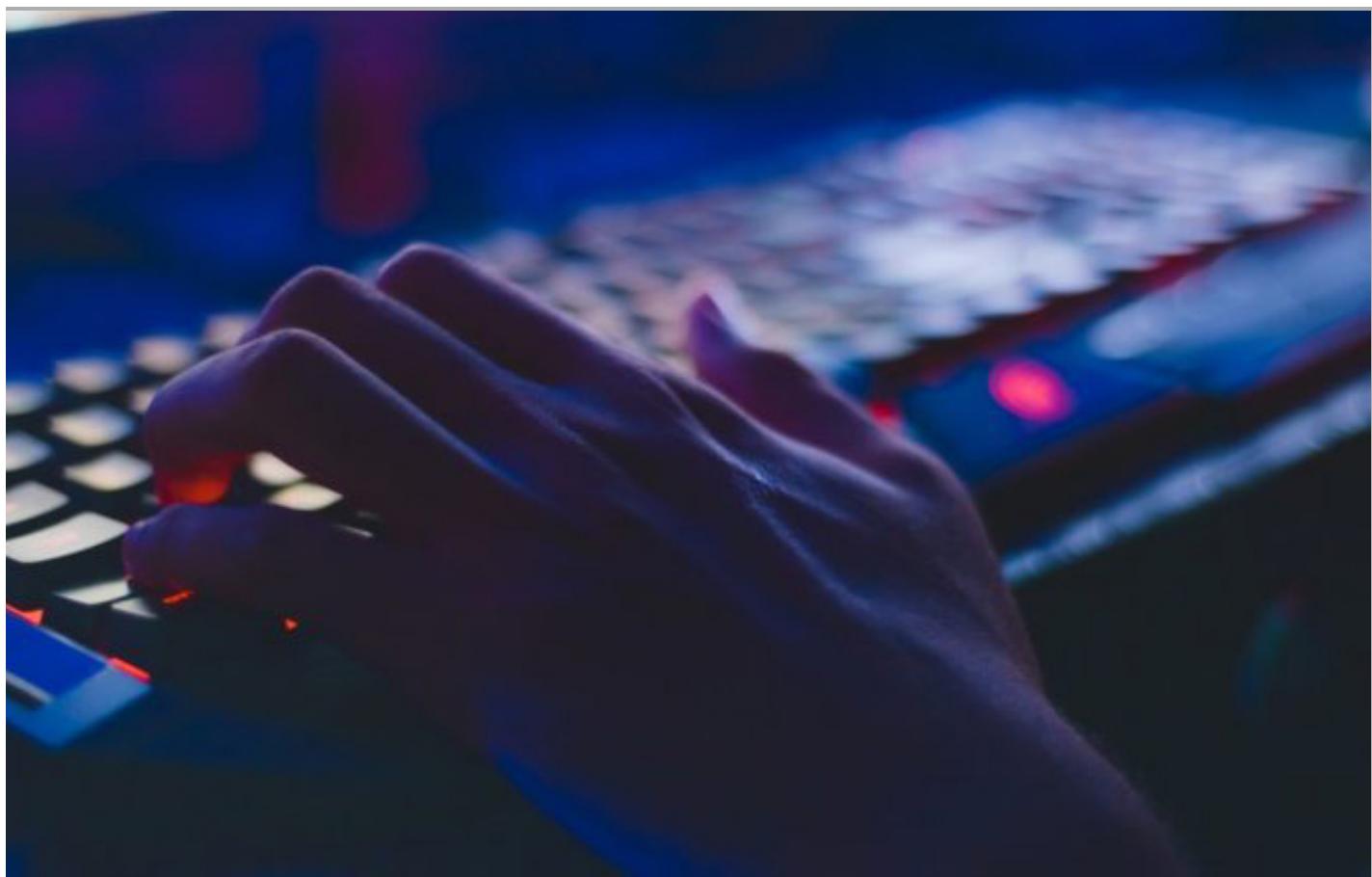
C'est un procédé bien plus vicieux, qui fait bien plus de dégâts que le crypto jacking. Un personne mal intentionnée s'introduit dans l'ordinateur de sa victime et en prend son contrôle. Après cela, il demande une rançon à sa victime pour qu'elle puisse récupérer le contrôle de son ordinateur. Malheureusement cette pratique se répand de plus en plus. Mais un article entier y a été dédié page 6 n'hésitez pas à le consulter.

## Les intrusions sur les objets connectés

De plus en plus de personnes se procurent des objets connectés : montres, assistants vocaux, dispositifs d'éclairage ou de sécurité... Les entreprises redoublent d'effort pour garantir la sécurité sur ces appareils, car ils sont souvent la cible des pirates. À cause du fait que toutes ces technologies sont récentes, les pare-feux sont confrontés à des failles qui peuvent être exploitées par des personnes mal intentionnées.

## Les scripts intersites ou cross-site scripting

Les navigateurs ont eux aussi des failles, les scripts intersites les exploitent. En injectant du contenu dans une page, un pirate peut ainsi modifier la page web selon ses envies et voler des informations grâce aux cookies.



## Les logiciels malveillants sur mobile

La mobile a dépassé en temps d'utilisation la télévision, les hacker l'ont bien compris et certains pirates se sont spécialisés de ce type d'attaque. Ils utilisent des failles que certains fabricants ont laissés sur le système de leur téléphone. Mais il n'y a pas besoin de s'inquiéter, il existe des entreprises spécialisées dans ce domaine qui prendront plaisir à résoudre les problèmes causés par ces failles.

## L'hameçonnage

Ce sont ces fameuses fenêtre pop-up qui s'affichent quand vous naviguez sur internet vous proposant des objets coûteux pour une valeur dérisoire. Ou bien des faux mails vous demandant vos identifiants de banque pour pouvoir vous vider votre compte bancaire. Beaucoup de personnes aujourd'hui se font encore hameçonner cette manière. Notamment les personnes qui utilisent internet peu fréquemment et qui ne sont donc pas habitué à voir ce genre de pratique. C'est pour cela qu'il faut faire de la prévention et informer les utilisateurs non aguerris. Par exemple, votre grand-mère qui n'utilise son ordinateur uniquement pour consulter ses nouveaux mails ou bien votre petit frère de six ans qui quand ses parents ont le dos tourné navigue librement sur internet et devient vulnérable face à l'hameçonnage.

## Les attaques contre les espaces de stockage cloud

Beaucoup de particuliers et d'entreprises ont abandonné le stockage traditionnel au profit du cloud computing, accessible partout. Les pirates informatiques ont trouvé des failles pour voler des clés de chiffrement et ainsi accéder à des informations sensibles et autres données confidentielles. Pour contrer ce fléau, il est conseillé d'investir dans un système de chiffrement sécurisé, fourni par un prestataire de confiance afin de protéger les données de votre société.

Par Léo Marques

# PROTECTION : COMMENT LES ENTREPRISES ÉVITENT-ELLES UNE CYBERATTAQUE ?

De nos jours, les attaques informatiques ont tendance à se multiplier et à être de plus en plus dangereuses. Comment éviter que toute l'informatique de son entreprise ne tombe en ruine ? Ne vous inquiétez pas, il existe beaucoup de solutions.

**Pour commencer : il est primordial de contrôler l'accès internet de son entreprise.**



Chaque point d'accès Internet de l'entreprise, qu'il soit au siège ou dans chaque site distant, est potentiellement un passage que va emprunter un pirate pour accéder au système informatique de l'entreprise. Pour éviter les attaques, il convient de privilégier une approche de réseau sécurisé privé virtuel (VPN) avec une sortie Internet elle aussi sécurisée unique en cœur de réseau. Il est aussi impensable de ne pas sécuriser les bornes Wifis sur le site de l'entreprise. Selon la portée de la borne, un point d'entrée non protégé peut même être accessible depuis l'extérieur des locaux. Plusieurs solutions existent comme l'entreprise zscaler qui propose des protections pour les points d'accès WIFI.

De plus, aujourd'hui, il serait difficile d'interdire aux salariés de surfer sur le Web. Cependant, avec des listes de sites malveillants régulièrement mises à jour, il est possible avec un pare-feu de bloquer les sites qui peuvent réellement vous nuire.



## Les sauvegardes de données sont elles aussi indispensables.

En cas de défaillance du système d'information, la possibilité de restaurer des données permet de préserver l'activité de votre entreprise. En faisant régulièrement des sauvegardes votre matériel informatique sera hors d'atteinte des fameux "ransomware". L'entreprise pourra en effet, poursuivre son activité en récupérant les données sauvegardées et bien sûr mises à jour régulièrement. Mais il ne faut pas oublier que les sauvegardes doivent être stockées à l'extérieur de votre entreprise sinon elles seront inefficaces.

Attention ! Dans le paragraphe précédent, il n'est pas question de sauvegarde par Cloud personnel. Malheureusement, les employés ont de plus en plus recours à ces services. Il vous faut en tant qu'entreprise lutter contre ces pratiques, car c'est un vrai problème de sécurité. En effet, les entreprises n'ont aucun moyen de contrôle quant aux fichiers que le salarié y dépose, aucun moyen de savoir s'il ne place pas ces informations en accès public. Bien souvent, ces plateformes sont hébergées aux États-Unis, ce qui pose potentiellement un risque juridique s'il s'agit de données nominatives.

## Pour finir : bien veiller à former le personnel de votre entreprise à la sécurité informatique.

La première contre-mesure, c'est de responsabiliser le personnel. Il faut indiquer au personnel quels sont les bons comportements à tenir face aux menaces de ce type, face à une clef USB que l'on trouve dans la rue, etc. Des règles de comportement simples permettent de déjouer bien des attaques. La plupart du temps, les pirates informatiques ont recours à l'ingénierie sociale, car elle est bien souvent plus efficace qu'une cyberattaque. En effet, il suffit qu'un e-mail douteux fonctionne sur une personne dans l'entreprise et malheureusement, c'est toute celle-ci qui sera en danger. Si être informé sur ces pratiques malfaisantes ne suffit pas pour garantir une sécurité optimale, certains antivirus peuvent analyser les mails douteux et donc offrir une double protection contre ce genre de piratage.

Par Léo Marques

# 3 CYBERATTAQUES HORS NORMES

**#3 Carbanak** : Le Carbanak, aussi appelé le braquage du siècle, aurait rapporté plus d'1 milliard de dollars en visant plus d'une douzaine de banques à travers le monde. Encore une fois, le virus a infiltré les systèmes en se cachant dans les pièces jointes de mails. Mais ce braquage fut long et on estime qu'il aurait fallu environ 4 mois pour mener chaque opération à bien. Les pays les plus touchés ont été la Russie et les États-Unis.

**#2 Le ver Stuxnet** : Ce ver informatique avait pour cible le programme nucléaire iranien et a réussi à s'infiltrer dans les appareils non seulement protégés, mais en plus déconnectés du réseau. Une fois avoir infesté les machines visées, ce virus a détruit les centrifugeuses nécessaires pour la création d'uranium. Et sans uranium, pas de nucléaire. Le ver Stuxnet aura réussi à retarder le développement du programme nucléaire de 2 ans.

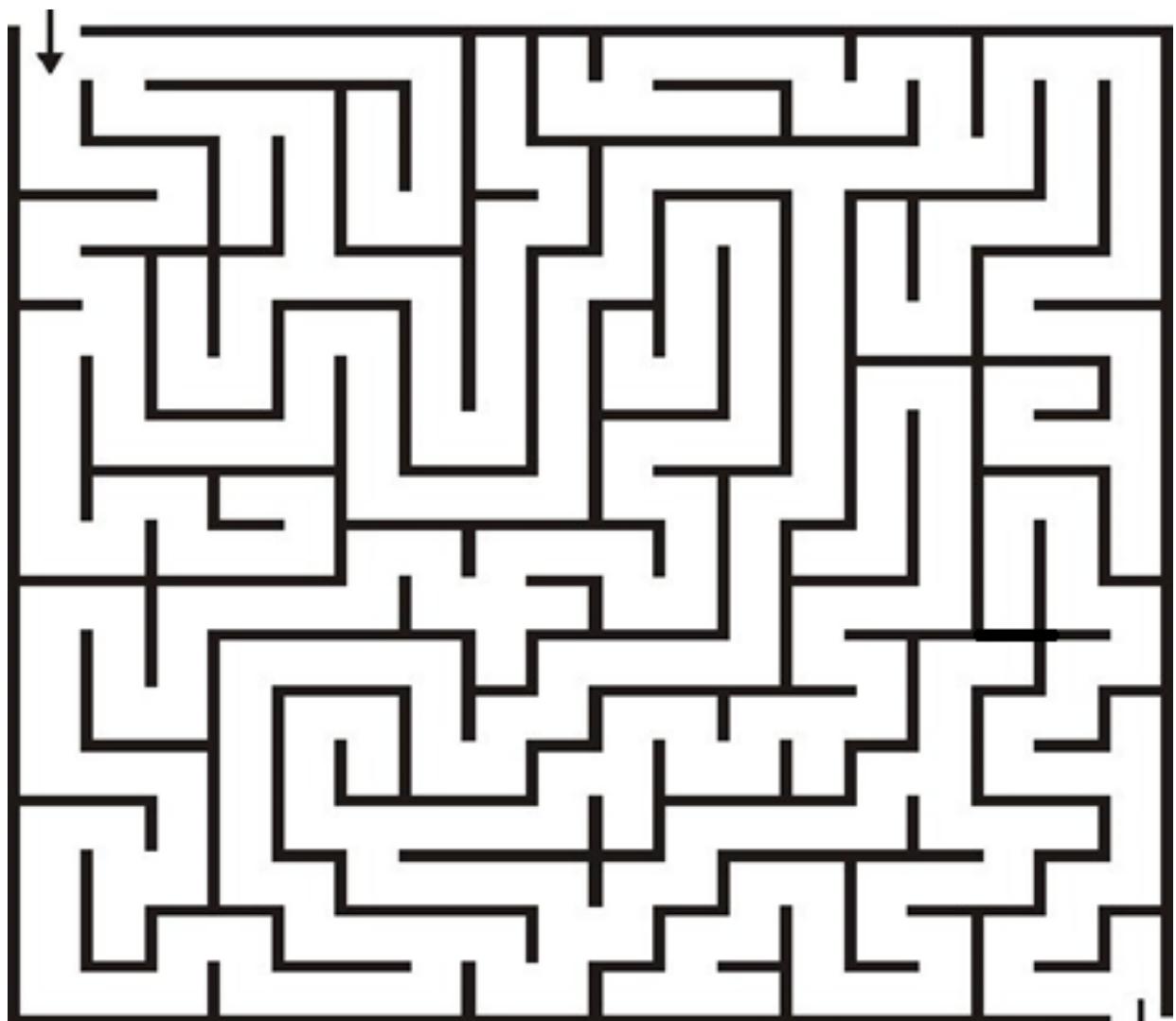
**#1 WanaCry** : Il s'agit d'un virus qui a beaucoup fait parler de lui en 2017. Il aurait fait plus de 300 000 victimes dans 150 pays différents. C'est un virus qui fonctionne comme un Ransomware. On estime que ce piratage aurait rapporté jusqu'ici 70 000\$.

Par Camélia Zahí

# JEU

## Le labyrinthe

Aide la police à retrouver le hacker avant qu'il ne soit trop tard !





evian  
Natural Spring Water



evian  
NATURAL SPRING WATER

