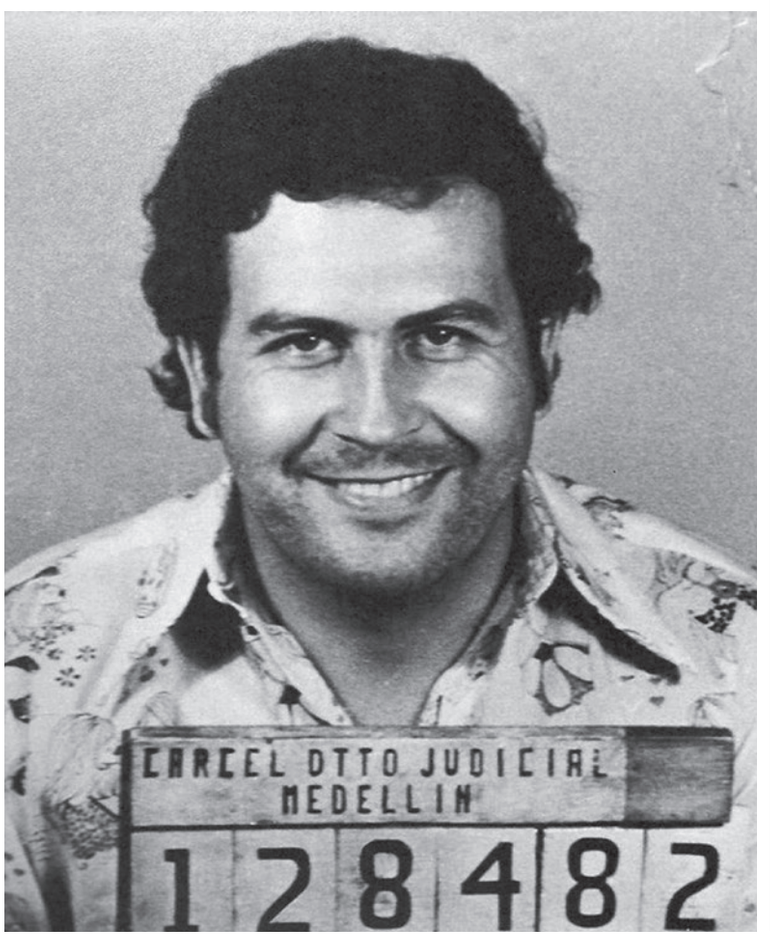
LE 44e VIRUS INFORMATIQUE

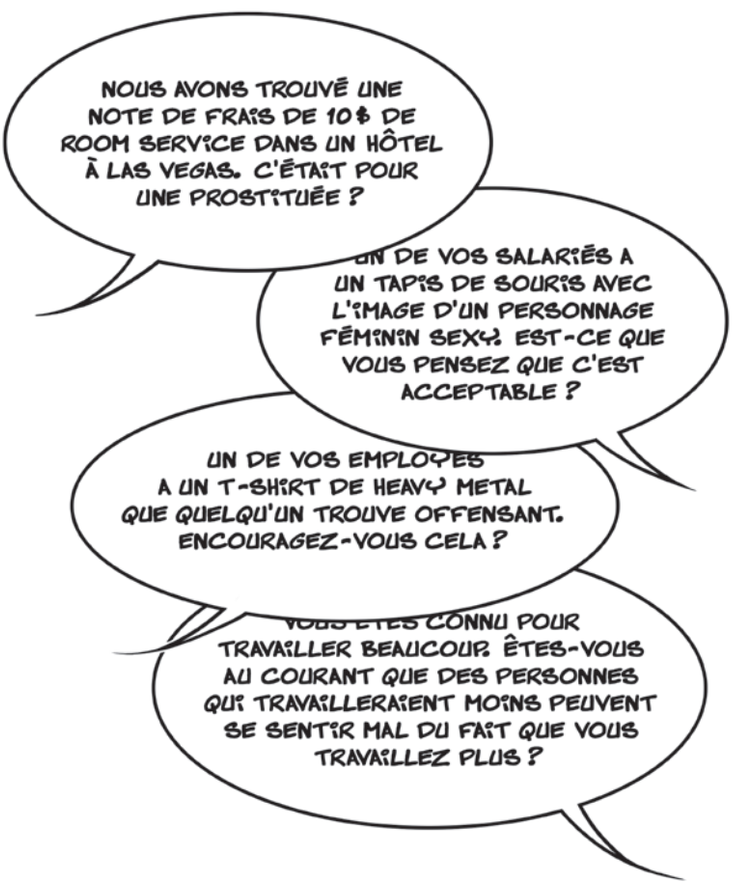
0 % de publicité !

De la came au scam : le stupéfiant nouveau business d'Escobar inc.



Affaire Quantic Dream : révélations !

Ce que Canard PC, Le Monde et Mediapart vous ont caché lors de leurs enquêtes contre la société de jeux vidéo



Hacking : les secrets des stations-service auto

Le Virus Informatique est édité par :

ACBM (OÜ)

Narva mnt 5
10117 Tallinn
Estonie
Tél. : +(372) 57554992
www.acbm.com
Société à responsabilité limitée
au capital de 2.500 €
Reg. : 12973311

La rédaction regrette de ne pas pouvoir répondre par téléphone aux demandes individuelles, mais pourra éventuellement traiter vos informations dans un prochain numéro si vous lui envoyez un dossier complet.

Directeur de la publication
Rédacteur en chef
Olivier Aichelbaum

Rédacteurs
Pas de Bill,
Patrick Gueulle,
Nick Larsen,
RayXamber, etc.

Illustrateurs
Bruno Bellamy,
Filip Škoda

Mise en page
J.-C. Lenormand
www.image-et-net.com

Dépôt légal :
2e trimestre 2020

Retrouvez-nous sur :

www.acbm.com
twitter.acbm.com
facebook.acbm.com
diaspora.acbm.com
mastodon.acbm.com
video.acbm.com

pour des informations inédites !

Édito : Des masques vont tomber

Il ne vous aura pas échappé que nous avons vécu, et vivrons encore pendant quelque temps encore, une période particulière. Nous espérons que vous et vos proches arrivez à la passer aussi bien que possible (beaucoup de nos lecteurs sont des retraités, parmi les plus menacés donc) : la vie et la santé d'abord ! Ce qui suit est secondaire. Le coronavirus SARS-CoV-2 a mis une partie de la planète quasiment à l'arrêt : salons annulés, annonces et lancements reportés, magasins fermés… L'actualité de l'informatique et des sujets connexes a été bien moins chargée ces dernières semaines et, du coup, nous aurons moins de choses, dans ce numéro, à vous raconter avec notre regard décalé. Espérons que tout rentre bientôt dans l'ordre et, d'ici là, portez vos masques !

Nous avons profité de cette période pour réaliser une grosse enquête. Il y a un peu plus de deux ans, des journalistes de trois médias (*Canard PC*, *Le Monde* et *Mediapart*) ont réalisé ensemble un lot d'articles, duquel il ressortait que la société française de jeux vidéo Quantic Dream était coupable d'une culture toxique en interne. L'information a fait le tour de la planète, de plus en plus déformée. Les rares voix discordantes, et qui pourtant avaient vécu les choses de l'intérieur, ont été lynchées virtuellement sur les réseaux sociaux. Nous avons décidé de mener une contre-enquête pour comprendre. Et, bien que nos moyens humains et financiers soient ridicules comparés à ceux des trois médias précités, nous avons fait plusieurs découvertes stupéfiantes dont ils n'avaient pas parlées. Là, ce sont des masques qui vont tomber. L'article est long, le plus long que nous n'avons jamais publié, mais il devrait rester digeste, car il est composé d'une multitude d'affaires différentes dans des thématiques différentes, à lire comme autant d'articles plus courts.

Bonne lecture !

Sommaire

Édito : Des masques vont tomber 2
Nous avons informé GoDaddy d'une grave faille de sécurité, la société nous a envoyés balader. 3
Actualité : plein d'infos révoltantes ou rigolotes. 4
Rappels à la pelle, attention matériels dangereux ! 8
Piqûre de rappel sur le codage numérique pour l'AFP 9
La culture toxique chez Quantic Dream : une intoxication de la part de médias ? 11
Les secrets des cartes de stations-service 22
De la came au scam : le stupéfiant nouveau business d'Escobar. 28
Bande dessinée. 31
Publicité super intéressante à lire ! 32

La rubrique du courrier des lecteurs reviendra dans le prochain numéro. N'hésitez pas à nous envoyer vos informations, vos témoignages, vos coups de gueule, vos astuces, vos idées de génie et autres !

Copiez et diffusez-moi !

À titre exceptionnel (exceptionnel, nous insistons sur ce point), grâce au financement préalable par ses lecteurs, ce numéro est sous licence de libre diffusion. Vous pouvez le diffuser à condition de mentionner la source (*Le Virus Informatique*, acbm.com), de ne pas modifier le contenu ni d'en faire un usage commercial (Licence Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License, plus de détails sur creativecommons.org/¬licenses/by-nc-nd/4.0/¬deed.fr). Exception : les codes sources sont, eux, modifiables. À noter : le passage sous licence de libre diffusion ne concerne que notre travail, certains éléments (comme certaines captures d'écran Web utilisées en guise d'illustration, par exemple) restent protégés par le droit d'auteur classique. Pour les autres numéros, nous ne pouvons pas passer sous licence de libre diffusion : n'oubliez pas que nous ne pourrons continuer d'enquêter que si nos ventes sont suffisantes. Les ventes en kiosques de ce numéro 44 permettront, nous l'espérons, de financer le numéro 46.

Merci !

Comme si la situation avec le coronavirus n'était déjà pas assez compliquée, Presstalis, notre distributeur pour la France et l'export vers tous les autres pays a fait faillite, nous privant de plusieurs mois de revenus y compris ceux pour les frais d'impression que nous devons payer (c'est notre distributeur qui collecte notre part des ventes chez les marchands de journaux et nous la reverse). Nous avons lancé un appel sur Ulule pour que nos lecteurs nous aident à financer ce numéro, ils ont réussi : merci à eux, ainsi qu'à ceux qui ont relayé notre appel au secours ! Par contre, il est impératif que vous restiez en contact avec nous si vous voulez être informés concernant le prochain numéro (lire p. 21), car il pourrait ne sortir que sous version téléchargeable, même si nous ferons notre maximum pour une sortie en kiosques.

Nous avons informé GoDaddy d'une grave faille de sécurité, la société nous a envoyés balader

En février, Micka Letatek Tuxun, un lecteur, nous alertait d'un étrange problème sur notre site Web : s'il y accédait directement en tapant acbm.com dans la barre de navigation, tout se passait bien. Mais s'il tapait cette requête dans Google, il tombait sur le site Web d'une pharmacie en ligne (dont les produits, sans doute des contrefaçons, auraient pu s'avérer dangereux pour la santé).

Nous n'avions pas constaté ce problème nous-mêmes, car nous ne passons pas pour Google pour nous connecter sur notre propre site Web. Après un moment d'incrédulité, nous avons enquêté et rapidement trouvé l'origine du problème : le fichier de configuration *.htaccess* de notre site Web avait été modifié à notre insu. Le *referer* (site de provenance) était analysé et, s'il s'agissait de Google (ou Yahoo, MSN, AOL ou Bing), notre visiteur était redirigé vers des pages écrites en *PHP* stockées dans des fichiers non créés par nous, mais stockés par un tiers inconnu « chez nous ».

Notre site Web est chez GoDaddy, il s'agit d'un hébergement mutualisé dans un répertoire à côté d'autres utilisateurs sur une même machine. Les avantages pour nous sont une économie (au moment où nous avions signé le contrat, plus vraiment de nos jours) ainsi qu'un gain de temps puisque toutes les mises à jour de sécurité pour combler les failles des logiciels doivent être faites par GoDaddy (en théorie…). En 2017, déjà, notre site Web avait été victime de l'attaque d'un ver écrit en langage *PHP*. De nombreuses pages avaient été, là encore, créées pour commercialiser des produits plus ou moins illicites. Ce ver avait probablement profité d'un problème de configuration dans le répertoire d'un autre utilisateur hébergé sur le même serveur, voire de la configuration du serveur lui-même. Heureusement, ces pages « pirates » n'étaient pas accessibles depuis celles que nous avons proposées, mais depuis d'autres sites Web victimes du même ver ; nos lecteurs n'ont donc pas dû tomber dessus. Nous n'utilisons que des pages statiques en HTML pur sur notre site Web, c'est plus sûr qu'un site écrit en *PHP* où chaque page est recréée à la volée pour le visiteur. À en croire différents forums, ce genre de problème a déjà été signalé à GoDaddy à maintes reprises, mais la société rejette la faute sur ses clients (cela nous arrivera aussi, ainsi que nous allons le raconter dans un instant).

Une astuce maison

Malheureusement, il n'y a pas de moyen de bloquer *PHP* chez notre hébergeur GoDaddy. Nous avons donc dû ruser, ainsi qu'expliqué dans *Virus Info* 42 : nous avons modifié le fichier *.htaccess* pour que tous les fichiers en *PHP* soient renvoyés vers une page inoffensive. Bien nous en a pris, puisque nous avons évité ainsi une nouvelle attaque en février 2018, sans conséquence cette fois. Mais, lors de l'attaque constatée début 2020, le fichier *.htaccess* avait été modifié pour faire sauter notre « protection ». *A priori*, il s'agissait donc d'une modification manuelle et non d'un ver. Cette fois, les fichiers *PHP* dataient, notamment, de novembre et décembre 2019.

Alertée, GoDaddy nous a répondu que nous sommes responsables de la sécurité de notre hébergement ; quand bien même, ici, le problème n'est pas dans notre périmètre technique ! Elle nous a redirigés, de manière totalement hors sujet, vers un texte pour choisir un bon mot de passe FTP. Non seulement nous n'utilisons pas FTP, car le mot de passe circule en clair sur le réseau et pourrait être « écouté » (GoDaddy devrait avoir honte d'utiliser cela encore en 2020), mais pis : la société impose que ce mot de passe soit le même pour les connexions chiffrées en *ssh* (service que nous utilisons exclusivement). Notre mot de passe est compliqué afin d'empêcher des attaques par dictionnaires ou force brute (toutes les possibilités), et nous ne le saisissons que sur des machines sécurisées (comprendre « pas sous *Windows* »). Au passage, la recommandation de GoDaddy nous incite à penser qu'elle n'a pas installé de compteurs de tentatives erronées de saisie de mot de passe, ce qui serait dommageable pour la sécurité de ses clients et contraire aux règles élémentaires.

En cherchant d'autres serveurs Web hébergés sur la même machine, nous avons découvert que nous n'étions pas les seuls concernés par l'attaque. L'explication la plus logique pour nous était que quelqu'un a réussi à avoir des droits d'administration de plusieurs clients hébergés du fait d'une faille quelque part sur cette

Les certificats SSL permettent de sécuriser en les chiffrant les visites d'internautes sur votre site Web. Google veut récompenser leur usage en sanctionnant le référencement de sites Web qui n'en ont pas. Malheureusement, GoDaddy n'accepte pas dans ses formules d'hébergement « économiques » les certificats émis gratuitement par Let's Encrypt. Ne croyez pas que GoDaddy souhaite réduire votre sécurité. Elle souhaite surtout vous vendre sa propre solution (à partir de 70 € par an au prix normal).

machine, voire ailleurs dans l'architecture de GoDaddy.

GoDaddy réduit la sécurité pour… vendre plus

Par précaution, nous avons demandé à GoDaddy de désactiver totalement FTP et *PHP* de notre compte, mais la société refuse. Si nous voulons moins de services, la société nous dit qu'il nous faut souscrire un hébergement… plus cher!
Trois mois ont passé, GoDaddy ne montrant pas la moindre curiosité pour les preuves que nous avons mises de côté pour elle, des fichiers avec leur horodatage pour faire des recherches dans les *logs*. Mais, début mai dans la presse, on apprend que GoDaddy a émis une alerte: les mots de passe *ssh* de clients du service Deluxe Hosting (celui que nous avons choisi) ont été compromis en raison d'un problème de sécurité dans son système. Faute de détails, nous pouvons craindre que les mots de passe eussent été stockés en clair. L'attaque aurait eu lieu en octobre 2019, mais n'a été repérée que dernièrement. Ce qui semble confirmer notre propre alerte qu'elle a ignorée! La société dit qu'elle va offrir aux victimes un an de protection gratuite contre les *malwares* et d'autres attaques. Au-delà de cette année, ce service deviendra payant. Bref, au lieu de se protéger elle-même, la société fait le *forcing* pour que les clients payent une protection contre ses failles à elle!
GoDaddy reconnaît 28 000 *webmasters* victimes de l'attaque. Un courriel leur a été envoyé et leurs mots de passe ont été changés. Nous n'avons pas reçu ce courriel et notre mot de passe n'a pas été changé par la société, il est donc probable qu'elle n'a pas encore compris l'étendue du problème (l'alerte a été donnée en Amérique, alors que nous sommes dans son centre serveur du Sud-est asiatique). En outre, elle affirme ne pas avoir constaté de modifications de données par le ou les pirates pour le moment, alors que nous lui avons notifié de tels incidents. À moins qu'il ne s'agisse, encore, d'un autre piratage? ■

```
RewriteEngine On
RewriteBase /
RewriteCond %{HTTP_USER_AGENT} (google|yahoo|msn|aol|bing) [OR]
RewriteCond %{HTTP_REFERER} (google|yahoo|msn|aol|bing)
RewriteRule . futures-befouled.php [L]
```

Le code rajouté par les pirates au début de notre fichier .htaccess

La page pirate qui a remplacé notre site Web

Le désordre des soldes

Il y a tout juste un an, nous avions épinglé Epic qui annonçait des soldes, hors période légale de soldes et pour des produits au stock illimité (en téléchargement) ne pouvant être soldés. Cela ne manque pas de piquant, mais la société récidive avec un communiqué annonçant « *le retour des Méga Soldes Epic Games sur l'Epic Games Store avec quatre semaines d'offres* » à compter du 14 mai. Nacon fait de même en nous annonçant des « *soldes monstres* […] *Les soldes « Skulls for the Skull Throne* 4 » [qui] *se déroulent du 28 mai au 2 juin 2020.* » Malheureusement, les communiqués de presse défectueux ne sont toujours ni repris ni échangés.

Nouvelle tromperie, il n'y a pas photo

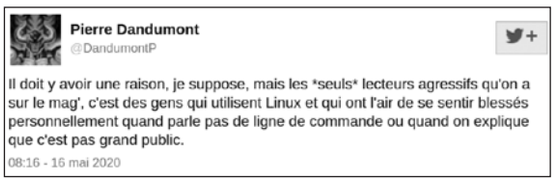
Huawei avait déjà été prise sur le fait de tromper le public en affirmant qu'une photographie avait été prise avec un de ses *smartphones*, le P9, alors qu'elle l'avait été, en réalité, avec un appareil de photo de type reflex (lire *Virus Info* 29). Malgré la mauvaise image pour… la marque suite à cet incident, l'histoire s'est répétée en 2018 avec le modèle Nova 3 (lire *Virus Info* 37), puis en 2019 avec les P30/P30 Pro. La leçon n'a toujours pas servi: 2020 a son scandale aussi. Pour annoncer un concours photo sur le réseau social Weibo, Huawei a utilisé un cliché de coucher de soleil avec la légende « *pris par un* smartphone *Huawei* ». Huapeng Zhao a reconnu cette photographie de Su Tie qu'il avait vue sur 500pix, un site Web permettant de partager de telles œuvres. Sur la fiche associée, il est indiqué que l'image a été capturée par un Nikon D850, un appareil photo à 3000 dollars. Huawei a plaidé l'erreur et présenté ses excuses. Rendez-vous l'année prochaine pour un autre scandale!

La photo originale et celle utilisée par Huawei

Xiaomi fabrique des *smartphones* sous *Android*. On aurait pu imaginer que Lei Jun, son p.-d.g., utilise un appareil de la marque, voire (encore mieux) un prototype d'un appareil à venir. Eh non: il a posté sur le réseau social Weibo depuis… un iPhone! Un accident sans doute, l'interface maison *MIUI* 6 ressemblant tellement à celle d'*iOS*.

Crazy Taxidermiste

Demiurge Studios, rachetée par Sega en 2015, a décidé de reprendre son indépendance. Les deux sociétés se servent de cette excuse pour empailler les jeux mobiles *SEGA Heroes* et *Crazy Taxi Tycoon* (ex-*Crazy Taxi Gazillionaire*). Seuls les achats de contenus *in app* réalisés avant le 17 mars dans le premier titre peuvent être remboursés, au terme d'une procédure plutôt complexe auprès de la boutique de téléchargement. Pour le second, disons que vous venez de vous faire arnaquer dans un jeu vidéo de taxi, du coup c'est encore plus réaliste!



Nous ne cautionnons en rien l'agressivité, mais nous pouvons comprendre la colère de « Linuxiens » face à la désinformation proférée par cet adorateur de *Microsoft Windows*, rédacteur en chef de *Canard PC Hardware*. Car nous ne sommes plus dans les années 1990. Sur PC, il existe des distributions de *Linux* faciles à utiliser (citons *Ubuntu*), et elles sont même plus faciles/rapides à installer et à mettre à jour que *Windows* généralement. En outre, *Linux* est le système d'exploitation le plus utilisé de la planète : il est utilisé par les possesseurs de plus d'un milliard de téléphones sous *Android*, une surcouche. Grand public, donc. Notre confrère devrait demander conseil à Madame Michu.

Un répéteur Wi-Fi vendu chez Amazon. À la louche, on dira qu'il y a au moins un problème dans l'image.

Y a-t-il un pilote à jour dans l'avion ?

En 2015, les autorités états-uniennes de l'aviation alertaient les compagnies aériennes : le Boeing 787 Dreamliner devait être redémarré tous les 248 jours pour contourner un bogue pouvant entraîner une coupure de courant généralisée dont on peut imaginer les conséquences en vol. Cette fois, elles ont annoncé qu'il faut éteindre et rallumer ces mêmes avions tous les 51 jours pour éviter des problèmes informatiques catastrophiques en raison d'une mémoire saturée de données sinon. Mesdames et Messieurs, veuillez regagner vos places et attacher vos ceintures de sécurité, nous allons bientôt rebouter !

En bref

Selon une étude de GameRefinery, le type de jeux les plus populaires sur *iOS* et générant 21 % des revenus aux États-Unis sont les jeux de *match-3* (où il faut aligner trois symboles identiques). Probablement joués par les joueurs les plus impatients d'avoir le prochain modèle d'iPhone, encore plus puissant.

Huawei intègre le moteur de recherche Qwant dans ses nouveaux téléphones, se félicite Qwant, Google étant impossible par sanctions états-uniennes contre Huawei. Vu que Qwant utilise Bing de Microsoft et que Microsoft n'a pas plus le droit de travailler avec Huawei, on se demande si Qwant ne risque pas d'être privée de Bing. Et, donc, de ne plus fonctionner.

YouTube annonce supprimer les vidéos complotistes mêlant 5G et coronavirus. Ouf, les auteurs de vidéos complotistes au sujet de la 4G, des compteurs Linky et autre du même acabit peuvent dormir tranquilles !

La régie publicitaire Awin a avalé son concurrent Affilinet. La plate-forme de cette dernière a été désactivée fin 2019. Les éditeurs de sites Web qui affichaient ses publicités ont été payés, sauf si la facture en attente faisait moins de 10 €, et ce, alors que rien de tel n'était prévu dans le contrat. Chez Awin, le gagnant-gagnant est devenu du gagnant-perdant.

Incitant à passer à la v2, Philips a arrêté les services en ligne de son Hue Bridge v1, il n'est donc plus possible de contrôler avec ses ampoules à distance. Pour maintenir le service actif, ses informaticiens avaient peur d'avoir des ampoules aux doigts ?

Alors qu'elle n'était encore qu'un projet, l'application *StopCovid* (alertant qu'on a croisé des personnes ayant attrapé le Covid-19) a tellement fait parler d'elle en France que, dès avril, des internautes ont voulu la télécharger sur leurs *smartphones.* L'outil géorgien similaire et de même nom s'est ainsi retrouvé dans le hit-parade des applications les plus téléchargées dans l'Hexagone. Trop viral à notre goût, Bluetooth pouvant causer des problèmes de sécurité informatique.

Pour protéger votre vie privée, nous vous déconseillons les enceintes connectées. Mais certains médias comme *Frandroid* vous recommandent de « bons plans » sur ces produits. Sachant qu'ils touchent une commission sur les ventes avec de tels articles, le bon plan est surtout pour eux : c'est votre vie privée qui est offerte en pâture aux GAFAM, pas la leur !

Une clé USB « anti-5G » baptisée 5GBioShield a été mise sur le marché (339 livres, soit environ 380 €) pour protéger des ondes dangereuses pour la santé. Elle fonctionne grâce à une « *technologie de catalyseur holographique quantique* » (si vous ne comprenez pas, c'est que vous êtes nul en informatique). Pen Test Partners a analysé l'objet : il s'agit en réalité d'une antique clé mémoire de 128 Mo (méga, vous avez bien lu) avec une LED au bout. Dans un rapport, un membre du conseil municipal de Glastonbury (Royaume-Uni) déclarait pourtant « *utiliser ce dispositif et le trouver utile.* » Mais l'histoire ne dit pas où il l'a « plugué ».

On ne vend qu'aux riches

Pendant que vous étiez confinés, Apple a lancé un iPhone SE. Pourquoi faire simple quand on peut faire compliqué : derrière ce nom identique à un appareil de 2016, on trouve dans un boitier semblable à un iPhone 8 des composants d'un iPhone 11 privé de ses derniers « gadgets ». Prix de référence aux États-Unis : 400 dollars (hors taxes) en version 64 Go. Ce prix varie ensuite selon les pays. Au Japon, cet iPhone SE est facturé au même moment l'équivalent de 416 dollars. Aux Philippines, le même modèle est vendu 521 dollars. Pour le modèle équipé de 256 Go, on passe de 563 dollars au Japon à 718 dollars aux Philippines. Bref, plus vous êtes d'un pays pauvre, plus on met l'étiquette chère pour être sûr que vous n'achetez pas (ce serait mauvais pour l'image de marque).

Se faire roulette chez Apple

Fin 2019, Apple a lancé un nouveau Mac Pro disponible à partir de 6 500 €. De nombreuses options permettent de faire monter la facture jusqu'à près de 45 000 €, dont des roulettes à 480 €. Cela avait fait jaser. Si vous avez des regrets de ne pas avoir commandé ces roulettes au départ, tout n'est pas perdu : Apple a finalement mis en vente un kit. Prix : 850 €. Nous n'osons pas regarder le prix de l'accessoire aux Philippines.

Stripe tease sur le Web à votre insu

Stripe, plate-forme de paiement utilisée par plus de 100 000 sociétés sur le Web (autant dire quasiment incontournable), a été accusée par le développeur Michael Lynch d'enregistrer, en douce, les déplacements de souris de l'utilisateur à l'aide d'un code en *JavaScript*. Pas la peine d'en faire tout un fromage ? La société capte également par ce moyen les adresses d'autres pages visitées ne concernant pourtant pas le paiement et attribue au visiteur un identifiant unique qui permet de le reconnaître sur d'autres sites équipés de Stripe, même si le visiteur n'a jamais utilisé ce service pour payer. Michael Lynch s'en est aperçu en déchiffrant le trafic de données en arrière-plan. En fait, des développeurs tiers s'en étaient inquiétés dans des forums depuis 2017. De notre côté, nous (qui utilisons des bloqueurs de scripts pour des raisons de sécurité) avons constaté que des sites Web divers comme Indiegogo ne s'affichaient pas du tout si le script du service de paiement est bloqué. À croire que la société fait du *forcing* pour vous pister ! Stripe répond que ce comportement est indiqué dans sa documentation technique, qu'il est nécessaire exclusivement pour identifier les robots qui essayeraient de frauder ses partenaires. L'internaute, lui, n'est pas toujours prévenu et, en réalité, Stripe expliquait aussi dans ses conditions d'utilisation que les informations concernant sa navigation peuvent être revendues à des annonceurs publicitaires. Une rédaction ambiguë, selon elle, qu'elle a corrigée dans la foulée. Stripe se paye vraiment notre tête.

Disque dur qui ne dure pas

Dans *Virus Info* 42, nous avions parlé de SSD de HPE qui doivent tomber en panne après 32 768 heures, à moins d'installer un correctif. Le constructeur a lancé une nouvelle alerte, similaire, pour des SSD de type SAS (Serial-Attached SCSI) qui doivent s'arrêter définitivement de fonctionner et perdre les données après 40 000 heures de fonctionnement, soit à partir d'octobre cette année pour les premiers modèles vendus. Un correctif aux *firmwares* *HPD7* et précédents est diffusé pour empêcher ce funeste sort à des composants qui ont pu être vendus seuls ou intégrés à d'autres machines (HPE ProLiant, Synergy, Apollo 4200, Synergy Storage Modules, D3000 Storage Enclosure, StoreEasy 1000 Storage). Dans le détail, il s'agit de SSD de 800 Go ou 1,6 To portant les références EK0800JVYPN, 846430-B21, 846622-001 ; EO1600JVYPP, 846432-B21, 846623-001 ; MK0800JVYPQ, 846434-B21, 846624-001 ; MO1600JVYPR, 846436-B21, 846625-001. Il se trouve que, peu avant, Dell-EMC a alerté d'un problème strictement identique pour les SSD D417 de ses modèles LT0200MO, LT0400MO, LT0800MO, LT1600MO, LT0200WM, LT0400WM, LT0800WM, LT0800RO et LT1600RO. Chez HPE, comme chez Dell-EMT, il semblerait qu'en fait le problème vienne du sous-traitant SanDisk. Là encore, un correctif est à installer de toute urgence, pour ne pas finir… sans disque.

Le marché n'était pas prêt

Dans le précédent numéro, nous avions parlé de plates-formes de placements P2P qui permettent de mettre en relation emprunteurs et investisseurs avec des taux de crédit plus intéressants qu'en passant par des banques. Orca Money se voulait un agrégateur permettant d'investir sur plusieurs de ces plates-formes à la fois. Malheureusement, l'aventure vient de s'arrêter faute d'atteindre les objectifs fixés dans un contexte de défiance du modèle P2P. La société fonctionnait grâce notamment à 575 110 livres sterling qu'elle avait levées en 2018 en échange de 22 % de son capital sur… un site de financement communautaire. Cela prête à rire.

En bref

On craignait le pire à cause du confinement, à force de ne pas bouger (le nombre de pas aurait baissé de 27 %), mais il semblerait que les Français n'aient pris que peu de poids (86 g en moyenne). D'où viennent ces chiffres ? De Withings, un fabricant d'objets connectés qui a relevé les compteurs : ses balances vous ont… balancés !

Un *remake* du jeu vidéo *Mafia* est en approche. C'est là qu'on peut voir que la Mafia, la vraie, n'a pas encore tout compris au monde moderne : elle n'a pas encore porté plainte pour usage de son nom sans autorisation.

Brave est un navigateur Web *open source* qui prétend protéger la vie privée. Il a été pris la main dans le sac par Cryptonator1337 à remplacer certaines adresses souhaitées de sites par des versions sponsorisées rapportant de l'argent à ses développeurs, et ce, à l'insu des utilisateurs. Les braves.

Fujitsu a présenté une nouvelle gamme de PC portables « *optimisés pour le travail à distance* », un argument commercial de poids alors que la pratique s'est développée avec le confinement. Mais, au fait, les PC portables ne sont pas utilisés depuis des décennies pour le travail à distance ?

The Pokémon Company a beau avoir gagné plus de 3 milliards de dollars selon des estimations avec son *Pokémon Go*, elle a décidé de faire des économies et de mettre un terme à *Pokémon Rumble Rush* seulement un an après son lancement mondial. Le 22 juillet, ce jeu pour appareils mobiles ne sera plus téléchargeable ni jouable, et les contenus achetés par les joueurs seront définitivement perdus. Bref, voilà un *Pokémon* qui a évolué en Pièjagogo !

Selon *The Hollywood Reporter*, Netflix a acquis les droits pour faire un film adapté du sublime *Dragon's Lair*, un jeu vidéo sur Laserdisc des années 1980 (lire *Puces Info* 27) à base de séquences de dessin animé. Il sera produit par son créateur Don Bluth. Soyons mauvaises langues : l'interactivité devrait être respectée.

Exercice

Au terme d'un accord avec la justice, Apple va devoir payer en France une amende transactionnelle de 25 millions d'euros pour avoir ralenti artificiellement par le biais de mise à jour des iPhone sans en informer les clients. Aux États-Unis, pour la même affaire, l'accord avec les autorités prévoit entre 310 et 500 millions de dollars. Nous ne connaissons pas le nombre de victimes dans chaque pays, mais il y a 327 millions d'habitants aux États-Unis et 67 millions en France. Si l'on considère des taux de vente équivalents, calculer de combien la France s'est fait avoir.

Kro ou Corona ?

En 2017 déjà, Bill Gates annonçait une pandémie et affirmait « *nous ne sommes pas prêts.* » 2020, le peuple est confiné pour faire face au coronavirus, le télétravail se met en place à vaste échelle. Microsoft Teams tombe en panne en Europe. La société annonce que le nombre d'utilisateurs a été multiplié par sept en une semaine. Bill Gates avait raison : l'Humanité n'était pas prête, Microsoft n'était pas prête.

Trackmania : la bonne ment

Pour son futur *Trackmania* à paraître le 1er juillet, Ubisoft adopte un nouveau modèle économique sur trois niveaux : gratuit mais très limité en termes de contenus, avec un accès « standard » à 10 € par an ou avec un accès « club » à 30 € par an (ou 60 € pour trois ans) pour des contenus additionnels. Des joueurs y voient une forme d'abonnement, alors qu'ils préféreraient acheter le jeu « une fois pour toute » (60 € est un prix courant pour cela). Ce n'est pas l'avis de l'éditeur, pour qui la formule est « *plus comme une licence dans un club de sport. Si vous voulez faire des compétitions ou vous entraîner régulièrement, une fédération aide à organiser les compétitions, maintenir les infrastructures et vous achetez une licence en retour. C'est pareil dans* Trackmania. » Or, en fait, même quand on « achète » un jeu vidéo au modèle économique classique, on ne paye en réalité qu'une licence d'exploitation (illimitée dans le temps, là), lire notre dossier sur acbm.com/virus/num_¬26/licence-to-bill.html. Le studio Nadeo en charge du développement du jeu rajoute une couche de mauvaise foi dans le forum Maniaplanet : « *En fait, ce n'est pas un modèle d'abonnement, mais un accès au jeu pour une durée limitée. Vous payez pour avoir accès au jeu pour une période et c'est tout. Quand le temps est passé, vous devez acheter à nouveau le jeu pour le temps que vous voulez y accéder.* » Puisque ce n'est pas un abonnement, nous invitons donc les joueurs à ne pas s'abonner.

L'école en ligne de mire

Les écoles primaires et secondaires ayant été fermées dans des régions chinoises à cause du coronavirus SARS-CoV-2, des applications ont été lancées pour permettre aux enfants de continuer de suivre les cours et de recevoir des devoirs en ligne. L'une d'elles est *DingTalk* du groupe Alibaba, équipée de nouvelles fonctionnalités pour l'occasion. Pas vraiment enchantés de devoir continuer l'école à la maison, de jeunes utilisateurs de l'application ont fait courir une rumeur sur les réseaux sociaux : en attribuant massivement une étoile à cette application, elle serait boutée hors de l'App Store. 15000 évaluations négatives sont soudain tombées, et du jour au lendemain, le 11 février, la moyenne de *DingTalk* est passée de 4,9 (sur 5) à 1,4. Vaine tentative : même si la moyenne de 1 avait été obtenue, Apple n'aurait sans doute pas supprimé l'application de sa boutique. L'éditeur de *DingTalk* a néanmoins diffusé une vidéo demandant à ses utilisateurs de mettre une note de 5. Une blague a alors circulé parmi les jeunes sur les réseaux sociaux : oui, un 5 serait obtenu… toutes les cinq installations cumulées (au moins, ils semblent bons en calcul !). Mais, miraculeusement, le 17 février, des milliers de notes 5/5 sont arrivées pour contrebalancer les commentaires négatifs. On peut soupçonner qu'elles ont été attribuées par ces employés qui travaillent dans des « fermes à clics et faux commentaires »… faute d'avoir pu ou voulu étudier pour avoir un meilleur *job*.

Pour fêter ses 60 ans, Sega lance une minuscule Game Gear Micro en hommage à sa console portable. Elle est tellement petite qu'une loupe sera proposée par la société pour mieux voir ce qui sera affiché sur l'écran, au point d'être la risée d'internautes et la cible de photomontages (artiste inconnu).

Du banc d'essai au banc des accusés (suite)

Plusieurs fabricants de *smartphones* ont déjà triché dans des *benchmarks* pour faire croire que leurs appareils étaient plus rapides : Samsung, One, Huawei et d'autres (lire précédents numéros). Cette fois, c'est le fabricant de puces « tout en un » MediaTek qui a été démasqué par *Anandtech* en comparant deux versions du *smartphones* Oppo Reno 3, l'une destinée à l'Europe (équipée d'un processeur Helio P95) et l'autre réservée à la Chine (équipée d'un Dimensity 1000L). Curieusement, la première affichait de meilleurs résultats dans *PCMark* alors qu'elle est censée être inférieur sur le papier. En creusant un peu, un fichier *power_whitelist_cfg.xml* a été découvert dans le répertoire *vendor/etc/*. Il y apparaît que lorsque le *firmware* détecte certaines applications, notamment de *benchmark* (*PCMark*, *GeekBench*, *AnTuTu* et *3DBench*), il passe en mode « sports » et accélère l'appareil de 30 % en moyenne (avec des pointes à 75 % pour certains sous-tests). En utilisant une version furtive spéciale de *PCMark*, la théorie a été confirmée. Du coup, *Anandtech* a repris ses tests d'anciens appareils équipés de puces MediaTek. Le bout de code a été retrouvé dans le Xperia XA1 (à sa puce Helio P20) de 2016 ! Les marques qui ont triché, peut-être même à leur insu, sont nombreuses : Oppo et Sony donc, mais aussi Xiamoi, Vivo, iVoomi, Realme… Liste sans doute non exhaustive. Comme à l'accoutumée dans les affaires précédentes, MediaTek nie toute triche et parle d'« *optimisation* » dont elle rejette l'activation (ou non) sur les constructeurs. Une optimisation obtenue au prix d'une surchauffe de l'appareil et d'une réduction de son autonomie, qui ne reflète pas les performances en usage normal. Vous ne pouvez pas imaginer, cette histoire de puces tricheuses, ça nous démange, mais à un point…

Sécurité : le carna

Riot Games, à qui on doit le hit *League of Legends*, a lancé son nouveau jeu, *Valorant*. Le logiciel est accompagné d'un pilote indispensable qui se charge au niveau du noyau de *Windows*, malgré des risques de dysfonctionnements potentiels dus à des incompatibilités. En clair : la société chinoise de jeux vidéo peut prendre le total contrôle de votre PC, même lorsque vous ne jouez pas à *Valorant* ! Elle explique que c'est là que se trouve son nouveau mécanisme de protection contre la triche. Elle ajoute qu'il ne sera pas seul, car d'autres jeux populaires utilisent déjà des solutions concurrentes comme *EasyAntiCheat*, *Battleye* ou *Xigncode3*. Et que ces droits d'accès renforcés ne lui permettront pas plus de choses que ce qui lui était permis en mode utilisateur. On se demanderait presque pourquoi les droits d'accès ont été inventés dans les systèmes d'exploitation ! Si l'exemple de vol de la « *recette de cuisine secrète de votre grand-mère* » qu'elle donne peut laisser penser que le risque est anodin, elle pourrait en réalité aussi voler les mots de passe (banque, réseaux sociaux…) utilisés sur cet ordinateur, y compris par un autre utilisateur. Et même si la société n'abuse pas du procédé (cela restera à prouver…), il y a le risque que le pilote introduise une faiblesse de sécurité qui sera utilisée à son insu par des pirates. Cela ne relève pas de la science-fiction : une telle mésaventure est arrivée dans le

Nintendo échoppe ses serveurs

Nintendo fermera l'eShop des familles Nintendo 3DS et Wii U le 31 juillet dans des territoires d'Amérique latine et des Caraïbes (dont la Guyane française, la Guadeloupe et la Martinique). Les codes d'achat non utilisés d'ici là seront perdus. Il ne sera plus possible de télécharger des mises à jour de logiciels. Et il ne sera plus possible non plus de retélécharger des jeux achetés, qui avaient été effacés par l'utilisateur pour faire temporairement de la place en mémoire par exemple. Le dématérialisé montre donc, une fois de plus, ses limites, car la richissime Nintendo (621 milliards de yens de trésorerie) ne souhaite plus dépenser quelques dizaines d'euros par mois pour maintenir des serveurs et respecter ses clients. Dans ce cas, remercions d'avance les pirates (des Caraïbes ?) qui s'en chargeront à sa place !

La cuisine interne de Cooking Mama

À peine lancé, *Cooking Mama: Cookstar* a rapidement disparu des boutiques de téléchargement occidentales de la Nintendo Switch, sans la moindre explication. Selon une rumeur, le jeu vidéo minait de la cryptomonnaie, ce qui aurait expliqué la surchauffe de la console constatée par les joueurs. L'éditeur, Planet Entertainment, tenait sa part de responsabilité : pour faire parler de lui, il avait annoncé à l'origine que son produit utiliserait une *blockchain.* En réalité, il semblerait que la surchauffe vient surtout d'une mauvaise programmation (le code relatif à la *blockchain* ayant été abandonné en route). Et c'est, peut-être, en partie la vraie raison de la disparition de *Cooking Mama: Cookstar* : Office Create, le propriétaire de la licence des jeux de cuisine *Cooking Mana*, s'oppose à sa diffusion, reprochant à Planet Entertainment le manque de qualité du projet. Elle affirme que des problèmes avaient été remontés, mais auraient été ignorés. Et c'est donc sans son accord que le jeu a été mis en vente. Pis, une version pour PlayStation 4 a été proposée en préachat en Europe par diverses enseignes, alors qu'une telle version n'était pas prévue contractuellement. Office Create a notifié à son ancien partenaire la rupture immédiate de leur contrat et évoque des poursuites judiciaires. La version en boite du jeu risque de devenir *collector* ! Planet Entertainment rétorque que les développeurs de 1st Playable ont respecté le cahier des charges et concrétisé plusieurs suggestions d'Office Create. Toutefois, des divergences créatives seraient apparues à la fin du développement, mais hors cadre contractuel, selon l'éditeur qui affirme donc pouvoir commercialiser librement le jeu vidéo, ajoutant que l'accueil des fans a été très positif. Voyons voir : selon *Metacritic*, qui compile les notes attribuées par des médias, *Cooking Mama: Cookstar* récolte 46 % (ce qui est mauvais), et une moyenne de 6,6/10 auprès de joueurs. Et aucune explication n'est donnée par l'éditeur concernant la version pour PlayStation 4. Pour en savoir plus, nous avons tenté de le cuisiner, en vain.

val de Riot Games

passé avec un *rootkit* (c'est le nom technique du procédé) installé par Sony (lire *Pirates Mag'* 21). Et l'éditeur annonce que *League of Legends* sera protégé de la même façon à l'avenir. Face aux inquiétudes, Riot Games promet finalement de 250 à 100 000 dollars aux *hackers* qui lui remonteront des failles dans son mécanisme de sécurité. Quoi qu'il en soit, rappelons que cette société est une filiale de Tencent, opérateur des télécoms qui file des coups de main (on parle d'aider ici, pas de kung-fu !) aux espions chinois. *(Merci à LC !)*

Chez Amazon, un disque dur externe Western Digital de 10 To est vendu 199 €. Dedans, on trouve l'équivalent d'un disque interne vendu, lui, 366 €. Une aberration écologique et économique, même si les revendeurs ne sont pas forcément les mêmes, puisque le boitier externe s'ouvre assez facilement pour extraire le disque dur. Et dire qu'il est censé supporter la taxe copie privée en sus par rapport au modèle interne… *(Merci à LC !)*

La petite commission d'Amazon

De nombreux sites Web vivent, en partie ou en totalité, de revenus tirés de l'affiliation Amazon : si un visiteur clique sur une publicité ou un lien spécial puis achète des produits, Amazon reverse une commission au site Web d'origine. Alors que les ventes du vépéciste ont explosé en raison de la crise du coronavirus et du confinement sur une partie de la planète, Amazon a décidé de réduire les taux de commission. Par exemple, les produits alimentaires ne permettront plus que de gagner 1 % au lieu de 5 % jusqu'à présent, les produits de beauté ou les instruments de musique 3 % au lieu de 6 %, les meubles ou produits pour animaux 3 % au lieu de 8 %… Bref, les revenus ont été divisés jusqu'à cinq fois, et ce, sur des biens de première nécessité. Coïncidence ou pas, le jour de cette annonce, Amazon atteignait un nouveau record de valorisation à la bourse. Ce n'est, d'ailleurs, pas la première baisse de commission dans l'histoire de la société. Rappelons aussi que le *cookie* de *tracking* n'est plus que valable 24 heures : au-delà, le vépéciste ne reverse plus aucune commission. La vie des affiliés Amazon est loin d'être un long fleuve tranquille, mais nous ne pleurerons pas pour eux : ils sont en partie responsables de la position d'Amazon (non, ce n'est pas sexuel) sur le marché.

Amazon nous fait marché

Dirigée par Lex Luth… pardon Jeff Bezos (désolé pour la confusion, ils se ressemblent tant physiquement et moralement !), Amazon est l'incarnation du mal dans le monde moderne. Nous avons vu, par exemple (références non exhaustives), qu'elle exploite ses salariés et les livreurs indépendants (*Virus Info* 36), vend des pièges à gogo (*Virus Info* 39) et de la contrefaçon (*Virus Info* 37), nous a spolié partiellement nos droits d'auteurs (*Virus Info* 35), utilise les paradis fiscaux, etc. Son imagination semble sans limites. Fin 2019, le *Wall Street Journal* avait aussi révélé que des revendeurs tiers indélicats profitaient des manques de contrôles d'Amazon pour faire expédier en son nom des produits trouvés dans des poubelles. Cette fois, le journal dit tenir d'anciens employés que la société se sert des chiffres de ventes de sa place de marché en ligne (Marketplace) ouverte aux vendeurs tiers pour repérer leurs produits qui ont du succès et les concurrencer en créant les siens sous la marque Amazon. Une pratique interdite. Amazone nie (jeu de mot offert, voulez-vous le rajouter à votre panier ?) et affirme qu'une enquête interne est ouverte au cas où. Voilà, elle est déjà refermée à cause des courants d'air.

En bref

Depuis plusieurs années, la cellule communication de l'État major des armées (françaises) utilise un courriel hébergé chez Gmail (Google) pour communiquer avec les journalistes notamment. Quelqu'un pour leur dire que Hotmail de Microsoft est plus sûr encore ?

En raison du confinement en France pour limiter la propagation du coronavirus, Internet a été particulièrement sollicité. Pour « éviter *de* [le] *saturer* », Orange a diffusé un fichier avec des conseils de sobriété numérique comme, par exemple, réduire la qualité du *streaming*. Le fichier en question pesait… 6 Mo, alors que ce texte aurait pu être 1 000 fois plus petit. Sur un malentendu, ça pourrait marcher avec une personne hors forfait.

Il y en a qui ont de l'avance : le nom de domaine covid20¬.com est déjà réservé. Covid21.com aussi, de même que covid22¬.com… En fait, tous jusqu'à covid37.com. Ah, tiens, covid38.com est disponible. Les spéculateurs semblent prévoir qu'on sera déjà tous morts en 2038. À moins que ce soit Internet. 2038 est l'année du prochain grand bogue (19 janvier).

Quand on vous dit « fondation », vous avez sans doute l'image d'une organisation qui œuvre pour le bien du monde. La Fondation Bill et Melinda Gates, celle du cofondateur de Microsoft et de sa femme, annonce avoir acheté au premier trimestre 500 000 actions… d'Apple, 60 000 actions d'Amazon, 85 000 d'Alphabet (Google), etc. Plein de bonnes actions, bravo !

Atari nous déçoit. Sa nouvelle console VCS est encore en retard, passe encore, mais la société n'a même pas pris la peine d'inventer une nouvelle excuse qui nous fait rire. Et ça se prétend société de divertissement !

Rappels à la pelle

En raison de risques physiques pour leurs utilisateurs, certains produits doivent être retournés à leur fabricant pour réparation, voire sont tout simplement retirés du marché. Voici la liste des récents rappels officiels relayés par les autorités.

En raison d'un risque de choc électrique, il faut faire remplacer les alimentations externes (référence APP524-051240U) vendues en Australie pour les SSD My Passport Wireless Pro et Hard Disk Western Digital des modèles WDBP2P0020BBK, WDBVPL0010BBK, WDBSMT0030BBK, WDBSMT0040BBK, WDBAMJ0010BGY, WDBAMJ0020BGY, WDBAMJ2500AGY et WDBAMJ5000AGY. support.wdc.com/support/¬case.aspx

En raison d'un risque de surchauffe, Epson rappelle les adaptateurs électriques (modèle A392AS, numéro de produit EADP-16CB E, G ou B) vendus dans divers pays (Australie, Amérique du Nord, Corée du Sud…) avec ou pour des scanners Perfection V30, V300 Photo, V33, V330 Photo, V37 et V370.

Du fait d'un risque de court-circuit, Modular Robotics rappelle les batteries vendues seules ou avec des produits Classroom Kits, GoPiGo et BrickPi. Elles sont de 9,6 V et 2000 Ah, de type NiMH, pour un courant maximal de 2 A. Elles portent une inscription « Dexter Industries Rechargeable Battery Pack » sur une étiquette blanche.

En raison d'un risque de court-circuit, Leedsworld rappelle des chargeurs portatifs Spare de 10 000 mAh. À piles et blancs, ils portent le numéro d'article 7121-18WH et le numéro de lot 1813582. Différents logos peuvent apparaître aussi, ces produits ayant été, parfois, offerts dans un cadre promotionnel.

Des résidus non précisés peuvent entraîner des moisissures (avec des conséquences pour la santé de rares personnes) sur des écouteurs et leur boite de rangement Panasonic RP-HD610N. Un remplacement gratuit est proposé si nécessaire.

L'Agence nationale (française) des fréquences (ANFR) fait rappeler les *smartphones* Razer Phone 2 en raison d'un dépassement de la norme en matière d'ondes électromagnétiques. La limite tolérée au niveau du tronc est de 2 W/kg, le Razer Phone 2 émet 3,79 W/kg. C'est rasoir ! Le rappel a débuté le 8 mai et va s'étendre sur six mois. Pour plus d'information : http://rzr.to/rp2-fr.

Il n'y a pas de campagne de rappel, mais si le verre de votre tablette Surface Laptop 3 (13 ou 15 pouces) est victime d'une fissure sans raison pendant la période de garantie, vous êtes éligible à un remplacement gratuit, voire à un remboursement si vous avez déjà effectué une réparation à vos frais. Ce défaut ne concerne qu'un nombre très limité de cas, selon Microsoft, qui l'explique par la présence d'une particule étrangère dure. Attention, si la fissure est due à une chute ou autre, cette garantie ne s'applique pas ! Pour plus d'informations : support.microsoft.com¬/fr-fr/help/4561768/sur¬face-laptop-3-cracked-¬screen-reported-inci¬dents

Trust rappelle ses pointeurs laser de référence 20430-02 et de code à barres 8713439204308 en raison d'un risque de lésion de la rétine pour l'utilisateur et son entourage (pas plus de détails, alors que c'est le cas de tous les produits de ce genre, si ce n'est que sa classe 3R impose la manipulation par un utilisateur connaissant les règles de sécurité).

Sont rappelées les batteries de téléphone portable 3,7 V – 1350 mAh de NX référence GML 90252 (EB494358VU) du lot C00317C190 en raison d'un risque d'incendie en cas de température excessive.

Apple propose une réparation gratuite aux iPad Air de 2019 (troisième génération) concernés par un écran devenu définitivement noir, éventuellement après avoir scintillé ou clignoté. Cela concerne des appareils fabriqués entre mars 2019 et octobre 2019. Ce programme de réparation est d'actualité durant les deux années suivant la première vente au détail du produit.

Sont rappelés en raison d'un risque de choc électrique, les chargeurs USB 2 en 1 de marque O.mee portant la référence JJH-069, les ensembles chargeur réseau/port USB/chargeur voiture Three-in-one charging kit d'Inkax de référence CD 43 type C et de lots CC 37/CD 36.

Des utilisateurs des premières cartes graphiques de la série ROG Strix Radeon RX 5700 d'Asus ont rencontré des problèmes de surchauffe. Le fabricant certifie avoir respecté les recommandations initiales d'AMD, le fournisseur de la principale puce. Mais les faits sont là : la pression entre cette puce et son radiateur n'est pas suffisante. Le fabricant de cartes graphiques indique avoir effectué des tests qui lui ont permis d'identifier les vis qui permettent, enfin, une meilleure conduction de la chaleur. Les produits désormais fabriqués sont conformes, avec des performances meilleures et moins de bruit à la clé. Mais si vous avez une carte qui a été vendue sans ces nouvelles vis, il faut contacter le centre Asus proche de chez vous pour que la modification soit effectuée gratuitement. ■

Mauvaises ondes

Lors d'un contrôle par un laboratoire mandaté par l'Agence (française) nationale des fréquences (ANFR), il a été constaté que le *smartphone* OnePlus 6T émettait 2,56 W/kg sur le DAS à 5 mm du tronc dans la bande des 1 900 MHz en 3G. Au-delà de la limite légale de 2 W/kg. L'importateur Eastern Sun Trading a demandé au fabricant de concevoir un correctif logiciel. En l'installant, les utilisateurs ne seront plus soumis qu'à 1,17 W/kg. À notre goût, ces problèmes de fréquences sont trop fréquents.

Piqûre de rappel sur le codage numérique pour l'AFP

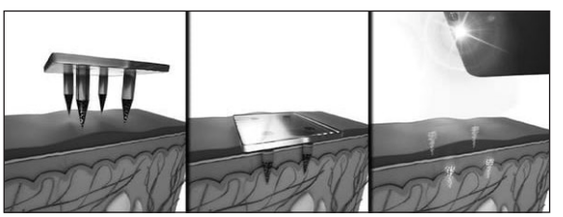
Selon une rumeur, Bill Gates veut profiter du Covid-19 pour vacciner la population avec une puce intégrée qui permettrait de la pister. AFP Factuel a publié un article[1] pour la démentir, et c'est une bonne chose. Mais l'agence de presse a été un peu vite en besogne en écartant sans ménagement une information pourtant plausible techniquement.

Lors d'une séance de questions/réponses sur le site *Reddit*, Bill Gates a déclaré[2]: « *finalement, nous aurons des certificats numériques pour montrer qui a guéri, a été testé récemment ou a reçu un vaccin, quand nous aurons un vaccin.* » De notre côté, nous y avions vu, comme d'autres, un lien possible (mais jamais annoncé) avec un système de vaccination mis au point, à la demande de la fondation Gates justement, par l'université RICE et le MIT[3] (États-Unis).

L'AFP explique qu'« *en sécurité informatique, un certificat numérique est une sorte de signature électronique virtuelle qui atteste de l'authenticité d'un site Web* » et ajoute que Dan Wattendorf, directeur des solutions technologiques innovantes de la Fondation Gates, lui a déclaré: « *La référence à des certificats numériques concerne la création possible d'une plateforme numérique en* open source *dans le but d'étendre l'accès* à un test à domicile qui soit sécurisé. » Ce propos est hors sujet, sans que l'AFP le relève. Car la vraie question est: où sera stocké le certificat numérique de chacun, ou son mécanisme de protection, pour que personne ne s'en serve à son insu (notamment pour les vaccinés dans les pays en voie de développement) ? La dépêche n'en dit rien.

L'AFP enchaîne: « *autre confusion fréquente, l'amalgame entre « certificats numériques » et « tatouages quantum-dot ». Ce sont des choses qui n'ont rien à voir* », et d'expliquer ce que sont les *quantum-dots*.

Nous n'avons pas d'objection concernant la présentation technique des *quantum-dots* faite par l'agence de presse, mais nous allons vous proposer la nôtre plus détaillée pour les besoins de notre démonstration. Il s'agit d'un *patch* d'un centimètre carré contenant des aiguilles (1,5 mm de long, ce qui ne ferait pas mal, assurent les chercheurs) contenant un vaccin, qui se dissolvent en laissant une sorte de marquage fluorescent sur la peau, des points de 4 nanomètres (les *quantum-dots*) invisibles à l'œil nu, mais visibles avec un dispositif lumineux spécial et un *smartphone* modifié équipé d'un logiciel de réseau neuronal. L'objectif est que cette lecture soit possible pendant au moins cinq ans (pendant l'expérience sur des rats, elle l'était neuf mois après l'injection). Il reste encore à vérifier que le procédé n'est pas toxique à long terme.



Crédit: Second Bay Studios.

65536 combinaisons possibles

Le *patch* laisse ainsi un message constitué de jusqu'à 16 points, une sorte de « *code à barres tatoué* » selon les chercheurs (on aurait pu aussi comparer visuellement à un QR code). Comme il ne semble pas possible de modifier un tel *patch*, tout nouveau vaccin est accompagné d'un nouveau *patch*. Précisons que le tatouage peut être effectué sans charge vaccinale, par exemple pour marquer que quelqu'un testé possède déjà des anticorps. La technologie est surtout prévue pour les pays en voie de développement, où tout le monde n'a pas ni carnet de santé ni *smartphone* pour stocker un QR code signé numériquement dont on peut vérifier l'authenticité en ligne (une solution adoptée en Estonie).

Nos lecteurs informaticiens connaissent le nombre par cœur: 16 points allumés ou éteints, 16 bits, cela représente 65 536 combinaisons possibles. Pas assez pour stocker un identifiant personnel (mais à l'avenir si le nombre de points augmente comme la résolution des écrans avec le temps, pourquoi pas; en attendant avec deux *patchs* côte à côte on dépasserait 4 milliards de combinaisons). Par contre, 65 536 c'est suffisant pour stocker, sous forme numérique, le code d'un vaccin et un bout de la date par exemple. Cela pourrait paraître un peu tiré par les cheveux, mais on pourrait d'ailleurs qualifier ce tatouage de « *certificat numérique* » (comme disait Bill Gates), puisque basé sur des nombres et sur une sorte de tampon réel comme il y en aurait sur un certificat papier, les points pouvant dessiner la figure souhaitée (carré, rond ou autre) en sus.

Bref, contrairement à ce qu'affirme l'AFP (et même si ce n'est pas ce que voulait dire Bill Gates), il n'y a pas forcément d'amalgame entre « certificats numériques » et « tatouages quantum-dot ». ■

1. factuel.afp.com/non-bill-gates-na-pas-propose-dimplanter-une-puce-electronique-la-population
2. gatesnotes.com/Health/A-coronavirus-AMA
3. news.rice.edu/2019/12/18/quantum-dot-tattoos-hold-vaccination-record/

La culture toxique chez Quantic Dream : une intoxication de la part de médias ?

Début 2018, trois médias (*Canard PC*, *Mediapart* et *Le Monde*) se sont associés pour publier des articles sur les conditions de travail dans l'industrie du jeu vidéo, notamment chez le studio Quantic Dream (*Fahrenheit*, *Heavy Rain, Beyond: Two Souls*, *Detroit: Become Human*…) fondé par David Cage et à qui il était reproché jusqu'à une « *culture d'entreprise toxique* » (*Le Monde*). L'information a été reprise par d'autres médias partout dans le monde. Le travail des journalistes français a, finalement, été remis en cause par *VentureBeat* début 2020. Une partie de l'affaire décrite est partie aussi devant la justice. Ayant lu la dernière décision de justice en date, nous avons constaté un gros décalage entre ce qui y est écrit et certains articles lus ici ou là. Nous avons décidé de lancer notre propre enquête pour comprendre qui dit vrai. Elle a été particulièrement difficile, mais avec de grosses surprises à la clé !

Nous ne recevons ni les communiqués de presse ni les jeux de Quantic Dream, nous n'avons pas de publicité dans nos pages (et nous ne voulons rien de tout cela). Ce qui nous intéresse, c'est la vérité, qu'elle vienne de *VentureBeat* ou des médias français ne change rien pour nous. Nous n'avons jamais rencontré ni les uns ni les autres. Basés à quelques milliers de kilomètres, nous pouvions donc enquêter de manière neutre et objective avec le recul nécessaire. Nous avons contacté toutes les parties impliquées : les victimes reconnues ou revendiquées, la société de jeux vidéo, des salariés et d'anciens salariés (contactés par nos propres moyens, sans passer par la société), les journalistes des trois médias, des syndicats de travailleuses et travailleurs. Notre objectif : proposer à chaque « camp » une place équivalente pour lui permettre d'exprimer son point de vue, nous faire et laisser notre lecteur se faire sa propre opinion.

Si *Mediapart* a refusé de répondre à nos questions, il nous a invités à réutiliser ses déclarations faites à Thomas Mahler dans un article du magazine *Le Point*, semblable à celui de Dean Takahashi chez *VentureBeat* (un média traitant de l'actualité des nouvelles technologies). Nous l'avons fait quand c'était possible, mais de nombreux points (justement…) resteront malgré tout sans réponses. Les journalistes de *Canard PC* et *Le Monde* n'ont même pas eu la politesse d'accuser réception. Quantic Dream a décliné en expliquant ne pas avoir le temps à cause de la réorganisation du travail face au coronavirus. Les victimes reconnues ou revendiquées n'ont pas répondu, à part une qui s'est montrée agressive (lire encadré) sans apporter aucune réponse à nos questions. Nous avons donc dû trouver d'autres sources d'information, en sus des articles susmentionnés. Les personnes ayant refusé de répondre portent l'entière responsabilité de ne pas contredire dans ces pages les accusations portées contre elles (nous aurions aussi pu publier, avec leur accord, les documents prouvant leurs versions). Si elles changent d'avis, nous pourrons envisager une suite à l'article que vous lisez.

Les petits du jeu vidéo sont invisibles

Parler de *crunch* dans le jeu vidéo, cela nous fait tout drôle. Nos bouclages sont souvent éprouvants, mais nous devons finir les magazines à temps, sinon il y aura une sanction administrative et fiscale en France qui entraînera l'arrêt des publications (les autres pays où nous diffusons ne nous mettent pas une telle pression). Et pas question de mettre n'importe quoi dans les pages pour finir plus vite, l'issue serait la même à terme. Nous n'avons pas les moyens de recruter pour faire les articles plus vite. Et aucune administration à qui nous plaindre pour obtenir une solution.

Lorsque nous allons sur des salons professionnels du jeu vidéo, nous ne sommes pas considérés comme du même monde que les David Cage et compagnie, nous sommes généralement tenus à l'écart des zones VIP, des évènements privés sur les stands, etc. En fait, nous rencontrons à ces évènements surtout des développeurs indépendants qui, eux, nous ressemblent beaucoup. Des « studios » d'une personne ou d'une poignée de personnes qui ne comptent pas les heures pour finir leur jeu parce qu'il faut le lancer pour espérer avoir de quoi payer loyer et nourriture. Ces indépendants représentent une part non négligeable du marché. Les gros succès sont toutefois rares, la majorité des studios survit tant bien que mal. Les autres médias qui font des enquêtes sur les conditions de travail dans le jeu vidéo ont tendance à les ignorer. Nous tenions à rendre hommage ici à ces entrepreneur(e)s, qui préfèrent « se battre » plutôt que de laisser tomber et aller pointer à l'agence pour l'emploi.

Une triste affaire de photomontages

Le 4 janvier 2018, les journalistes du trio de médias se rendent chez Quantic Dream. Leur enquête porte notamment sur une affaire de photomontages à la base de procédures aux prud'hommes. Depuis plusieurs années, un développeur responsable du pôle Game Logic (présent dans la société depuis une dizaine d'années et également délégué du personnel) réalisait sur son temps libre des photomontages de ses collègues, de la direction (par exemple David Cage en Joconde barbue) et de lui-même. Ces photos étaient envoyées aux intéressés, voire à quelques autres personnes. Certaines ont été affichées, par exemple, à la machine à café, parfois par les intéressés eux-mêmes, sans que cela ne fasse scandale ni en interne ni à l'extérieur. Si une personne demandait à ne plus en être mise en scène, son souhait été respecté, affirme la direction de Quantic Dream à *VentureBeat*, qui ajoute qu'il n'y avait aucune volonté d'humilier ou de se moquer.

Pour le 600e photomontage, en février 2017, c'est le responsable du service informatique (en charge du réseau interne d'ordinateurs, etc.) qui est mis en scène, sa tête collée à un corps de Sylvie de *Super Nanny* faisant un doigt d'honneur. Il s'en est ému à la

direction, qui a immédiatement réagi en demandant au coupable de cesser et en lui donnant un avertissement. Cette sanction, ainsi que des excuses personnelles à la victime à plusieurs reprises dans les jours suivants, seront insuffisantes pour le responsable du service informatique qui exigera le licenciement de son collègue, à en croire *VentureBeat*.

Il existait un litige entre les deux employés depuis que les développeurs s'étaient vus interdire de jouer en ligne au bureau « *pour des raisons de sécurité* » (alors qu'au service informatique, des salariés ne se privaient pas de jouer, selon des témoignages que nous avons recueillis). À leur tour, les trois autres membres (non-cadres) du service informatique entreront en conflit avec l'employeur. Une médiation est enclenchée, mais ne peut aboutir faute d'accord sur son périmètre : Quantic Dream veut la limiter à l'affaire des photomontages, alors que les salariés exigent que la discussion porte sur leur départ de l'entreprise accompagné de grosses indemnités.

Un chantage ?

À notre avis, des lanceurs d'alerte auraient immédiatement prévenu la presse et/ou les autorités compétentes. Ici, le combat semble avoir été bien plus personnel, selon les documents judiciaires que nous avons consultés. D'ailleurs, selon *VentureBeat* relayant Quantic Dream, l'ancien responsable informatique aurait exigé un an de salaire plus 40 %, sinon il menaçait de « *raconter toute l'histoire à la presse.* » Lors de l'audience, la société a clairement affirmé être victime d'un « *chantage* ». Malheureusement, la personne mise en cause n'a pas souhaité nous donner sa version, pas plus qu'à *VentureBeat*. Aucune des deux parties ne nous a communiqué de documents qui prouveraient sa version, il nous est impossible de trancher en l'état.

Quantic Dream refusant de céder, des autorités compétentes ont, enfin, été saisies par le responsable informatique. Dans un cas, l'affaire a été classée sans suite. Dans l'autre cas, elle a été conclue par un rappel à la loi en septembre 2017 de la part du procureur de la République pour « *des faits d'injures non publiques aggravées en raison du sexe ou de l'orientation sexuelle de la victime.* » Précisons que ce rappel à la loi a été prononcé contre l'auteur des photomontages (qui a quitté l'entreprise depuis), pas contre l'employeur.

Une série de photomontages odieux, dont nous allons parler plus loin, ont été envoyés à des journalistes (nous ne faisions pas partie des destinataires). Les quatre employés du service informatique ont engagé des poursuites devant les prud'hommes afin que leurs démissions soient requalifiées en licenciement.

Condamnée et blanchie (c'est assez quantique ?)

Dans *Virus Info* 35, nous vous avions informé que deux des ex-employés avaient été déboutés devant les prud'hommes début 2018 (un d'eux va en appel). Le Conseil estime les photomontages problématiques, mais reconnaît que la société est intervenue promptement à l'alerte sur le 600e. Il déclare que le salarié a « *réagi bien tardivement à l'existence des photomontages le concernant pour pouvoir obtenir aujourd'hui la rupture de son contrat de travail aux torts de son employeur ; que, de surcroît, après avoir demandé une rupture conventionnelle de son contrat, demande acceptée par la SA Quantic Dream, il a ensuite refusé la proposition de celle-ci* » (il était question, là, d'images plus anciennes que la 600e). Il ajoute que la société « *démontre (sans doute* a minima*, mais que pouvait-elle faire de plus à son niveau) avoir apporté une réponse peu ou prou appropriée au problème qui lui avait été signalé ; qu'il sera utilement observé ici que* [le salarié] *aurait sans doute pu mieux se pourvoir, directement à l'encontre du ou des auteurs des photomontages qui l'ont blessé.* »

Enfin, il remarque qu'« *il est permis de s'interroger sur le fait de savoir si* [le salarié] *n'aurait pas été instrumentalisé par d'autres ou n'aurait pensé pouvoir profiter d'un effet d'aubaine et obtenir une indemnisation financière bien supérieure.* »

De nombreux médias de la planète qui avaient relayé les accusations n'ont pas pris la peine d'informer leurs lecteurs de ce résultat qui déboutait le plaignant.

La deuxième décision tombée le même jour est similaire. L'autre plaignant s'est vu répondre qu'il n'a pas « *apporté au Conseil la justification du fait que les problèmes de santé qu'il a pu rencontrer étaient imputables à son employeur.* »

À *VentureBeat*, Quantic Dream évoque des documents concernant les entretiens annuels de ces salariés, quelques semaines avant l'incident, lors desquels ils auraient affirmé être heureux dans la société et que l'atmosphère de travail était agréable. Nous aurions aimé lire ces documents, et les autres, mais ni l'employeur ni les ex-employés ne donnent suite à nos demandes.

Plus tard cette même année, un troisième ex-employé avait eu gain de cause (là, c'est la société qui va en appel). Enfin, la quatrième procédure a été tranchée par un juge professionnel, les conseillers des prud'hommes n'ayant pas réussi. L'ex-responsable informatique réclamait 14 352 € d'indemnité compensatrice de préavis, 1 435 € de congés payés afférents, 5 621 € d'indemnité conventionnelle de licenciement, 86 112 € d'indemnité de licenciement sans cause réelle et sérieuse, 5 000 € pour manquement à l'obligation de santé-sécurité et 2 000 € pour les frais de procédure, soit un total de près de 115 000 €. Précisons que son salaire mensuel brut était de 4 784 € (il est important de le préciser, alors que nos confrères évoquaient des employés mal payés dans leurs enquêtes). En face, Quantic Dream sollicitait le débouté, 14 352 € pour préavis non effectué et 5 000 € de frais de procédure. Une réponse du berger à la bergère plutôt habituelle devant la justice (on parle de « demandes reconventionnelles »).

L'ex-employé reprochait devant le juge que son mot de passe avait été changé. La décision hiérarchique a pourtant été déclarée légitime aux yeux de la justice. La défense avait argumenté que le responsable informatique était en congé maladie et n'avait aucune raison de se connecter de l'extérieur, qu'il n'avait « *laissé ni les mots de passe ni les procédures nécessaires* », ce qui a « *désorganisé l'entreprise en bloquant le service informatique* [...] *mettant en péril la société à un moment stratégique* » (une société de services a dû intervenir en urgence). À l'audience, il a présenté outre le photomontage « Super Nanny », un autre plus ancien (dont il ne s'était pas plaint à

Des victimes collatérales à cause de Canard PC

Ce serait sans doute « très vendeur », mais nous avons choisi de ne publier aucun des photomontages litigieux pour illustrer cette enquête, ces photomontages étant destinés à une diffusion dans un cadre privé à l'origine, ce qui en limitait leur nuisance. Il ne s'agit pas pour nous de minorer la responsabilité de leur auteur à vos yeux, bien au contraire. *Canard PC* a rendu publiques certaines images représentant « *des collègues qui n'avaient rien demandé. Le bandeau minuscule n'empêchait nullement de les reconnaître et certains ont très mal vécu cela* » (le milieu professionnel du jeu vidéo étant petit), nous a déclaré un délégué du personnel de Quantic Dream. Nous ne voulons pas infliger à ces personnes cette peine à nouveau.

Année	Chiffre d'affaires	Résultat	Employés
2017	10,595 K€	-2,396 K€	non précisé
2016	10 406 046 €	473 854 €	186
2015	13 632 299 €	153 635 €	176

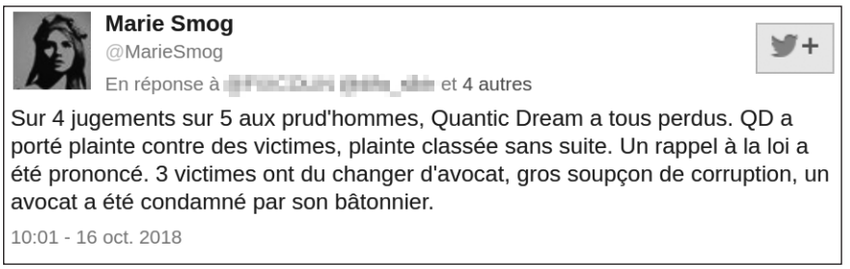
Quantic Dream, en chiffres (ceux de 2018 et 2019 sont inconnus pour le moment)

l'employeur à l'époque) où il était représenté en porte-jarretelles, mèche et moustache à la Hitler, le bras tendu en un salut nazi. Quantic Dream a répondu que ce « *photomontage le représentant en Hitler n'a jamais été diffusé sur le lieu de travail, et a été obtenu frauduleusement.* » C'est cette image, en réalité partagée avec tous les salariés selon l'ancien responsable informatique, qui a valu à son auteur un rappel à la loi évoqué plus tôt.

Des informations minimisées, voire tues

Le tribunal estime qu'« *il n'est pas contesté qu'aucune plainte n'a été émise avant le 27 février 2017 quant à ces photomontages* […] *Au vu de l'absence de plainte du salarié jusque-là s'agissant de cette pratique, de l'unique photo le concernant diffusée ce jour-là* [celle en Super Nanny]*, et de la réaction immédiate de la direction, elle ne constituait pas à elle seule un manquement de l'employeur faisant obstacle à la poursuite du contrat de travail.* » Fin 2019, l'ex-salarié a été débouté de ses principales demandes, car il n'a « *pas apporté la preuve d'une dégradation des conditions de travail au sein de l'entreprise ou encore d'un conflit important et récurrent* […]*, la production d'articles de presse* […] *ne suffisant pas à établir ces faits.* » En clair, l'ambiance toxique dépeinte par certains médias n'est pas démontrée, la victime ne recevra donc que 5 000 € au titre de l'obligation de sécurité (plus 2 000 € de frais de procédure), car l'entreprise aurait dû prendre les devants. Insistons, au cas où vous seriez tombés sur un média de mauvaise qualité ici ou là sur la planète, sur le fait que la société n'a pas été condamnée pour avoir réalisé ou fait réaliser ces photomontages. La victime a décidé de faire appel.

Encore un mensonge signé Marie Smog. *VentureBeat* avait proposé la parole à la principale victime des photomontages dans son article, mais celle-ci a refusé de répondre. Le site Web n'est pas responsable.



Marie Smog diffuse de fausses informations. Quantic Dream n'a pas perdu les premières procédures : les prud'hommes y déclarent que « *l'article 696 du Code de Procédure civile dispose que la partie perdante est condamnée aux dépens*. » Or ce sont les plaignants qui ont été condamnés à ces dépens, pas Quantic Dream, quand bien même la société a été déboutée de ses demandes reconventionnelles.

Le trio de médias – ceux dont les articles ne sont pas retenus dans cette décision judiciaire – a titré sur la condamnation de Quantic Dream, mais il fallait lire les articles en entier (pas toujours accessibles gratuitement, contrairement à leur titre) pour découvrir que l'ex-salarié avait été débouté de ses principales revendications. Pourquoi ne pas titrer sur cela aussi ?

Le montant alloué (5 000 €) peut sembler généreux, mais l'ancien responsable informatique de Quantic Dream avait déclaré lors de l'audience : « *retrouver un travail aujourd'hui est compliqué pour moi, c'est un petit milieu. Les employeurs ne veulent pas prendre de risque.* » En réalité, il pourrait faire exactement le même métier ailleurs que dans le jeu vidéo, comme il le faisait déjà avant (il n'était pas développeur de jeux chez Quantic Dream). Les informaticiens ont été très recherchés pendant toutes ces années, les sociétés peinaient à recruter. Et, de fait, il avait retrouvé un emploi dans une société plus industrielle, mais un autre incident s'y est produit (lire encadré)… ciblant Quantic Dream ! Un point qu'il a oublié de préciser au juge, tout comme *Le Monde* et *Canard PC* ont « oublié » d'en informer leurs lecteurs.

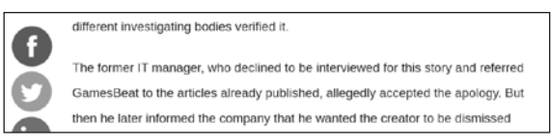
Pourtant, « *du côté des journalistes qui ont accusé Quantic Dream, on nous assure que tout, au contraire, a été fait pour s'assurer qu'il ne s'agissait pas d'une simple vengeance personnelle, mais d'un « problème systémique »* », peut-on lire dans *Le Point*… On aurait presque envie de rire, car l'homme se serait aussi vanté à des ex-collègues de Quantic Dream d'avoir gagné une procédure aux prud'hommes contre son employeur précédent. Qu'en est-il ? Encore une fois, l'intéressé n'a pas souhaité répondre à nos questions et, contacté par nos soins, cet ancien employeur n'a pas été plus loquace. Même sans mettre en cause la légitimité de cette vieille procédure, nous estimons que des incidents de parcours professionnels répétés méritent d'être signalés au lecteur ; ce n'est visiblement pas le cas de nos confrères du trio de médias.

Il y avait pire malheureusement

Revenons à la décision de justice elle-même : « *le photomontage montrant* [le salarié] *en « super nanny » faisant un doigt d'honneur, s'il apparaît vulgaire, n'est ni homophobe, ni raciste, ni pornographique* ». Ce point important n'a été relayé à leurs lecteurs ni par *Le Monde* ni par *Mediapart*. Quantic Dream n'a pas été condamnée pour homophobie ou racisme, pas plus qu'elle n'a été condamnée pour une quelconque ambiance toxique de manière générale. Il est important de le préciser, car d'autres médias de la planète ont laissé entendre le contraire, l'information étant déformée au fur et à mesure qu'ils se recopiaient les uns sur les autres, sans vérifier à la source. Malgré une décision de justice favorable sur ces points, Quantic Dream n'en ressort pas blanchie médiatiquement, au contraire.

En réalité, devant la justice, il a été aussi question d'autres photomontages du lot de 600 mettant en scène d'autres personnes ou les mêmes. Le jugement dit que, parmi les échantillons versés au débat, « *certains sont homophobes, misogynes, racistes ou encore profondément vulgaires. En restant passif face à cette pratique plus que contestable, qui ne peut se justifier par l'esprit « humoristique » dont se prévaut la société, l'employeur a commis une violation de l'obligation de sécurité.* »

L'avocat des plaignants soulignait « *une misogynie évidente ; les femmes sont volontairement enlaidies insultées, le terme « pute » est récurrent. Quelques*


different investigating bodies verified it.

The former IT manager, who declined to be interviewed for this story and referred GamesBeat to the articles already published, allegedly accepted the apology. But then he later informed the company that he wanted the creator to be dismissed

***VentureBeat* a voulu interviewer l'ancien responsable informatique de Quantic Dream, c'est précisé dans l'article. Pour éviter d'être accusés de ne pas avoir contacté cette personne et ces collègues, nous avons du coup fait notre demande en privé et publiquement.**

exemples : « Ce soir c'est sodo » […] *« Toutes les femmes naissent égales mais les meilleures deviennent comptables* [mot précédent rayé] *putes ». Certains montages sont à connotation raciste, homophobe ou bien dégradants pour les personnes handicapées : « Mariage de vieux pds ».* » Nous n'irons pas plus loin dans la description pour ne pas choquer nos lecteurs les plus sensibles, tant ces photomontages sont abjects.

La direction de Quantic Dream prétend qu'elle en ignorait l'existence, qu'elle ne les a découverts que lorsque le lot de 600 photomontages a été dévoilé d'un coup. Selon elle, les photomontages de ce genre seraient une douzaine, mais Marie Smog affirme qu'il y en a plus de 150 qui sont de ce calibre. Malgré leur dureté, aucune des autres victimes n'a porté plainte et il n'y a pas eu de condamnation à leur sujet. Seule l'ancienne équipe informatique a réagi en justice, quand bien même le photomontage concernant le responsable informatique (celui en Super Nanny) n'aurait pas eu la même gravité, si on s'en réfère à la décision du juge. Nous pouvons comprendre des différences de sensibilité, nous compatissons avec toutes les victimes et nous trouvons d'autant plus déplacé (pour ne pas dire suspect) que l'une d'elles se venge sur nous (totalement extérieurs à cette affaire) en nous rendant… victimes de ses calomnies (lire encadré).

Nous vous tiendrons informés des appels en justice. Ajoutons qu'en parallèle, les anciens employés du service informatique déclarent qu'ils ont déposé en juin 2017 plainte pour harcèlement contre Quantic Dream et que celle-ci suit (trop doucement) son cours. En attendant, revenons à l'enquête du trio de médias.

Une interview édifiante

La direction de Quantic Dream affirme à *VentureBeat* avoir reçu des questions douteuses : « *nous avons trouvé une note de frais de 10 dollars de* room service *dans un hôtel à Las Vegas. C'était pour une prostituée ?* », « *un de vos salariés a un tapis de souris avec l'image d'un personnage féminin sexy. Est-ce que vous pensez que c'est acceptable ?* », « *un de vos employés a un t-shirt de* heavy metal *que quelqu'un trouve offensant. Encouragez-vous cela ?* », « *vous êtes connu pour travailler beaucoup. Êtes-vous au courant que des personnes qui travailleraient moins peuvent se sentir mal que vous travaillez plus ?* »… Elle ajoute avoir eu le sentiment que les journalistes avaient « *leur propre angle. Ils voulaient démontrer qu'une entreprise à succès devait être toxique et ils cherchaient la moindre preuve pour appuyer leur théorie.* » Les intéressés contestent.

Sur Twitter, Sébastien Delahaye (co-auteur de l'article de *Canard PC* avec Cécile Fléchon) parle de « *questions inventées* » et donne un lien vers la liste des vraies questions envoyées à Quantic Dream le 26 décembre 2017 : celles avancées par *VentureBeat* n'y sont pas. Et Ivan Gaudé, le directeur de la publication, ajoute : « *Y a juste un problème : ces questions* [litigieuses] *n'ont jamais fait partie de la liste envoyée le 27/12/17 à Quantic Dream.* » Nous pouvons nous sentir manipulés, car Dan Israel, co-auteur avec Mathilde Goanec de l'article de *Mediapart* (média qui semble le plus honnête du trio), reconnaît publiquement que « *ces questions ont été posées à l'oral, dans une conversation de deux heures. Elles semblent avoir été résumées par écrit par Quantic Dream, et de façon caricaturale, par ailleurs* » et il précise ne pas en être l'auteur. Ivan Gaudé ajoute alors qu'elles ont été « *réécrites, résumées, déformées et totalement sorties du contexte de la longue conversation qui a suivi.* » William Audureau du *Monde* est, lui, resté totalement muet face à ces accusations.

Ces journalistes n'ont pas voulu nous dire quelles étaient les questions réellement posées et qui d'eux les a posées. Ils n'ont pas souhaité non plus nous transmettre l'enregistrement réalisé lors de l'entretien qui nous aurait permis de vérifier qui dit vrai. Des choses à cacher ? *Le Point* déclare, toutefois, qu'un des journalistes (dont l'identité n'est pas précisée) lui a confirmé les questions, de « *simples vérifications* » selon l'interlocuteur. Il est étonnant que les trois médias ne les aient pas évoquées dans leurs articles, préférant ainsi passer sous silence l'état d'esprit des accusateurs de Quantic Dream.

Des cas de harcèlement sexuel ?

Pour le trio de médias, ces photomontages seraient symptomatiques des coulisses de Quantic Dream. *Le Monde* rapporte que « *de nombreux témoins dénoncent par ailleurs des blagues à connotation raciste ou homophobe, tant au sein des équipes que de la hiérarchie.* » Des accusations de racisme et d'homophobie que dément David Cage, qui rappelle ses

Les commentaires reçus par *Le Point* sur Twitter sont parfois violents (ceux reçus par le journaliste de *VentureBeat* le sont aussi, mais nous avons opté pour ceux du *Point*, car tous en français). Une partie de ces personnes au moins semble ne pas avoir lu l'article ciblé pourtant puisque *Le Point* informe que Quantic Dream a été condamnée. Rappelons que l'injure et la diffamation publiques sont punissables par les tribunaux.

Accusations de racisme au syndicat international des travailleurs du jeu vidéo

Nous apprenons de *Games Industry* que Marijam Didžgalvyte n'est plus responsable de la communication de l'organisation syndicale internationale Game Workers Unite. Des membres de la branche de Seattle (États-Unis) se plaignaient d'elle pour des « *comportements d'exclusion et d'intimidation* », des faits de « *harcèlements* » (non détaillés dans le communiqué hébergé chez… Google !). Selon l'accusée, cela ferait suite à un différend entre elle et Sisi Jiang de la société de jeux vidéo Lionkiller : la seconde souhaitant une action internationale contre le suprémacisme blanc, la première au niveau local estimant que le problème aurait donné une connotation trop occidentale à l'organisation. Mais, de son côté, Sisi (qui a quitté le syndicat depuis) affirme que Marijam lui a « *déclaré qu'ils* [au niveau international du syndicat] *ne voulaient pas aliéner les développeurs de jeux en condamnant le racisme.* » Elle se plaint aussi du refus du compte Twitter principal de relayer une cagnotte de soutien aux manifestants contre le racisme aux États-Unis suite à la mort de George Floyd. Marijam Didžgalvyte a plaidé le malentendu, en vain. La branche de Seattle exige désormais un comité pour enrayer le « *racisme latent présent dans toute l'organisation* », une accusation relayée ou confirmée par d'autres branches locales de Game Workers Unite (Los Angeles, Detroit, Argentine).

collaborations avec Ellen Page (son *coming out* est postérieur toutefois) et Jesse Williams. *Mediapart* avance, lui, que « *des blagues sexistes ou misogynes, parfois de la bouche de supérieurs hiérarchiques, quelques commentaires sur les tenues des femmes de l'équipe, des tentatives de drague plus ou moins lourdes, nous ont été rapportées…* » *Le Monde* est plus précis, décrivant un directeur délégué général « *imbu de son pouvoir et ambigu avec les femmes, adeptes des bises appuyées, des remarques déplacées. Lors de soirées professionnelles, il est accusé par d'anciennes salariées de les avoir draguées avec insistance, par exemple en tentant de les faire boire au goulot de sa bouteille.* » Ce que l'intéressé a nié catégoriquement, selon l'article. À *Mediapart*, les « *délégués du personnel indiquent avoir eu « très peu d'alertes sur ces sujets » et qu'elles ont « à chaque fois fait l'objet de discussions et d'actions avec les RH* [ressources humaines] *ou la direction* » ». Ces accusations n'étaient pas tombées lors du phénomène #MeeToo, où de nombreuses victimes de tels agissements dans le monde ont osé prendre la parole, mais quelques mois plus tard, juste avant le lancement du jeu *Detroit: Become Humain*, qu'elles auraient pu plomber commercialement le public étant devenu très sensible sur ce sujet. Coïncidence de calendrier ?

Plus grave encore : en septembre 2019, c'est un article de *20 Minutes* qui revient à la charge, évoquant « *deux hommes travaillant au sein du studio* […] « *L'un d'eux est connu comme le loup blanc dans la profession. Tout le monde sait que c'est un gros prédateur », précisent plusieurs des femmes interrogées.* » Un peu plus tôt, un communiqué avait été diffusé : « *Le syndicat Solidaires Informatique se joint à l'organisation internationale Game Workers Unite pour un appel à témoignages concernant la présence de prédateurs sexuels éventuels à Quantic Dream. Nous avons été informés d'actes de harcèlements sexuels et d'agressions sexuelles commis sur des femmes travaillant et ayant travaillé dans l'entreprise. Ces délits sont extrêmement graves et sont punis par la Loi, cependant ils semblent se répéter impunément depuis plusieurs années à cause d'une forte omerta, cela doit cesser.* » Le syndicat est très affirmatif dans sa deuxième phrase et son accusation a été relayée par plusieurs journalistes sans prendre de pincette. Y a-t-il a eu dépôt de plainte à la police ? Nous avons contacté le syndicat pour en savoir plus, mais nous n'avons pas eu de réponse. Par contre, quelques jours plus tard, nous apprenions qu'il était… poursuivi en diffamation depuis juillet 2019. La justice devra donc estimer s'il y a eu des « *actes de harcèlements sexuels et d'agressions sexuelles.* » En attendant, selon *Le Point*, « *chez les délégués du personnel de Quantic Dream, on assure n'avoir jamais reçu un signalement pour harcèlement sexuel* » et, dans un communiqué, la direction déclarait : « *nous encourageons vivement toute personne concernée par le harcèlement à contacter les autorités compétentes.* »

Les conditions de travail

Outre des accusations de sexisme et de blagues racistes, la direction se voit reprocher dans les articles le travail lui-même. Selon *Mediapart*, concernant David Cage, « *le mot « tyrannique » revient régulièrement pour décrire son comportement professionnel, tout aussi souvent opposé à son caractère, ouvert et avenant, dès lors qu'il ne s'agit pas de la création de jeux.* » Il lui est reproché de chercher à imposer ses idées dans les jeux, ce qui gênerait certains employés. Mais après tout, c'est lui le *boss*, non ? Alors qu'il décide… et assume si le choix est au final mauvais. Malheureusement, il lui est reproché aussi des conséquences au niveau du planning. Des (ex-)salariés se sont plaints à nos confrères des périodes de *crunch*, faisant état de semaines de 50 à 60 heures dont le payement est, parfois, mis en cause. Ce *crunch* correspond aux dernières étapes de conception de jeu ou pour des versions intermédiaires à l'occasion de salons, par exemple. La société a répondu que ce rythme est sur la base du volontariat, les heures supplémentaires étant déclarées et payées (toutefois la règle de calcul était compliquée à une époque avec un système de crédit d'heures).

Canard PC affirme que « *des jeunes gens en CDD* [contrat à durée déterminée] *dont on souhaite prolonger un peu la collaboration verront leur contrat déchiré et remplacé par un autre. Pour coller au plus près des besoins de l'entreprise (le calendrier de production étant soumis à de fréquents changements).* » Niant une « *politique* », la direction a admis la possibilité d'erreurs commises par des employés de la comptabilité ou des ressources humaines.

Le trio de médias

Une partie des employées de Quantic Dream d'origines diverses réunies sur une photo à l'occasion de la journée de la femme (non, ces sourires ne sont pas un photomontage !)

rapporte une procédure étrange qui aurait été répétitive dans la société (le nombre de cas recensés diverge toutefois selon les médias). Prenons la version de *Mediapart* qui évoque 10 cas pour l'année 2016 en lien avec la fermeture d'un service : « *Le salarié est d'abord licencié, puis il conteste ce licenciement, ce qui donne lieu à une négociation avec l'entreprise, au terme de laquelle il reçoit une somme complémentaire sous la forme d'une indemnité transactionnelle* […] *Ce ballet en trois mouvements se renouvelle souvent, avec des courriers types où seuls les noms, les dates et les sommes versées diffèrent* […] *Selon Sophie, « tout est rédigé en même temps » : les lettres de convocation à l'entretien préalable, puis de licenciement, la contestation du salarié, puis la transaction* […] *À notre connaissance, la transaction versée pour ces départs n'est pas systématiquement déclarée à Pôle emploi, contrairement aux règles en vigueur. Cela évite au salarié la période de carence avant le versement des indemnités chômage, qui est appliquée par Pôle emploi lorsqu'une somme supérieure aux indemnités légales de licenciement a été payée.* » Cela aurait arrangé d'ex-salariés, mais selon « Sophie » la pression serait mise sur les récalcitrants. Quantic Dream a assuré au média « *respecter les procédures* [légales et] *qu'un autre poste, « au même échelon et au même salaire », a été proposé à la salariée, qui l'a refusé.* »

Un des cas est particulier puisqu'il s'agit de Guillaume de Fondaumière, le fondateur et vice-président du Syndicat national des jeux vidéo (SNJV) français (après en avoir été président), vice-président du conseil d'administration de son équivalent continental (l'European Games Developer Federation) après en avoir été président aussi, administrateur de PEGI (l'organisme qui classifie les jeux vidéo en fonction de l'âge des joueurs)… *Mediapart* raconte que « *Fin 2016, une lettre de licenciement, signée par David Cage, lui reproche « un comportement très personnel » et regrette son « refus de suivre les directives ».* […] *Mais malgré ce licenciement, Guillaume de Fondaumière est resté dans l'entreprise.* […] *Il était jusque-là rémunéré au titre de deux postes différents, directeur général délégué, mais aussi* producer *exécutif du studio. C'est cette seconde casquette qu'il a perdue dans la procédure, mais il est resté directeur général de Quantic Dream. Il n'a pas non plus perdu de salaire et a même obtenu une augmentation de quelques milliers d'euros. Ce qui ne l'a pas empêché pour autant d'empocher une coquette somme dans l'opération : plus de 100 000 euros, au titre des indemnités de licenciement et de l'accord transactionnel, conclu avec l'entreprise qu'il dirige ! Embarrassant pour celui qui est une des figures majeures du secteur en France.* »

L'explication juridique

Guillaume de Fondaumière a nié toute irrégularité à *Mediapart*, sans vouloir détailler sa position, ni à nos confrères ni à nous. L'augmentation de rémunération au poste de directeur général délégué (DGD) ne nous choque pas si elle correspond aussi à une augmentation du temps travaillé, puisque de l'autre côté la rémunération et le temps passé en tant que *producer* sont réduits à néant. Une augmentation de salaire peut aussi permettre de cotiser pour une assurance chômage facultative (lire la suite). La transaction ne nous choque pas non plus : cela ne regarde que ceux qui payent, c'est-à-dire les actionnaires, si les prélèvements sociaux et fiscaux relatifs sont effectués au passage dans le respect de la loi bien sûr.

La chose importante que n'expliquait pas *Mediapart* au lecteur qui pourrait être novice en la matière, c'est que dans une société anonyme (SA) un poste de DGD est un « mandat social » pour la représenter, par exemple pour signer des contrats. Le DGD est choisi par le conseil d'administration, lui-même choisi par les actionnaires (dont, ici, David Cage à 60 %). En fait, dans un premier temps (depuis 2011), il semblerait (à en croire le Bulletin officiel des annonces civiles et commerciales) que Guillaume de Fondaumière n'était qu'administrateur (un mandat social, là encore), pas DGD, contrairement à ce qu'on a pu lire dans de nombreux médias pendant des années. Une formalité oubliée par la société ?

Censuré à une conférence du SNJV

Fin 2013, notre rédacteur en chef avait été invité à une table ronde par l'organisateur d'une conférence destinée à des créateurs indépendants de jeux vidéo. Sans contrepartie, cette participation (annoncée publiquement) avait pour objectif de partager des conseils pour faire parler de ses créations dans la presse quand on est désargenté. Finalement, cette participation a été annulée sur demande du coorganisateur SNJV, dont des responsables n'avaient visiblement pas digéré un précédent article sur les échecs entrepreneuriaux de l'un d'eux paru quelques mois plus tôt dans notre publication sœur *Pocket Videogames*. Au SNJV, certains intérêts personnels semblent primer sur l'intérêt général de ses membres.

Des documents volés ?

Le Monde a confronté le directeur général délégué à un enregistrement audio réalisé à son insu et qui concernerait, au moins, son licenciement de son poste de producteur. Un enregistrement « *sorti de son contexte* », « *tronqué* » et qui « *n'a aucun sens* », selon l'intéressé. Il dit probablement vrai, puisqu'il aurait expliqué dedans que son changement de statut lui permettrait de toucher l'assurance chômage si nécessaire, alors qu'en réalité un tel changement entraînerait le contraire. L'enregistrement pourrait donc, effectivement, concerner tout autre chose.

Lors de leur entretien avec les journalistes du trio de médias début 2018, les responsables de Quantic Dream ont eu le sentiment que les journalistes avaient aussi en mains des données, notamment comptables et administratives, qui leur avaient été volées. Ils avaient porté plainte en juillet 2017 pour « *intrusion illicite dans un système informatique* » en visant notamment l'ancien responsable informatique suspecté d'avoir récupéré des documents internes avant de quitter la société. Cette plainte a été classée sans suite après audition, garde à vue et perquisition de matériels informatiques. Dans la foulée, Quantic Dream a déposé une deuxième plainte similaire, mais cette fois avec constitution de partie civile, ce qui entraîne d'office la nomination d'un juge d'instruction.

Une troisième plainte pour le même motif a été déposée en octobre 2019. Une source nous indique que la société française d'objets connectés Parrot (sans rapport avec le jeu vidéo, à part à titre accessoire quelques anciens jeux pour téléphones) a alerté Quantic Dream après avoir trouvé dans son système informatique des fichiers du studio de jeux qui n'avaient rien à faire là. Un constat d'huissier a été réalisé. Coïncidence ? L'ancien responsable informatique de Quantic Dream travaillait désormais dans cette société (ce n'est plus le cas). Parrot n'a pas souhaité commenter. *Mediapart* a évoqué ce dernier épisode en une phrase. *Canard PC* et *Le Monde* ont été plus laconiques encore sur ces plaintes, ce qui là encore peut faire pencher la balance du côté de la thèse d'une enquête à charge contre Quantic Dream.

Le cas Marie Smog

Parmi les personnes que nous avons contactées, il y a « Marie Smog » (pseudonyme), qui se présente comme victime de Quantic Dream, voire agit en porte-parole de toutes les victimes, et qui est très active contre la société sur Twitter. Précisons qu'il n'y avait aucune femme au service informatique (une femme d'un service administratif a cependant contesté aux prud'hommes un licenciement en juillet 2017 pour faute grave, ce n'est pas d'elle dont nous parlons ici). Cette personne, un homme donc, n'a pas souhaité donner suite à notre proposition de témoignage. C'est son droit et nous n'avons pas insisté. Elle aurait pu en rester là, mais elle a décidé de se lancer dans des calomnies publiques contre nous : « *soyez fiers de participer à cette communication qui discrédite Quantic Dream et sa direction qui ne cesse de répandre rumeurs et dénigrements à l'encontre des victimes* », etc. Alors que nous avions à peine commencé notre enquête sans savoir où elle allait nous mener et sans le moindre *a priori* sur notre interlocuteur, nous avons donc très rapidement compris que nous avions affaire à une personne capable de mentir pour nuire à autrui (attention, cependant, son comportement ne doit pas remettre en cause la crédibilité des autres victimes reconnues ou revendiquées !). De toute évidence, Marie Smog nous reprochait de vouloir donner la parole à Quantic Dream. Or si un(e) journaliste veut comprendre, faire un article neutre et objectif, il/elle se doit de donner la parole à toutes les parties. Si nous avions obligation de faire un article à charge contre Quantic Dream pour recueillir le témoignage de cette personne, il y a lieu de se poser des questions sur les articles qui ont pu avoir son témoignage.
Marie Smog s'en prend aussi à son propre avocat de départ. Il y a eu certes un litige concernant le payement d'honoraires indus, mais l'ex-client va plus loin et passe publiquement, en quelques mois, de « *trois victimes ont dû changer d'avocat, gros soupçon de corruption* » à « *nous, on paye des avocats soudoyés.* » Aucune preuve n'est fournie par lui. Dans la liste de ses griefs, l'homme ajoute « *articles de presse et vidéos sponso*[risées]. » Là, à lire le reste de ses interventions, semblent visés notamment *VentureBeat* et *Le Point* qu'il accuserait ainsi d'être « à la solde » du studio de jeux vidéo au mépris des règles de déontologie journalistiques. Une fois de plus, aucune preuve n'est fournie par lui.
Si nous comprenons qu'une victime veut cacher son identité, un pseudonyme utilisé pour diffuser de fausses informations et des calomnies contre des tiers ne mérite aucune protection particulière.

Selon la même source officielle, l'homme n'est devenu DGD que fin 2018, bien après l'article de *Mediapart*.
Peu importe : qu'il ait été administrateur ou DGD, un mandat social n'est pas un emploi salarié au sens classique du terme. Les règles juridiques sont différentes entre les deux statuts (par exemple, la nomination doit être notifiée au tribunal de commerce, un tel mandataire ne cotise pas de manière obligatoire à l'assurance chômage et ne peut donc en bénéficier, etc.). Les deux statuts sont légalement cumulables si l'activité salariée est réelle avec un lien de subordination (ce qui n'est contesté par personne ici). Si le président de la société a estimé que le producteur exécutif salarié ne répondait plus aux exigences pour son poste, les actionnaires ont pu estimer que le mandataire avait, lui, parfaitement réussi l'autre mission qui lui avait été confiée. Quand *Mediapart* parle de « *vrai-faux licenciement du directeur général* », il déforme la réalité juridique d'une situation qui, il est vrai, peut paraître « *absurde* » au non initié. Un tribunal, plus qu'initié lui, pourrait toutefois lui pardonner une telle imprécision au nom de la liberté de (ton de) la presse. Mais…

Les trois médias se contredisent

De son côté, *Canard PC* publie : « [David Cage] *lui annonce son licenciement. Lequel n'entend pas se laisser faire, et conteste par écrit ce licenciement le 7 octobre 2016* […] *le rebelle à qui l'on reprochait en juin « un comportement très personnel », une mauvaise exécution des tâches qui lui étaient données et enfin un « refus de suivre les directives » réintègre immédiatement l'entreprise dès la fin de son préavis de licenciement, en tant que directeur général délégué.* » Une autre version que *Mediapart* donc, puisque ce dernier affirmait que Guillaume de Fondaumière était déjà directeur général délégué. Les dates ne collent pas non plus : la lettre de licenciement date-t-elle de juin ou de fin 2016 ? Enfin, le passage de *Canard PC* porte le sous-titre *Quand la direction se licencie elle-même*, une assertion limite trompeuse, mais le magazine de jeux vidéo n'est pas poursuivi en diffamation (lire encadré).
Penchons-nous sur ce que raconte *Le Monde* maintenant : « *selon des documents internes auxquels* Le Monde *a pu avoir accès,* [Guillaume de Fondaumière] *s'est autolicencié le 30 septembre 2016 pour « mésentente avec la direction » pour se réengager le lendemain à un autre poste.* » Là, les dates (il était même question de 31 septembre dans un premier temps !) ne collent pas avec celles de *Canard PC*. *Le Monde* partage, par contre, avec le magazine de jeux vidéo la thèse du nouveau poste, en opposition avec *Mediapart*. Enfin, *Le Monde* accuse Guillaume de Fondaumière de s'être autolicencié alors que les deux autres médias affirment que c'est David Cage qui a procédé au licenciement.
Bref, voilà trois médias qui affirment avoir travaillé ensemble et avoir eu les mêmes informations, mais qui racontent trois histoires contradictoires au niveau des faits (la version la plus proche de la réalité nous semblant celle de *Mediapart*) ! Quoi qu'il en soit, dans le fond, les trois versions laissent planer un doute nauséabond sur Guillaume de Fondaumière, alors que comme nous l'avons expliqué la procédure était légale. Des journalistes soucieux de trouver la vérité pour en informer leurs lecteurs sans flou ni erreur auraient relayé éventuellement l'avis d'un juriste.

Contrôle du fisc et de l'Urssaf

Après les graves accusations dans les articles des trois médias - et on peut penser que c'est lié - Quantic Dream a subi un contrôle fiscal en 2018 et un contrôle Urssaf en 2019 (relatif aux cotisations sociales). En général, de tels contrôles portent sur les trois années civiles précédentes. Selon *Le Point*, ces contrôles se sont soldés par… un remboursement de 47 471 € de l'Ursaff pour

trop versé. Ce qui semblerait confirmer que Quantic Dream a agi légalement (la société ne nous a pas permis de lire les documents relatifs à ces contrôles). Chez *VentureBeat*, David Cage a évoqué un troisième contrôle conclu sans suite (Quantic Dream n'a pas voulu nous confirmer lequel) – il pourrait s'agir de l'inspection du travail (option la plus probable), voire de la Cnil ou du Défenseur des droits, tous saisis. Le trio de médias n'a pas informé ses lecteurs de ces conclusions blanchissant Quantic Dream.

Des employés quasi tous heureux ?

En parallèle, la société a commandé en 2019 à l'institut People Vox un sondage concernant « *la qualité de vie au travail. 90 % des salariés ont accepté de répondre anonymement au questionnaire proposé. 94 % d'entre eux se déclarent satisfaits de Quantic Dream comme employeur, et 98 % se disent contents des relations humaines dans l'entreprise* », peut-on lire dans *Le Point*. *Canard PC* conteste que ce sondage puisse servir d'objection à son article, car il a été payé par la société et les faits décrits par lui datent d'une autre année. Nous avons demandé à Quantic Dream ce rapport, elle ne nous l'a pas communiqué.

Le Monde affirme « *en tout, en 2015 et 2016, une cinquantaine de collaborateurs ont quitté l'entreprise, dont des cadres qui avaient été recrutés à l'étranger. Un an et demi plus tard, ces derniers ne veulent plus entendre parler de Quantic Dream.* » Avec, peut-être, la volonté de faire croire à une fuite massive de l'équipe. Or l'auteur de ces lignes, spécialisé en jeu vidéo, ne peut ignorer une spécificité de cette industrie qu'il ne rappelle pas à ses lecteurs du grand public : les métiers nécessaires évoluent en fonction de l'avancement des projets, d'où un recours massif aux contrats à durée déterminée. Quantic Dream, acteur de taille moyenne du secteur, n'a pas assez de projets en cours simultanément pour transformer certains contrats en durée indéterminée. Selon les chiffres officiels, en 22 ans d'existence, plus de 1 000 employés sont passés dans ses rangs. L'effectif actuel varie entre 150 et 200 personnes, selon les périodes.

Bien sûr, comme dans toutes les sociétés, il peut y avoir malheureusement des insatisfactions, voire des litiges (d'ailleurs, *Le Monde* n'a-t-il jamais été poursuivi aux prud'hommes ?). Quantic Dream affirme à *VentureBeat* qu'en dehors des procédures relatives aux photomontages elle n'a eu qu'une seule affaire perdue aux prud'hommes, sans rapport. La société précise que l'ancienneté moyenne dans ses rangs (hors contrats à durée déterminée, on imagine) est de sept ans, ce qui ne colle pas vraiment avec des employés malheureux. Une grosse partie de l'effectif a entre 30 et 50 ans, avec souvent des obligations familiales. 15 % du personnel est composé de femmes, ce taux n'est pas spécifique à Quantic Dream, c'est malheureusement la moyenne dans l'industrie des jeux vidéo et, plus largement, de l'informatique. À la décharge de cette société, les femmes représentent chez elle environ 50 % du personnel d'encadrement, ce qui est rare ailleurs dans le monde de la technologie (quelle est la place des femmes dans l'encadrement de *Canard PC* ?).

Même si nos confrères du trio de médias ont aussi donné la parole à des (ex-)employés qui ont déclaré apprécier ou avoir apprécié l'ambiance de Quantic Dream, le sentiment global à la lecture de leurs enquêtes peut paraître négatif contre cette société. De notre côté, nous avons interrogé des dizaines d'employés et d'anciens employés (contactés par nos soins, nous insistons). Pas un seul ne nous a confirmé les accusations portées contre Quantic Dream qui ont déjà été démenties par elle. Les personnes en conflit avec la société, et qui peuvent avoir pour certaines un intérêt à la traîner dans la boue, sont-elles vraiment nombreuses ou y a-t-il eu effet grossissant sur des cas plutôt rares dans les articles du trio de médias ? Peut-être n'avons nous pas eu de chance lors de notre « pèche » aux témoins ? Nous avons donc demandé à nos confrères de prévenir leurs propres témoins que nous préparions un article et qu'ils pouvaient nous contacter (bien sûr, leur anonymat aurait été garanti). Nos confrères n'ayant pas donné suite, nous ne pouvons donc pas confirmer leurs dires.

Des biais politiques ?

Alors que le SNJV est parfois accusé de représenter avant tout le patronat des sociétés de jeux vidéo, le syndicat des travailleurs et travailleuses du jeu vidéo (STJV), jeune et encore assez peu représentatif, s'est positionné contre Quantic Dream. Nous l'avons contacté, lui aussi, afin de pouvoir, enfin, recueillir des témoignages d'employés anciens ou actuels insatisfaits de cette société. En vain, là encore.

Dans les colonnes de *VentureBeat*, on peut lire le témoignage de Vincent Jolly, du journal *Le Figaro*, qui a mené une enquête sur

Canard PC : un lectorat volatil

Quantic Dream n'a pas porté plainte en diffamation contre *Canard PC*. Le magazine y voit la preuve qu'il racontait la vérité, rien que la vérité (alors que nous venons de démontrer le contraire). Il y a, peut-être, une autre explication : le studio de jeux vidéo souhaitait éviter à *Canard PC* de vivre une situation économique très difficile et de s'en voir reprocher les conséquences par des joueurs. En effet, en 2018, *Canard PC* avait déjà lancé un appel aux dons auprès de ses lecteurs, expliquant avoir de graves difficultés économiques à cause du distributeur de presse Presstalis (le magazine n'avait pas dit à ses lecteurs que la grosse retenue de 25 % n'était que temporaire ; elle a été remboursée comme promis depuis, au final ne restait qu'une autre retenue de 2,25 %). Mais comme nous l'avions expliqué (acbm.com/virus/¬num_36/1010_Com¬ment_Canard_PC_a_¬pigeonne_ses_lec¬teurs.html), le plus gros problème – passé sous silence par *Canard PC* – est la grosse perte de lecteurs qu'a subie le magazine depuis sa belle époque et qui représente bien plus que ces 2,25 % de frais Presstalis en sus. Finalement, la société de presse a pu finir cette année-là avec un petit profit, mais sans les dons de lecteurs, cela aurait été des pertes (lire *Virus Info* 42). Les chiffres financiers 2019 ne sont pas encore connus. Presstalis a été mise en redressement judiciaire depuis. Parti chez le distributeur concurrent MLP entretemps (et donc non concerné par le blocage récent de 100 % du produit des ventes), *Canard PC* évoque une possible « *campagne de financement participative plus élaborée* » à venir (ce serait sa troisième).

Quantic Dream vs Twitter

Un autre volet annexe de cette affaire n'a pas été traité par les autres médias. En décembre dernier, Quantic Dream et Twitter se retrouvaient à la Cour d'appel de Paris. Mais – surprise ! – les sociétés ont indiqué au juge qu'il n'avait plus besoin de trancher : elles ont trouvé un accord amiable dans l'intervalle. Tout avait commencé en 2018 lorsque Quantic Dream avait exigé de connaître des informations concernant des messages sur Twitter qu'elle considérait comme portant atteinte à ses intérêts. Dans un premier temps, le tribunal avait ordonné que le réseau social se plie à cette requête, mais Twitter avait demandé, et obtenu, sa rétractation en référé, contestée par Quantic Dream en appel donc. Quels étaient les messages ciblés par la société de jeux vidéo ? Quels sont les termes de l'accord avec Twitter ?

Des employés et anciens employés heureux

« *Selon des informations du* Monde*, les dirigeants de Quantic Dream ont invité leurs employés à les défendre publiquement* », écrit le quotidien. C'est possible. Pourtant, de notre côté, il nous a été difficile de recueillir des témoignages en contactant directement employés et anciens employés, tous devenus quasiment « paranoïaques » à l'égard des journalistes. Dans *Le Point* (qui fait figure d'exception), nous avions déjà pu lire des déclarations comme « *ces articles étaient tellement à côté de la plaque* [...] *personnellement, du jour au lendemain, je me suis énormément méfié de tous les médias. Je ne suis pas le seul à le penser cela, on en a beaucoup discuté avec mes collègues* » ou « *pourquoi ça n'intéressait pas les journalistes de nous rencontrer ? C'est facile d'écouter un ancien employé. Vous balancez des ragots, mais nous, on reste avec ça sur le dos, et jamais la vérité n'est rétablie* », « *ces articles, ça veut dire qu'on aurait fermé les yeux sur ce qui s'apparente à de l'esclavage* »... Un délégué du personnel (différent de celui impliqué pour les photomontages) se plaignait que « *même des anciens collaborateurs nous ont dit que leurs propos avaient été déformés. Ça a changé ma vision de votre métier. Voir à quel point les gens peuvent déformer les choses, ça m'a sincèrement choqué.* »

Du coup, beaucoup de méfiance à notre égard (surtout que chez *Virus Info* nous sommes connus pour « taper » sur les sociétés...), mais jamais la moindre animosité, sauf chez la personne utilisant le pseudonyme de Marie Smog, ce qui a paradoxalement incité les autres à se confier à nous. Finalement, tous les témoignages que nous avons réussi à obtenir ont été globalement positifs. Tous.

Des salariés cyber lynchés par... des joueurs ?

Ces témoignages ont été possibles à une condition : que nous respections leur anonymat. Quelques-uns avaient défendu publiquement Quantic Dream dans le passé, mais « *à la moindre information contredisant le point de vue énoncé sur* Canard PC*,* Le Monde *ou* Mediapart*, une armée de comptes* [sur Twitter] *viennent insulter les gens qui ont posté* [...] *Cela me fait presque penser à la « ligue du LOL » même si cela n'a bien évidemment pas tout à fait les mêmes conséquences* », nous explique un employé. Parmi ces comptes qu'il n'est pas toujours possible d'identifier de manière certaine, de nombreuses personnes qui semblent totalement étrangères à l'affaire et qui n'ont que faire de découvrir les différentes versions. Il se trouve que si les jeux de Quantic Dream, misant sur le côté narratif et l'émotion, ont un succès commercial, ils ont aussi beaucoup de « haters » (détracteurs) parmi des joueurs qui leur reprochent leur manque d'interactivité notamment. Certains d'eux pourraient estimer légitime de projeter cette haine aussi contre des employés de la société eux-mêmes, surtout dans le contexte actuel.

Les témoignages d'(ex-)employés ont été recueillis auprès de personnes aux profils différents, tous n'étant pas soumis aux mêmes contraintes : administratif, programmeur, artiste... Nous ne préciserons pas le sexe de nos interlocuteurs, les professions et autres dans la suite pour éviter de rendre les profils reconnaissables. Plusieurs femmes nous ont répondu, aucune ne s'est plainte à nous d'un comportement déplacé qu'elle aurait vu ou subi en raison de son sexe.

Un ancien employé, resté quelques années en poste, nous déclare concernant l'incident des photomontages qu'il n'a « *rien ressenti de particulier : je suis habitué à cette pratique (que je ne cautionne pas) depuis les études, et je consulte peu les* mails *extra-professionnels. Je n'ai pas prêté attention au* mail *de l'incident. L'entreprise ayant traité le problème rapidement, je n'ai jamais été confronté aux images problématiques au sein de l'entreprise.* » Quant à son traitement médiatique, il déclare l'avoir trouvé « *disproportionné, et qui mêlait des sujets sans rapport.* » De manière générale, il décrit les conditions de travail et de salaire comme « *bonnes. Je n'ai pas ressenti de stress ni de pression de mes* managers*. L'ambition des projets fait que la charge de travail peut être élevée, mais cela varie suivant le stade d'avancement.* » Par rapport à ses expériences antérieures et postérieures dans le jeu vidéo, il les juge similaires : « *Les horaires sont globalement les mêmes, les à-cotés et activités extra-professionnelles relativement proches et on retrouve le même type de profils. Développer un jeu reste une tâche ardue qui peut occasionner des frictions dans les plannings.* »

Un autre ancien employé a, lui, ressenti les photomontages « *comme quelque chose qui m'a fait rire (j'ai été régulièrement sur des montages), comme quelque chose de purement fait entre collègues qui passaient du temps le midi à déconner entre eux. Les montages étaient envoyés seulement aux personnes présentes dessus. Certaines personnes pouvaient évidemment ne pas trouver ça drôle du tout, mais du coup elles n'apparaissaient alors plus si elles le voulaient.* » Le traitement médiatique de l'épisode a été pour lui « *extrêmement blessant, biaisé, et je ne préfère pas m'étendre.* »

Concernant le travail en général chez Quantic Dream, il parle d'« *années géniales là-bas. L'ambiance et le travail ont été un super moteur pour moi. Évidemment, comme partout, il y a des moments plus compliqués que d'autres, c'est sûr, mais ce n'est pas du tout ce que je retiens de mon passage. C'est mon expérience personnelle. D'autres n'ont peut-être pas la même, cela dépend de tellement de choses, mais je pense ne pas être le seul à avoir aimé y travailler. Loin de là. Les conditions de paye étaient classiques je dirais. Les heures supplémentaires payées, les repas du soir si il fallait assurer un coup de bourre aussi. Je n'ai jamais eu à me plaindre.* » Un employé actuel nous dit qu'« *au niveau des conditions de travail chez Quantic Dream, je les trouve plutôt très bonnes. C'est très agréable de retrouver mes collègues et je suis très content de faire partie de cette société.* [Je] *n'ai jamais eu à faire de* crunch*. Ce n'est bien sûr pas le cas de tout le monde* [...] *Niveau salaire, je suis convaincu qu'à mon entrée, j'aurais pu obtenir un meilleur salaire dans le reste de l'industrie (SSII, finance ou autre), mais le cadre de travail n'est pas le même* [...] *En revanche mon évolution de salaire après la sortie de* Detroit [...] *a été très correcte et je suis tout à fait satisfait de mon niveau actuel de salaire.* »

Par manque de place, nous arrêterons ici, les témoignages suivants étant très similaires. Nous aurions aimé avoir des témoignages plus critiques pour les relayer de la même façon, mais impossible faute d'en avoir reçu. Dans un prochain numéro si les contradicteurs se montrent plus constructifs ?

Nos valeurs

Notre équipe est formée de femmes et d'hommes de toutes origines géographiques, religieuses et sociales, de toutes orientations sexuelles, de tous âges ainsi que de personnes handicapées.
Nous limitons autant que possible nos consommations de papier, électricité, eau, etc. Nos magazines sont imprimés généralement sur du papier recyclé. Nous utilisons des matériels de récupération autant que possible (meubles, ordinateurs...). Nous préférons les transports en commun, bicyclettes, etc. Nous évitons les déplacements qui ne sont pas indispensables...
Nous soutenons financièrement et publicitairement des associations caritatives comme l'Armée du Salut (dernier don en mars 2020 d'un montant de 2000 €).

l'affaire, mais a finalement choisi de ne rien écrire : « *J'ai couvert Quantic Dream fréquemment les dernières années et, connaissant certains des employés moi-même, je ne vois aucune preuve non biaisée qui confirmerait les affirmations des investigations* [...] *Il n'y a, de mon point de vue, simplement aucune histoire ici.* » Notez qu'il parle d'« *employés* », alors que *Canard PC* dans un entretien à *Gamekult* a voulu faire croire que dans cette phrase il était question du p.-d.g. de Quantic Dream. Il se trouve que *Le Figaro* est un média de droite, à l'inverse de *Mediapart*, très à gauche. Dans un passage où *Le Point* évoque « *l'influence des biais idéologiques* », *Mediapart* répond n'avoir « *découvert l'existence du STJV qu'au cours de nos enquêtes, et contrairement à ce que sous-entendent les dirigeants de Quantic Dream, nous n'avons pas établi un partenariat informel avec le syndicat, ou même été manipulés par lui.* »

La contre-attaque

Début 2018, Quantic Dream a porté plainte en diffamation contre *Mediapart* et *Le Monde* (mais pas *Canard PC*, lire encadré). L'audience au tribunal était prévue fin 2019, mais a été repoussée à mai 2021 en raison de la grève des avocats. Dans un premier temps, la direction de la société avait été conseillée par des spécialistes en communication de garder le silence et d'attendre l'issue de la procédure en justice. Mais cette dernière s'éternisant, il tarde aux plaignants d'avoir l'occasion de laver leur honneur, d'où les récentes déclarations chez *VentureBeat* et *Le Point*.
Dans un édito intitulé *Les nouveaux avocats de Quantic Dream*, *Canard PC* reproche à *VentureBeat* « *les points de vue contraires* [à ceux de Quantic Dream] *n'apparaissant que pour le principe* » allant jusqu'à dénigrer le travail de son confrère en le qualifiant d'« *embarrassant communiqué de presse.* » En fait, l'angle de l'article de *VentureBeat* portait plus sur le traitement médiatique de l'affaire que l'affaire elle-même (c'est en tout cas ainsi que l'auteur défend son travail dans un entretien avec *Gamekult*) et les journalistes mis en cause par *VentureBeat* avaient la possibilité de répondre dans cet article. Il aurait donc été plus honnête que ceux de *Canard PC* répondent longuement plutôt que de critiquer de manière insultante un déséquilibre dont ils sont la cause par leur refus de répondre. *VentureBeat* n'est pas irréprochable non plus et il aurait sans doute subi moins de critiques s'il n'avait pas cherché à faire passer abusivement son travail pour une « contre-enquête » (une forme qui aurait nécessité de contacter de nombreux employés, anciens et actuels, et sans passer par l'employeur).
Sur le fond, si le message que la direction du studio avait voulu faire passer pour sa défense avait été retranscrit complètement et fidèlement par le trio de médias - ce qu'elle conteste - Quantic Dream n'aurait pas besoin de chercher à s'épancher dans d'autres colonnes. N'en déplaise à *Canard PC*, *VentureBeat* et *Le Point* ont moins été les avocats de cette société que ceux d'un système dans lequel la presse - comme la justice - doit donner la parole à l'accusé pour lui laisser la possibilité de démontrer qu'il n'est pas coupable. Un exemple qui peut laisser penser à un travail à charge au lieu d'être à charge et à décharge : fin 2019, à l'occasion d'un énième article contre Quantic Dream, Guillaume de Fondaumière a demandé à William Audureau de rendre public un courriel que le DGD a envoyé au journaliste du *Monde*. À notre connaissance, cela n'a pas été fait.
Ironie de l'histoire, malgré les erreurs et « oublis » relevés ici, le journaliste du *Monde* a été promu entre-temps à la rubrique *Les décodeurs* dont l'objectif est de lutter contre les *fake news*. ■

Dernière minute : Ubisoft dans la tourmente

Alors que nous finissons ce numéro, de nombreux témoignages font à nouveau état de harcèlements sexuels, d'ambiance sexiste et homophobe dans l'industrie du jeu vidéo, notamment dans divers bureaux d'Ubisoft. Paradoxalement alors que plusieurs femmes passées à la fois chez Quantic Dream et Ubisoft nous en avaient dit le plus grand bien, la considérant comme un modèle. Mais elles pourraient ne pas être au courant de tout, dans un cas comme dans l'autre, surtout qu'Ubisoft est une structure de 15 000 employés dispersés dans le monde. Sans attendre les conclusions, la société a publié un communiqué où elle se dit désolée et a diligenté des enquêtes internes (insuffisant, selon nous). Elle annonce aussi revoir ses procédures pour comprendre où il y a eu défaillance, afin de mieux prévenir et bloquer tout comportement inapproprié.

Les secrets des cartes de stations-service

Cartes de lavage de voitures, de fidélité, ou de paiement de carburant, les pétroliers proposent depuis longtemps une vaste panoplie de cartes privatives à la clientèle de leurs stations-service. À puce ou magnétiques, elles suscitent une telle convoitise qu'une analyse approfondie de leurs mécanismes de sécurité était bien tentante…

Patrick Gueulle

Avec un prix du carburant qui n'en finit pas de flamber, des programmes de lavage de voiture de haut de gamme coûtant plus de 15 €, et des cadeaux de fidélisation de plus en plus alléchants, les cartes émises par les pétroliers prennent toujours davantage de valeur. Par quels moyens leur sécurité est-elle assurée ? Leurs défauts de jeunesse ont-ils été complètement corrigés ? Quelques surprises pourraient bien nous attendre…

Ne jamais avoir payé un seul lavage de voiture depuis 1992, ou s'approprier les points de fidélité d'illustres inconnus, ce ne sont là que deux scénarios nullement invraisemblables, et parfois même vécus. Sont-ils toujours d'actualité ? Nous allons bien voir !

Puce ou piste magnétique ?

Historiquement, les premières cartes « pétrolières » ont fait appel à la technologie de la piste magnétique. Un chiffre 7 leur a même été réservé en première position de leur numéro, contre 4 pour les Visa ou 5 pour les Mastercard, dont elles étaient techniquement assez proches. Surtout destinées aux grands rouleurs, elles servent en effet principalement à bénéficier d'une facturation différée (et parfois de tarifs avantageux) pour les achats de carburant. Tout comme les cartes bancaires, elles sont de plus en plus souvent équipées de puces électroniques apportant une sécurité accrue à cette application éminemment « sensible ».

Une exception, toutefois : les cartes prépayées non rechargeables (genre Jubileo de Total), pour lesquelles cela coûterait sans doute trop cher par rapport aux risques de fraude, qui pèsent de toute façon davantage sur les clients que sur l'émetteur…

Les cartes de fidélité, pour leur part, ont également une vocation « monétique », dans la mesure où les points qu'elles collectent peuvent servir à se procurer non seulement de menus cadeaux, mais aussi des bons d'achat ou des cartes de lavage arborant des valeurs faciales en euros sonnants et trébuchants. Pourtant, on a assisté ces dernières années à une migration en sens inverse, de la puce vers la piste magnétique (le meilleur exemple étant Shell, aussi bien en France qu'au Royaume-Uni). Problèmes de sécurité ? Coût excessif ? Peut-être, mais surtout frénésie de centralisation. Tout comme la grande distribution, les pétroliers ont relié tous leurs points de vente par un réseau informatique suffisamment performant pour que les points de fidélité puissent être gérés, en temps réel et à moindre coût, par un serveur distant. La carte (magnétique ou même à code-barres) ne contient alors plus de « compteur de points » autonome, mais un numéro d'identification identique à celui qui est imprimé dessus. Cela facilite évidemment la commande de cadeaux par Internet, tandis que les points d'une carte perdue (et mise en opposition) pourraient théoriquement être sauvés. Mais cela permet aussi de surveiller plus finement le comportement du client, notamment à des fins de « marketing »… L'inconvénient, c'est que la falsification devient enfantine : après effacement avec un simple aimant, une piste magnétique peut très facilement être réencodée avec un contenu lu sur une autre, ou construit de toute pièce. De quoi détourner, vers un seul et même compte, des points censés être acquis par plusieurs clients distincts, par exemple. Même sans aucune manipulation technique, il arrive déjà couramment qu'une caissière complaisante fasse profiter un client des points dont aurait pu bénéficier le suivant, hélas dépourvu de carte de fidélité ! Inversement, une carte « clonée » pourrait, en l'absence de code confidentiel ou de contrôle d'identité, permettre de se procurer des cadeaux en station grâce aux points de quelqu'un d'autre…

Enfantine à lire ou à copier (une seule piste encodée à 75 bpi…)

La borne de lecture de cartes d'une piste de lavage Total.

En matière de cartes de lavage, c'est Mobil qui a courageusement essuyé les plâtres de la technologie carte à puce. Il y a de cela presque trente ans, c'était une grande nouveauté, directement inspirée de la première génération de la Télécarte. Vendues « sans limitation de durée » (entendons par là sans date limite de validité), leurs 10 ou 20, puis 12 ou 24 unités de lavage étaient toujours utilisables, au moment où nous écrivions ces lignes, dans certaines stations BP, quitte à procéder à un « couper-coller » soigneux dans le cas des cartes (*collector* !) dont la puce était en position AFNOR. Les cartes vendues aujourd'hui (avec une puce à seulement six contacts en position ISO) sont cependant

La première « carte lavage » à puce de Mobil!

basées sur une technologie plus récente (dite Eurochip), présentant une sécurité bien supérieure à la précédente, si facile à émuler avec quelques composants électroniques courants. Venue sur ce marché un peu plus tard, Total a commencé aussi par la technologie dite « T1G » (puce à huit contacts), mais avec une possibilité au moins latente de traçabilité, comme nous n'allons pas tarder à le démontrer. Au bout de quelques années, ses cartes ont migré vers la très innovante puce CryptoMemory d'Atmel, ce qui leur permet d'être éventuellement rechargeables en station.
Cela nous fait donc trois technologies carte à puce à analyser, à partir d'une « matière première » facile à se procurer aux abords des pistes de lavage.

Les cartes lavage « T1G »

Développée dès 1983 pour équiper les premières Télécartes françaises, la technologie T1G doit être considérée aujourd'hui comme complètement obsolète. La tension Vpp de 21 volts nécessaire à l'écriture dans sa mémoire EPROM NMOS de 256 bits n'est d'ailleurs plus fournie par les lecteurs de cartes à puce actuellement fabriqués.
Il n'empêche que l'on peut toujours construire, pour une bouchée de pain, des lecteurs-encodeurs « maison » pour les « bricoler » à volonté (voir notre ouvrage *Cartes à puce et PC* dans la collection ETSF des éditions Dunod).
Les « cartes lavage » initialement émises sous la marque Mobil ont vu leur puce venir en position AFNOR au moment où ses stations-service sont passées sous l'enseigne BP. Rien n'a cependant changé, à ce stade, sur le plan fonctionnel. Contrairement aux Télécartes qui contenaient toutes, dans leurs 96 premiers bits « à lecture seule », un numéro de série unique et un « message d'authenticité » permettant une vérification cryptographique rudimentaire, toutes les premières « cartes lavage » Mobil ou BP de même valeur faciale avaient un contenu strictement identique!
Voici par exemple ce que l'on pourrait lire dans n'importe quelle carte neuve de 24 unités à puce « 8 contacts »:

```
1000 1000 1000 0000 0010
0000 0000 0010
0011 1100 0111 0101 1000
0010 0010 0100
1010 0001 0000 0000 0000
0000 0000 0001
0000 0000 0000 0000 0000
0000 0000 0000
0000 0000 0000 0000 0000
0000 0000 0000
0000 0000 0000 0000 0000
0000 0000 0000
0000 0000 0000 0000 0000
0000 0000 0000
```

Lorsque toutes les unités sont consommées, 24 zéros consécutifs sont devenus irréversiblement (?) des uns, ce qui permet de repérer où résident les « jetons » matérialisant le contenu monétique de la carte:

```
1000 1000 1000 0000 0010
0000 0000 0010
0011 1100 0111 0101 1000
0010 0010 0100
1010 0001 0000 0000 0000
0000 0000 0001
0000 0000 0011 1111 1111
1111 1111 1111
1100 0000 0000 0000 0000
0000 0000 0000
0000 0000 0000 0000 0000
0000 0000 0000
0000 0000 0000 0000 0000
0000 0000 0000
0000 0000 0000 0000 0000
0000 0000 0000
```

Dans le cas d'une carte de 12 unités, le mécanisme est exactement identique, mais le contenu des 96 premiers bits est légèrement différent:

```
1000 1000 1000 0000 0010
0000 0000 0010
0011 1100 0111 0101 1000
0010 0001 0010
1010 0001 0000 0000 0000
0000 0000 0001
```

À vrai dire, seul le « pouvoir financier » de la carte, exprimé en BCD, est de 12 (0001 0010) au lieu de 24 (0010 0100). La solution de facilité consistant à ne pas individualiser la zone de 96 bits de chaque carte a certainement contribué à limiter les coûts de production, tout en ayant de grandes chances, à l'époque, de passer inaperçue. C'était pourtant là une faute de sécurité que l'on considérerait aujourd'hui comme impardonnable, car rendant d'éventuels clones absolument indétectables. Or, si France Télécom a été contrainte d'appliquer des procédés anti-clones sur ses publiphones jusqu'à la généralisation de la T2G (Télécarte de seconde génération), c'est bien en raison de la déconcertante facilité avec laquelle des émulateurs rechargeables pouvaient être bricolés à partir de mémoires EPROM effaçables aux ultra-violets (en l'occurrence des « 2716 », lire *Pirates Mag'* HS3, à paraître).
Total a pour sa part adopté une démarche plus prudente, dans la mesure où ses cartes de lavage à technologie T1G n'étaient pas toutes identiques pour une valeur faciale donnée. Pendant un temps, elles n'ont même été utilisables que dans la seule station où elles avaient été achetées! Faut-il en déduire que les numéros des cartes arrivant à épuisement étaient systématiquement mis en « liste noire » (d'abord locale, puis centralisée) afin de détecter d'éventuelles tentatives de rechargement? Pour le vérifier, il aurait fallu essayer de tricher, et nous ne mangeons évidemment pas de ce pain-là...
Voici donc comment se présentait, par exemple, une carte de 18 unités lorsqu'elle était neuve:

```
1100 0001 1000 0101 0000
0000 0000 0000
1010 0000 0000 1111 1101
0001 1111 1001
0000 0000 0000 0000 0001
0001 0100 0001
0000 0010 0001 0001 0001
0010 0011 0111
0100 1001 0011 0001 0001
1101 1001 0000
```

La première carte lavage de Total.

```
0000 0000 0000 0011 1111
1111 1111 1111
1111 1111 1111 1111 1111
1111 1111 1111
1111 1111 1111 1111 1111
1111 1111 1111
```

Comparons avec une autre carte de même valeur faciale, mais épuisée:

```
1100 0011 1000 0101 0000
0000 0000 0000
1010 0000 0010 0111 1001
1011 1001 0100
0000 0000 0000 0000 0001
0001 0100 0001
0000 0010 0001 0001 0001
0010 0111 1000
0001 1010 0001 0101 0001
1110 1101 1111
1111 1111 1111 1111 1111
1111 1111 1111
1111 1111 1111 1111 1111
1111 1111 1111
1111 1111 1111 1111 1111
1111 1111 1111
```

Là encore, la zone dite « des unités » est facile à repérer, mais il est intéressant de noter que les différences entre les deux cartes se situent non seulement parmi les 96 premiers bits, inaltérables, mais également dans les 60 bits « vierges à 0 » qui précèdent le compteur d'unités. Comme leur valeur ne change pas d'une utilisation à l'autre, le semblant de « certificat » qu'ils pourraient constituer n'authentifierait donc pas le débit d'unités, mais plutôt le numéro de série. Rien n'interdit d'ailleurs de chercher une corrélation entre les quelques octets qui diffèrent ainsi d'une carte à l'autre et le numéro qui est imprimé au verso, mais le moins que l'on puisse dire est qu'elle ne saute pas aux yeux.

Les cartes lavage compatibles Eurochip

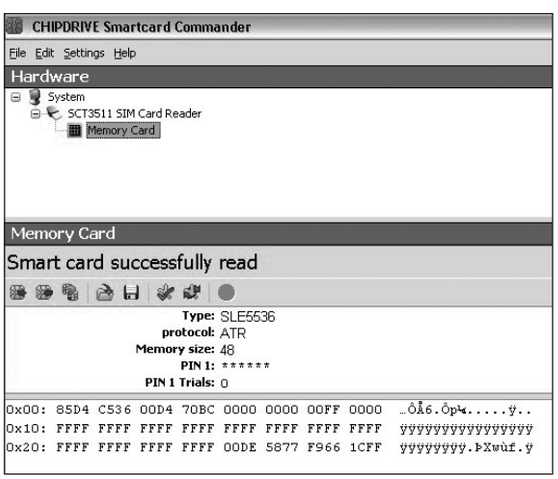
D'origine allemande (Infineon *alias* Siemens), la technologie Eurochip n'est rien d'autre que la concurrente dite « européenne » de la T2G franco-française. C'est elle qui a été retenue pour équiper les « cartes lavage » BP lorsque les

La « carte lavage » BP de seconde génération (puce Eurochip à 6 contacts).

bornes de lecture des pistes à rouleaux ont été modernisées. En introduisant au passage de nouvelles valeurs faciales : 36 unités, mais également 6, destinées à être offertes à titre promotionnel.
Comme il aurait été commercialement et juridiquement périlleux de rendre inutilisables du jour au lendemain des cartes vendues sans date de péremption, une possibilité de lecture des anciennes (et donc aussi de leurs éventuels clones !) a toutefois été maintenue.
Dans une telle carte fonctionnant selon le principe bien connu du « boulier », les unités sont enregistrées dans des groupes de huit bits faisant office de « compteurs » par 1, 8, 64, 512, et 4096. Dans l'exemple ci-dessous, trois bits étant à 1 dans le compteur « par 1 », la carte contient encore 3 unités.
1010 0001 0010 1011 1010 0011 0110 1010

0000 0000 0000 0010 1101 0110 0111 1101
0000 0000 0000 0000 0000 0000 0000 0000
0000 0111 1111 1111 0000 0000 0000 0000
1111 1111 1111 1111 1111 1111 1111
1111 1111 1111 1111 1111 1111 1111
1111 1111 1111 1111 1111 1111 1111
1111 1111 1111 1111 1111 1111 1111
1111 1111 1111 1111 1111 1111 1111
1111 1111 1111 1111 1111 1111 1111
1111 1111 1111 1111 1111 1111 1111
0000 0000 0111 1011 0001 1010 0101 0100
0001 0000 1011 1101 1011 0110 1111 1111
1111 1111 1111 1111 1111 1111 1111
1111 1111 1111 1111 1111 1111 1111
1111 1111 1111 1111 1111 1111 1111
1010 0001 0010 1011 1010 0011 0110 1010

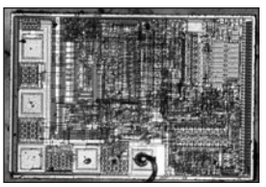
Contrairement aux cartes en technologie T1G, qui ne peuvent plus guère être lues sur un PC qu'avec des lecteurs de fabrication personnelle, les Eurochip sont reconnues par certains lecteurs du commerce. C'est ainsi que le logiciel *CardEasy*, supportant le regretté lecteur ACR 20 d'ACS ou le CyberMouse des premiers kits BasicCard, présentait le contenu de la carte sous la forme de 11 groupes d'octets exprimés en hexadécimal et… légendés.
Identifiant de la puce : 85 D4 C5
Identifiant de la carte : 56 00 40 6B BE
Compteur x 4096 : 00
Compteur x 512 : 00
Compteur par 64 : 00
Compteur x 8 : 00
Compteur x 1 : E0
Zone de contrôle : FF
Zone utilisateur 1 : 00 00
Clef cryptographique : FF FF FF FF FF FF
Zone utilisateur 2 : 00 DE 58 2A 08 BD 6D FF
On obtient des résultats voisins avec certains lecteurs (SCR3310, par exemple) de la marque Identiv (autrefois SCM Microsystems), supportés notamment par le logiciel semi-professionnel *Smart Card Commander,* dont la version 1.3 est toujours disponible en téléchargement.
Par rapport à une lecture en binaire, dans l'ordre naturel des bits, on remarquera quelques « trous » intéressants à explorer par des moyens que nous révélerons plus loin, mais surtout que chaque octet est présenté poids faible en premier, ce qui est une convention courante dans le monde des cartes à puce. Si l'identifiant de la puce (dit « numéro de silicium »), indiquant la famille du composant interne (ici Eurochip), est invariable, en revanche l'identifiant de la carte est unique. Son premier octet joue un rôle intéressant, dans la mesure où l'on peut mettre en évidence une corrélation entre sa valeur (4Ah, 52h, 56h, 92h, 96h…) et au moins deux variantes de la puce électronique. Respectivement



Exploration d'une carte lavage BP avec *Smart Card Commander*

Cette puce Eurochip mesure 1,3 x 1,3 mm.

marqués M1332 et M2432, ces « masques » sont clairement identifiables au microscope après extraction à l'acide sulfurique concentré et bouillant. Or, on murmure qu'une « Eurochip 2 » (nettement plus complexe) aurait été développée en urgence pour corriger de sérieuses failles de sécurité dans la première version du composant…



Cette nouvelle puce, pourtant plus complexe, mesure 1,3 x 0,9 mm.

De plus, chaque carte contient une clef cryptographique unique, dont la lecture est évidemment interdite de l'extérieur (elle est masquée par des octets FFh). Certaines séries de cartes, repérables selon le numéro imprimé au verso, bénéficient également de ce qui ressemble à un certificat dans leur « zone utilisateur » n° 2. Bref, on l'aura compris, l'arsenal sécuritaire est désormais sans commune mesure avec celui des cartes en technologie T1G, réduisant quasiment à néant le risque de clonage…

Ces « gros » chiffres font 20 millièmes de millimètre de haut!

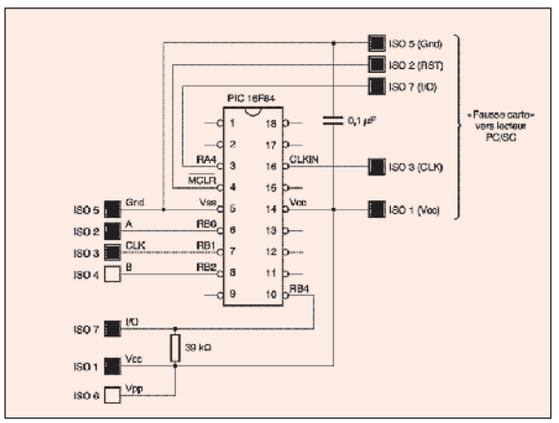
s'il est mis en œuvre à bon escient.
Beaucoup de manipulations intéressantes peuvent être menées sur ces cartes jetables, et donc présentes en grandes quantités (pas forcément vides !) dans les poubelles des stations-service. Mais comme il est souvent considéré comme illégal de les fouiller, on fera mieux de s'en procurer d'une autre façon…

Un adaptateur pour lecteur PC/SC

À défaut d'un lecteur permettant d'y lire et écrire directement, nous avons conçu un adaptateur « intelligent » capable de les rendre compatibles avec n'importe quel lecteur PC/SC, et par conséquent avec la programmation en *ZCBasic* si chère aux habitués de la BasicCard.
On voit sur ce schéma qu'un microcontrôleur PIC16F84 est tout simplement intercalé entre un connecteur de cartes à puce recevant l'Eurochip (à gauche), et une « fausse carte » en circuit imprimé de 8/10 mm (à droite) à insérer dans le lecteur PC/SC.

Un exemple de réalisation pratique de l'adaptateur.

Pour un exemple de réalisation matérielle, avec typons, on se reportera utilement aux pages 81 et suivantes de notre ouvrage *Plus loin avec les cartes à puce*, que nous avons décidé d'offrir en téléchargement gratuit (http://www.du¬nod.com/contenus¬-complementaires/car¬tes-puces-et-pc) depuis que tous ses exemplaires « papier » se sont mystérieusement volatilisés dans les entrepôts où ils étaient stockés (ce



Le schéma de l'adaptateur PC/SC pour cartes Eurochip.

qui n'a bien évidemment aucun lien avec les révélations « dérangeantes » qu'il contient sur la carte Vitale !).

Par rapport au projet d'origine, prévu pour lire et écrire dans les Télécartes T2G, il faut programmer le PIC avec un micro-logiciel spécifiquement développé pour les Eurochip.

```
; Adaptateur PC/SC pour
EUROCHIP (PIC 16F84)
; (c)2001,2010 Patrick
GUEULLE
;
list p=16F84
#include <p16F84.inc>
; Oscillateur en mode XT
; PWRT OFF
; WDT OFF
org 0
goto init
org 4
init bsf 3,5 ;bank 1
movlw 0 ;port A:
SSSSSSSS
movwf 85
movlw 10 ;port B:
SSSESSSS
movwf 86
bcf 3,5 ;bank 0
;mise au repos Eurochip
bcf 6,0
bcf 6,1
bcf 6,2
;ATR
call tx ;mode sortie
movlw .50
movwf 10
tempo call delay1
;retard avant ATR
decfsz 10,1
goto tempo
movlw 3F ;emission ATR
call even
movlw 00
call even ;emission ATR
call rx
;RESET Eurochip
bsf 6,0
call delay1
bsf 6,1
call delay1
bcf 6,1
call delay1
bcf 6,0
;attente commande
cde call rx ;mode
entree
call recv ;attente
reception octet CLA
call recv ;attente
reception octet INS
movf 11,0
movwf 2E
movwf 2D
movlw 44 ;l'octet recu
est-il 44h ? (UP)
xorwf 11,1
btfsc 3,2
goto UP ;si oui micro-
instruction UP
movlw 22 ;l'octet recu
est-il 22h ? (PROG)
xorwf 2D,1
btfsc 3,2
goto PROG ;si oui
micro-instruction PROG
call recv ;ignorer P1
call recv ;ignorer P2
call recv ;ignorer LEN
call tx ;mode sortie
call delay1
movlw 6F ;compte-rendu
d'erreur SW1SW2 = 6F00
call even
movlw 00
call even
goto cde ;attendre
prochaine commande
UP call recv ;ignorer
P1
call recv ;ignorer P2
call recv ;ignorer LEN
call tx ;mode sortie
;lecture «avant»
movlw 50
btfsc 6,4
movlw 0A0
movwf 2F ;resultat
"avant" dans registre 2F
;avance 1 bit
bsf 6,1
call delay1
bcf 6,1
;lecture «apres»
movlw 05
btfsc 6,4
movlw 0A ;resultat
«apres»
addwf 2F,1 ;2 resultats
dans registre 2F
;reponse au lecteur
movlw 90 ;SW1 = 90h
call even
movf 2F,0 ;registre 2F
dans SW2
call even
goto cde
PROG call recv ;ignorer
P1
call recv ;ignorer P2
call recv ;ignorer LEN
call tx ;mode sortie
call delay1
movlw 90 ;SW1 = 90h
call even
movlw 22 ;SW2 = 22h
call even
call delay1
;corps de la micro-
instruction PROG
bsf 6,0
call delay1
bcf 6,0
call delay1
bsf 6,1
movlw .100 ;impulsion
programmation
movwf 10
ttt call delay1
decfsz 10,1
goto ttt
bcf 6,1
call delay1
goto cde
;bibliotheque T=0
convention inverse
tx bsf 3,5 ;routine de
mise en mode sortie
bcf 85,4
bcf 3,5
return
rx bsf 3,5 ;routine de
mise en mode entree
bsf 85,4
bcf 3,5
return
send movwf 0D ;routine
UART emission
comf 0D,1
movlw 8
movwf 0E
bcf 5,4
call delay1
next bcf 3,0
rlf 0D,1
btfsc 3,0
bsf 5,4
btfss 3,0
bcf 5,4
call delay2
decfsz 0E,1
goto next
return
recv clrf 11 ;routine
UART reception
btfsc 5,4
goto delay3
call delay4
movlw 8
movwf 10
rnext bcf 3,0
rlf 11,1
btfsc 5,4
bsf 11,0
call delay1
decfsz 10,1
goto rnext
parity call delay4
;ignorer le bit de
parite recu
comf 11,1 ;bit a 1 =
niveau bas (convention
inverse)
return
call delay1
even call send
;emission d'un octet en
parite paire
bsf 5,4
call delay1
bsf 5,4
call delay1
return
odd call send ;emission
d'un octet en parite
impaire
bcf 5,4
call delay1
bsf 5,4
call delay1
return
delay4 movlw .34
;temporisation 1,25 bit
goto time
delay3 movlw .14
;temporisation 1/2 bit
call time
goto recv
delay2 movlw .27
;temporisation 1 bit
(104 uS a 9600 bauds)
goto time
delay1 movlw .28 ;duree
d'un bit de start/stop
time movwf 0F ;boucle
de temporisation
redo decfsz 0F,1
goto redo
retlw 0
mute goto mute ;boucle
sans fin (mutisme et
blocage de la carte)
end ;(il faudra faire
un RESET pour repartir)
```

En pratique, on pourra soit compiler le code source assembleur EUROCHIP.ASM (disponible, comme les autres fichiers évoqués ici, sur http://acbm.com/virus/¬num_44/), soit télécharger directement le fichier EUROCHIP.HEX à « brûler » dans un PIC16F84 au moyen d'un programmateur approprié.

Grâce à cet artifice, l'Eurochip munie de son adaptateur est vue comme une carte asynchrone « T=0 », pour laquelle on pourra écrire des logiciels *ZCBasic* très simples, qui fonctionneront sur n'importe quel PC équipé d'un système d'exploitation *Windows* 32 ou 64 bits.

Quelques logiciels applicatifs

CREDEURO.BAS permet ainsi d'afficher directement le nombre d'unités que contient une « carte lavage » BP, sans se compliquer la vie en interprétant des bits ou des octets lus avec un lecteur pour cartes synchrones.

```
#include CARDUTIL.DEF
#include COMMERR.DEF
ComPort=101
Declare Command &H22
&H44 UP(S$,Disable Le)
Call WaitForCard:CLS
ResetCard:Call
CheckSW1SW2
Print»Lecture EUROCHIP
(c)2010 Patrick
GUEULLE»:Print
For F=1 To 66
S$="":Call UP(S$)
Next F
C=0
For F=1 to 5
S$="":Call UP(S$)
IF SW2=&HAA OR SW2=&H5A
Then C=C+4096
Next F
For F=1 to 8
S$="":Call UP(S$)
IF SW2=&HAA OR SW2=&H5A
Then C=C+512
Next F
For F=1 to 8
S$="":Call UP(S$)
IF SW2=&HAA OR SW2=&H5A
Then C=C+64
Next F
For F=1 to 8
S$="":Call UP(S$)
IF SW2=&HAA OR SW2=&H5A
Then C=C+8
Next F
For F=1 to 8
S$="":Call UP(S$)
IF SW2=&HAA OR SW2=&H5A
Then C=C+1
Next F
Print:Print»Il reste :
«;C; « UNITE(S)»
Print:Call
WaitForNoCard
```

Obtenu par compilation au moyen du kit BasicCard (sur basic¬card.com), le fichier exécutable CREDEURO.EXE peut être lancé avant ou après introduction de l'adaptateur dans le lecteur PC/SC, la « carte lavage » ayant été préalablement insérée dans son connecteur. Et la bonne

surprise, c'est qu'une proportion non négligeable (autour de 3 %) des cartes jetées par les clients des stations-service, contiennent encore des unités!
Pour inspecter au bit près le contenu de la mémoire (EEPROM) des cartes Eurochip, on utilisera cette fois (nous y voilà!) le logiciel EURO.BAS:

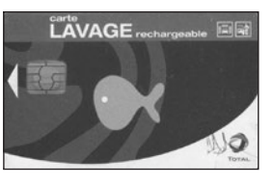
```
#include CARDUTIL.DEF
#include COMMERR.DEF
ComPort=101
Declare Command &H22
&H44 UP(S$,Disable Le)
Call WaitForCard:CLS
ResetCard:Call
CheckSW1SW2
Print»Lecture EUROCHIP
(c)2010 Patrick
GUEULLE»:Print
FOR F=1 TO 16
FOR G=1 TO 8
FOR H=1 TO 4
S$="":Call UP(S$)
IF SW2=&HAA OR SW2=&H5A
Then L$="1"
IF SW2=&H55 OR SW2=&HA5
Then L$="0"
IF F+G+H>3 Then Goto
bit
IF SW2=&HA5 OR SW2=&HAA
Then Print"1";:H=H+1
IF SW2=&H5A OR SW2=&H55
Then Print"0";:H=H+1
bit:Print L$;
Next H
Print" “;
NEXT G
Print
NEXT F
Print:Call
WaitForNoCard
```

Là encore, la version exécutable, compilée par nos soins, est directement téléchargeable sous la forme du fichier EURO.EXE. Elle pourra notamment servir à débusquer les cartes dont le compteur d'adresses « fait le tour » avant le 512e bit, et plus précisément au 480e. Tel semble être le cas lorsque la dernière ligne de 32 bits qui s'affiche est identique à la première au lieu d'être remplie de « 1 », phénomène qu'il est particulièrement instructif de corréler avec le modèle de puce électronique que contient la carte…
Tout comme avec la version T2G de l'adaptateur, il est possible non seulement de lire, mais aussi d'écrire des bits, autrement dit de transformer des « 1 » en « 0 », avec ou sans mise en œuvre du mécanisme de « retenue » (effacement d'un compteur lors de l'écriture d'un bit dans celui de poids supérieur). Est-il besoin de préciser que ces manœuvres sont uniquement destinées à débiter des unités, et en aucun cas à « recharger » les cartes?
On se servira pour ce faire du logiciel MANIP.EXE (version compilée de MANIP.BAS), en se référant aux explications détaillées que fournit notre ouvrage précité, et que nous n'avons pas la place de reprendre dans ce dossier déjà copieux.

```
#include CARDUTIL.DEF
#include COMMERR.DEF
ComPort=101
Declare Command &H22
&H44 UP(S$,Disable Le)
Declare Command &H22
&H22 WR(S$,Disable le)
Call WaitForCard
ResetCard:Call
CheckSW1SW2
CLS
Print» barre d'espace :
avance lecture»
Print» touche + : mise
a 0 de bit»
Print» touche - : mise
a 0 de bit avec
retenue»
Print" touche ESCape :
quitter":Print
FOR F=1 TO 16
FOR G=1 TO 8
FOR H=1 TO 4
S$="":Call UP(S$)
IF SW2=&HAA OR SW2=&H5A
Then L$="1"
IF SW2=&H55 OR SW2=&HA5
Then L$="0"
IF F+G+H>3 Then Goto
bit
IF SW2=&HA5 OR SW2=&HAA
Then Print"1";:H=H+1
IF SW2=&H5A OR SW2=&H55
Then Print"0";:H=H+1
bit:Print L$;
touche:Z$=Inkey$:If
Z$="" Then Goto touche
If Z$=Chr$(32) Then
Goto suite
If Z$=Chr$(43) Then
Goto pgm
If Z$=Chr$(45) Then
Goto carry
If Z$=Chr$(27) Then
Exit
Goto touche
suite:Next H
Print" “;
NEXT G
Print
NEXT F
ResetCard:Call
CheckSW1SW2:Exit
carry:S$="":Call WR(S$)
pgm:S$="":Call WR(S$)
fin:IF Inkey$<>"" Then
Goto fin
Goto touche
REM (c)2001 Patrick
GUEULLE
```

Les cartes de lavage à CryptoMemory

Désormais rechargeables en station, les actuelles « cartes lavage » *alias* Total Wash de Total sont basées sur une puce électronique particulièrement intéressante et de capacité mémoire très supérieure, la CryptoMemory d'Atmel. Fidèle à sa tradition du « rideau de fumée », son fabricant n'a dévoilé que très partiellement (ou alors contre engagement de non-divulgation) les caractéristiques de ce composant, ou plus exactement de cette famille de composants. Il ne faut pas davantage lui demander dans quelles applications on retrouve ses puces « sur le terrain », ce qui donne naturellement envie de partir à leur recherche! Nous en avons notamment trouvé dans des cartes de fidélité telles que l'éphémère carte des supermarchés U (voir notre dossier http://www.acbm.com/¬inedits/carte-puce-fidelite-secrets.html) et dans une Cartaplus, tellement verrouillée que l'on ne pouvait même pas y consulter son solde de points par ses propres moyens: il fallait se rendre chez un commerçant équipé du terminal *ad-hoc*, ou interroger le serveur central par Internet!
La grande originalité des cartes équipées de ces puces est que, bien qu'il s'agisse de cartes « à mémoire » (et non pas « à microprocesseur »), elles fonctionnent en protocole asynchrone (T=0). Elles sont par conséquent compatibles avec les terminaux de point de vente acceptant les cartes bancaires, mais aussi avec n'importe quel lecteur PC/SC, ce qui va singulièrement nous faciliter les choses…
À force de recouper des informations de nature publique avec des investigations personnelles, nous avons fini par reconstituer une bonne partie de ce que le fabricant des puces s'évertuait à garder confidentiel, et donc à comprendre l'essentiel du fonctionnement des cartes de lavage basées sur cette technologie prometteuse.



Les cartes de lavage Total sont rechargeables!

Toute une partie de leur mémoire est librement accessible en lecture, au moyen de commandes faciles à programmer en langage « script » ou en *ZCBasic*.
00 B6 01 00 08 retourne ainsi, outre un compte-rendu de bonne exécution « 90 00 », les huit octets dont se compose la « réponse au reset » (ATR) de la carte: 3B B2 11 00 10 80 00 02 dans le cas du composant AT88SC0204C (à mémoire de 2 Kbits).
00 B6 00 08 08 va chercher huit octets identifiant notamment le fabricant de la puce et son encarteur. À noter que dans ces parages, deux octets sont à écriture libre: on peut donc les modifier à volonté, notamment à des fins de test.
00 B6 00 10 08 donne accès à huit octets contenant des informations sur l'historique du lot de composants à partir duquel la carte a été fabriquée.
Avec 00 B6 00 18 08, nous entrons vraiment dans le vif du sujet, puisque c'est là que réside le numéro d'identification de la carte, celui-là même qui est bien souvent imprimé au verso. Dans la carte n° 0001361083, nous avons ainsi lu FF 00 00 00 01 36 10 83. Le premier octet (ici FFh) est baptisé « DCR », et cette valeur « par défaut » indique qu'aucune des options particulières que peut supporter le composant n'est activée. Cela commence bien!
00 B6 00 20 08 permet de prendre connaissance des conditions de sécurité auxquelles est soumis l'accès aux quatre zones utilisateur de la mémoire. Ici, la réponse EF 3F EF 3F EF 3F EF 3F indique que les règles sont les mêmes pour ces quatre partitions, à savoir pas de chiffrement, pas de mots de passe, mais une authentification mutuelle de la carte et du terminal avant toute opération d'écriture. En d'autres termes, nous pourrons consulter librement le solde de la carte, mais ni débiter celui-ci, ni encore moins le créditer (rechargement). Un bon compromis, finalement!
Par comparaison, nous avions lu 9F 38 9F 38 9F 39 9F 39 dans une Cartaplus, ce qui signifie qu'une authentification mutuelle était exigée avant l'écriture ou même la lecture (sans chiffrement), et qu'un mot de passe devait être présenté, en plus, avant de pouvoir écrire. À l'inverse, la regrettée carte U à puce se contentait d'un simple mot de passe en écriture, sans chiffrement ni authentification mutuelle, autrement dit d'un mécanisme de sécurité pour le moins

basique et donc plutôt facile à déjouer : BF F8 BF F9 BF F8 BF F9.
Une commande 00 B6 00 40 10 permet enfin de lire une zone de 16 octets dite « code émetteur », qui est ici remplie de 00h, à l'exception d'un 02h en troisième position.
Quelques octets de plus pourraient encore être lus en accès libre, mais ils n'apporteraient rien d'utile à notre exploration dans le cas spécifique des cartes de lavage.
Intéressons-nous plutôt aux zones utilisateur dont le contenu, variant au fil de la vie des cartes, est infiniment plus amusant à analyser ! Pour y accéder, il faut commencer par sélectionner une région de 64 (ou 40h) octets parmi les quatre que contient la carte. Dans le cas qui nous occupe, seule la première (n°0) est utilisée, et nous enverrons donc la commande 00 B4 0B 00 (00). Pour atteindre la seconde (n°1), nous enverrions 00 B4 0B 01 (00), et ainsi de suite. Une fois la zone « ouverte », nous pouvons la lire en totalité au moyen d'une commande 00 B2 00 00 40.
Voici ce que nous avons trouvé dans une carte initialement chargée de 10 €, et qui avait servi à payer, le 7 novembre 2010, un lavage coûtant (à l'époque !) 3,90 € :

```
00 00 02 62 00 00 00 60
FF FF FF FF FF FF FF FF
97 80 00 00 01 00 00 11
17 04 08 00 00 03 E8 FF
00 00 00 00 00 00 00 00
00 00 FF FF FF FF FF FF
05 95 22 07 11 10 90 01
00 00 03 E8 00 00 00 CE
```

À condition de convertir le solde restant (610 centimes) en hexadécimal (02 62), on repère immédiatement où il est enregistré. À noter que la valeur du chargement initial (03 E8 h pour 10 €) est indiquée vers la fin de la seconde ligne. En huitième position, un octet initialement fixé à EBh (03 XOR E8, dirait-on) est par ailleurs passé à 60h (02 XOR 62, n'est-ce pas ?), mais c'est dans la dernière ligne (initialement remplie de 00h) qu'il s'est passé le plus de choses ! On y trouve, notamment, la date du lavage qui vient d'être effectué (07 11 10), et le solde de la carte avant celui-ci. Aucune trace évidente, par contre, du montant qui a été débité (01 86 h), mais il suffit de faire une soustraction ! Les quelques autres octets qui ont changé (05 95 22) dépendent quant à eux de la station ayant assuré la prestation de lavage.
Autre exemple, qui nous permet de confirmer nos supputations avec… presque sept ans de recul : un lavage effectué le 16 mars 2017 dans la même station, mais payé cette fois en complétant avec une seconde carte les 1,40 € (00 8C h) que contenait celle-ci, qui se trouve par conséquent complètement vidée (solde de 00 00 h) :

```
00 00 00 00 00 00 00 00
FF FF FF FF FF FF FF FF
97 80 00 00 01 00 00 11
17 04 08 00 00 03 E8 FF
00 00 00 00 00 00 00 00
00 00 FF FF FF FF FF FF
05 95 22 17 03 16 90 01
00 00 00 8C 00 00 00 AD
```

Et que penser de cette carte dans laquelle il reste 2 € (C8h) après un lavage payé 16,40 € le 16 février 2020 ? Les deux montants 0B54h et 1068h évoquent respectivement un rechargement de 29 € (25 + 4 de bonus) crédité le 6 décembre 2019, et un chargement initial de 42 € (35 + 7 de bonus) en date du 13 octobre 2017.

```
00 00 00 C8 00 00 00 C8
FF FF FF FF FF FF FF FF
97 80 10 22 01 05 95 22
13 10 17 00 00 10 68 FF
05 95 22 06 12 19 00 00
0B 54 FF FF FF FF FF FF
07 81 10 16 02 20 90 05
00 00 07 30 00 00 00 00
```

La réponse est évidente : elle est vraiment suivie à la trace !
Reste maintenant à déterminer dans quelles stations ces évènements se sont produits…

Piratages de pompes à essence

Des médias ont informé en 2017 et 2018 que des pompes à essence ont été vidées de leur carburant par piratage chez Total en France, avec un préjudice de 120 000 litres à la clé. Les voleurs ont utilisé des télécommandes infrarouges en vente libre (notamment sur Internet) permettant de passer en mode de maintenance (un tel accessoire parfois compatible avec plusieurs types de pompes coûte dans les 100 €) pour changer le prix du carburant et fixer les limites de remplissage. Le contenu des cuves pouvait alors être récupéré gratuitement. Le piratage était possible, car le code PIN de sécurité avait été laissé dans certaines stations à la valeur par défaut : 0000. En connaissant les spécifications du signal ou en dupliquant celui d'une télécommande légitime, il aurait été même possible d'utiliser une télécommande universelle programmable plus économique.
En parallèle, les pompes à essence connectées à Internet se multiplient. En 2015, Trend Micro avait publié une étude sur les attaques contre le système de pompes à essence de Guardian AST. Si une attaque « par saturation » a été constatée sur le terrain, d'autres scénarios plus élaborés avaient été envisagés. Il n'aura pas fallu très longtemps pour passer de la théorie à la pratique. Fin 2017, des chercheurs notamment de chez Kaspersky Labs alertaient Orpak Systems de failles dans son système utilisé dans des dizaines de pays, un boîtier de contrôle, véritable petit ordinateur sous *Linux* configuré en différents serveurs. Les experts ont repéré un mot de passe par défaut dans une documentation mise en ligne… sur le site officiel. Ce mot de passe a permis de se connecter à une pompe en Espagne dont ce mot de passe n'avait pas été changé et d'analyser tous ses fichiers. Une porte dérobée a été trouvée dans le code source avec un autre mot de passe stocké « en dur ». À partir de là, il était possible de passer en mode administrateur avec une interface Web sur n'importe lequel des exemplaires du boîtier pour mettre à l'arrêt les pompes ou de changer les prix. Il était également possible de contrôler la température et la pression dans le réservoir, de le vider, soit de quoi déclencher des explosions à distance selon certaines spéculations.
Autres possibilités pour les pirates : intercepter les numéros des cartes utilisées pour payer, contrôler les caméras de sécurité, effacer les *logs* (et donc les traces du piratage), modifier le logiciel embarqué… Il se trouve que début 2018 la police russe avait annoncé avoir démantelé une arnaque : un *malware* placé avec l'aide de complices dans les logiciels de pompes à essence (un autre modèle *a priori*) permettait de détourner une partie des achats que les voleurs pouvaient récupérer plus tard.

Nous en savons de toute façon bien assez pour développer un très pratique petit logiciel *ZCBasic* (TOTAL.BAS), capable d'afficher le numéro de la carte et son solde exprimé en centimes d'euro !

```
#Include CARDUTIL.DEF
#Include COMMERR.DEF
ComPort=101
Declare Command &H00
&HB6 RDC(Lc=0,S$)
Declare Command &H00
&HB2 RDU(Lc=0,S$)
Declare Command &H00
&HB4 WRC(S$,Disable Le)
Call WaitForCard
ResetCard:Call
CheckSW1SW2:Print
CLS:Print"Carte No ";
Call
RDC(P1=0,P2=&H18,S$,Le=8)
For F=4 To Len(S$)
C$=MID$(S$,F,1):C=ASC(C
$):C$=HEX$(C)
IF LEN(C$)=1 then
C$="0"+C$
Print C$;
Next F:Print:Print
Call
WRC(P1P2=&H0B00,Lc=0,S$)
Call
RDU(P1P2=&H0000,S$,Le=4)
E$=""
For F=1 To Len(S$)
C$=MID$(S$,F,1):C=ASC(C
$):C$=HEX$(C)
IF LEN(C$)=1 then
C$="0"+C$
E$=E$+C$
Next F
E=ValH(E$)
Print»Il reste «;E;»
centimes d'euro»
Print:Print
Call WaitForNoCard
```

Là encore, c'est sa version compilée (TOTAL.EXE) que l'on exécutera sous *Windows*, en insérant simplement la carte dans un quelconque lecteur PC/SC installé sur le PC. Bien que nous nous trouvions en présence d'une carte réalisée en « logique câblée » (c'est-à-dire n'exécutant aucun micro-code en interne), nous communiquons avec elle comme s'il s'agissait d'une carte à microprocesseur, très sensiblement plus coûteuse. Et de la façon dont elle est mise en œuvre, rien ne nous permet de penser pour le moment que sa sécurité pourrait laisser à désirer… ■

De la came au scam : le stupéfiant nouveau business d'Escobar

Le nom Escobar inc. vous fait, sans doute, penser au célèbre « baron de la drogue » colombien, Pablo Escobar (Gaviria). En fait, ce nom n'est pas une coïncidence : il s'agit d'une réincarnation depuis 2014-2015 de sa *holding* fondée en 1984 et aujourd'hui dirigée par son frère cadet, Roberto de Jesús (73 ans). Elle s'est lancée un domaine où on ne l'attendait pas : la téléphonie mobile. Et ce n'est pas la dernière des surprises qui vous attendent ! Promis, ce qui suit est véridique et n'a pas été rédigé sous l'effet de substances illicites.

Fin 2019, Escobar avait annoncé le Fold, un *smartphone* pliable (lire acbm¬.com/virus/1176_Nou¬velle_production_Esco¬bar_decrochez_.html). Son prix nous semblait trop beau pour être vrai, d'autant plus qu'il s'agissait d'un FlexPai de Royole visiblement recarrossé, un modèle vendu bien plus cher. Et, en fait, malgré des messages annonçant un report des livraisons en février 2020 en raison d'« *incroyables améliorations matérielles et logicielles* », la plupart des personnes qui l'ont commandé ne l'ont jamais reçu. Sauf, apparemment, celles jouissant d'une certaine exposition médiatique. Le « YouTubeur » Marques Brownlee dit MKBHD fait partie des veinards (quoiqu'un second exemplaire commandé sous un autre nom ne lui a jamais été livré). Il a même reçu à la place un modèle Fold 2 (400 dollars) annoncé en février justement. Eh bien, non seulement l'interface *Android* de l'appareil est, cette fois, celle d'un Galaxy Fold de Samsung, de même que le *look*, mais il a lui simplement fallu retirer un *sticker* pour faire apparaître la marque sud-coréenne dissimulée en dessous ! En grattant un peu le dos, le revêtement doré (de mauvais goût) d'Escobar a laissé place à l'« Argent Stellaire » du Galaxy Fold, un modèle vendu 2 000 dollars (la « blague » avec Samsung ne s'arrête pas là, lire encadré). Bref, il n'est économiquement pas possible qu'Escobar vende son Fold 2 cinq fois moins cher et on comprend mieux que les clients risquent d'attendre (très) très longtemps leur colis qui est indiqué comme étant en préparation, même si la société prétend avoir trouvé un gros stock d'invendus à bas prix en Chine. MKBHD laisse entendre que d'autres « influenceurs » ont été payés par le biais du service Cameo pour faire la promotion du *smartphone* et piéger les gogos à leur insu. Des clients d'Escobar ont-ils « sniffé » non pas de la cocaïne, mais de la farine pendant des années sans s'en apercevoir ?

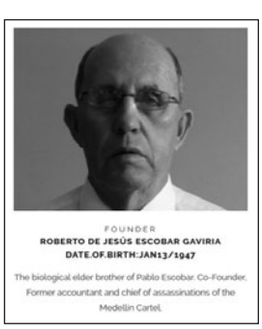
Le lancement sexiste de l'Escobar Fold premier du nom. Femmes en petite tenue non livrées avec, pour paraphraser la publicité.

MKBHD a découvert qu'un Galaxy Fold de Samsung se cache derrière le Fold 2 d'Escobar.

La faute à un ex-dirigeant en fuite ?

Rebondissement ! Fin avril 2020, Escobar initie une procédure devant une cour fédérale des États-Unis contre Daniel (David) Reitberg, son ancien chef des opérations. Il aurait été engagé en 2014, limogé fin 2019, puis réembauché en mars 2020, avant de s'évaporer sans explication au bout de quelques jours. La société lui reproche d'avoir siphonné les caisses au passage et de demander une importante somme d'argent en échange du contrôle de la chaîne YouTube d'Escobar dont il aurait changé le mot de passe. Cette chaîne serait capitale car, selon sa plainte, elle aurait permis de générer un million de dollars de chiffre d'affaires grâce à ses vidéos publicitaires à succès (elles mettent en scène des femmes en petites tenues - des anciennes mannequins de *Playboy* - dans des positions parfois suggestives). On y apprend aussi que Daniel Reitberg aurait fermé des comptes bancaires (où l'argent des clients arrivait par virements, depuis que les interfaces de paiement à la PayPal et compagnie avaient rompu leurs contrats avec Escobar) et qu'il aurait détruit les documents qui faisaient le lien entre paiements et commandes. La société se sert de cette excuse, en sus du coronavirus bien sûr, pour expliquer qu'elle n'a pas envoyé tous les *smartphones* commandés. Les autres médias s'étant généralement arrêtés ici, à la suspicion d'arnaque de la part d'Escobar, voire rarement au rôle supposé de l'ancien dirigeant, nous avons décidé de creuser plus loin.

Précisons que nous n'avons pas réussi à joindre Daniel Reitberg pour avoir son point de vue. On pourrait imaginer qu'il ne soit qu'un



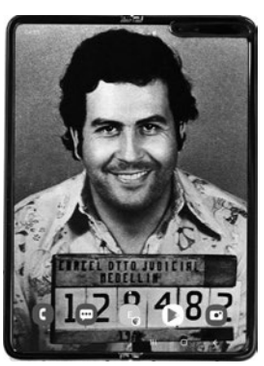
Le site officiel de la société Escobar nous explique, le plus sérieusement du monde, que son cofondateur Roberto Escobar était le comptable et chef des assassinats du cartel de Medellín (il a passé 12 ans en prison). Selon des estimations, on doit 5 000 meurtres à ce cartel entre 1989 et 1993. En cas de commande non livrée, à votre place, on ferait très (très) attention avant de se plaindre au service après vente !

Plus fort que Zlatan !

Tombé dans l'informatique avec son premier ordinateur à 7 ans, Olof K. Gustafsson (26 ans) est présenté comme un homme d'affaires suédois précoce avec une première société à 13 ans, spécialisée dans la vente en ligne de bandes dessinées. À 17 ans, il était déjà à la tête de quatre sociétés (une agence Web, l'éditeur en Suède des *Simpson* notamment et une société de presse en sus de sa boutique en ligne d'origine). Son rêve affiché alors : devenir milliardaire en dollars. Ses entretiens avec la presse locale laissent deviner une personne arrogante ; il se présente comme « *meilleur que tout le monde* ». Le magazine *Entreprenör* invite à « *oublier Zlatan* [Ibrahimović] *et Kamprad* [le fondateur d'Ikea]*, voici les nouveaux héros !* » Olof construit sa légende : refusé par une école de *business*, il décide d'émigrer aux États-Unis où il devient un temps SDF (toujours selon ses dires), vivant de petits boulots payés un dollar par heure. En 2014, sa route croise celle de Roberto Escobar, à qui il veut consacrer un jeu vidéo. Trois mois plus tard, à 20 ans, Olof devient le p.-d.g. d'Escobar inc. Avec son collègue d'alors Daniel Reitberg, il a aussi monté la société Adenheim en 2015.

On a pu lire dans *The Washington Post* comment Olof K. Gustafsson est suspecté d'avoir aidé Donald Trump, alors candidat à la présidentielle des États-Unis, à gagner de nombreux abonnés sur les réseaux sociaux (Olof a confirmé à *Expressen*). Mais, en janvier 2019, il a lancé pour le compte d'Escobar inc. le financement communautaire d'une campagne visant à destituer le président Donald Trump, campagne qui a récolté 10 millions de dollars en quelques heures avant d'être désactivée par la plate-forme GoFundMe. Aujourd'hui, Olof K. Gustafsson prétend résider à Dubaï, aux Émirats arabes unis, un autre paradis fiscal.

lampiste et que sa disparition de la circulation soit la volonté d'un ou plusieurs de ses anciens collègues, mais ce n'est qu'une hypothèse parmi d'autres. Nous aurions aimé aussi la preuve qu'il a vraiment été de retour dans la société pour quelques jours seulement. La direction d'Escobar inc. n'a donné suite à aucune de nos demandes.



Il vous plaît le fond d'écran ?

Un business depuis la Suède

Escobar inc. est enregistrée à Puerto Rico, un paradis fiscal rattaché aux États-Unis, chez la société de domiciliation Regus. Elle a aussi des opérations déclarées dans l'hôtel NH Colection à Medellín en Colombie. Cette société ne fait que récolter des *royalties* sur les marques relatives à Pablo Escobar ; Roberto Escobar est, d'ailleurs, son « chef des marques ». Derrière elle, le montage est plus complexe. Selon les conditions de vente, la boutique du site officiel EscobarInc.com est dans les mains de Pablo Phone, une société anglaise au capital d'une livre sterling hébergée à Londres, elle aussi chez Regus. Son directeur et seul propriétaire est Roberto Escobar. Les envois sont indiqués comme effectués depuis Hongkong (c'est courant pour des produits du Sud-est asiatique) ou la Suède (c'est plus surprenant). Klarna Bank, premier service utilisé pour prélever l'argent sur les cartes bancaires lors des ventes de *smartphones*, est suédoise. En décembre 2019, elle a mis fin à un contrat avec Affideer après seulement quelques jours de collaboration. Revenons aux conditions de vente sur EscobarInc.com : elles stipulent que les informations de la commande sont stockées par Affideer AB, une société suédoise dirigée par Gustav Ingvar Gustafsson, qui a été élu social-démocrate au conseil municipal de sa ville à une époque. Il se trouve que le p.-d.g. d'Escobar inc. est Olof K. Gustafsson, son fils.

L'argent a été gelé par Klarna Bank. Selon *Digital Di*, Olof K. Gustafsson lui réclame 4 millions de couronnes suédoises, l'équivalent d'un millier de commandes environ. Dans un courriel envoyé fin janvier 2020, la banque justifie sa décision par des « *raisons éthiques* ». Elle explique avoir sélectionné aléatoirement 20 plaintes de consommateurs pour non-livraison et a demandé, le 13 janvier, la preuve des envois de la marchandise. Le 24 janvier, elle n'a reçu en réponse qu'une liste des pays de destination pour des envois effectués les… 16 et 17 janvier. La mauvaise foi d'Affideer semble établie.

Olof K. Gustafsson, Roberto Escobar et Daniel D. Reitberg

Mais il n'est pas impossible, même si la probabilité est faible, que cette décision de la banque de bloquer les fonds dès décembre ait mis les partenaires d'Escobar dans l'impossibilité de payer le fournisseur chinois et donc de livrer les clients. D'ailleurs, comment après seulement trois jours d'activité, la banque a-t-elle pu deviner que la marchandise ne serait pas envoyée ? Ou le problème n'était au départ que le nom d'Escobar ? Et l'argent a-t-il finalement été renvoyé à tous les acheteurs de *smartphones* depuis ? Elle refuse de commenter le cas.

Défections en série des services de paiement

Après Klarna Bank, c'est Stripe qui a pris le relais en tant que processeur de paiement pendant une dizaine de jours, avant de mettre fin au contrat. Puis au tour de son concurrent CCBILL en janvier 2020, et pendant un mois, avant de stopper la fourniture de son service. Jusqu'à la mi-février, des clients se sont vus demander de virer directement à l'argent à la Wells Fargo Bank sur le compte de la société Reichste, enregistrée dans le Wyoming (États-Unis) avec Olof K. Gustafsson pour dirigeant, puis dissoute en 2017 avec effet en avril 2019. Puis jusqu'à début mars 2020, il fallait utiliser un compte chez Nordea en Suède appartenant à nouveau à Affideer. Puis, pendant quelques jours en mars, d'autres clients ont été invités à transférer l'argent à la USA Community Federal Savings Bank sur un compte de BH Cash, une autre société (en

Les noms de domaine, c'est aussi leur domaine !

En 2019, Escobar a initié une procédure contre le courageux (inconscient ?) détenteur du nom de domaine pabloescobar.com qui exigeait trois millions de dollars pour la rétrocession. Escobar a gagné l'arbitrage international. On aurait donc pu imaginer que la société connaissait les risques en matière de *cybersquatting*. Mais, en mars 2020, c'est Samsung qui a initié une procédure contre elle au sujet du nom de domaine ripsamsung.com (pour « *repose en paix Samsung* ») qu'elle avait redirigé vers une page Web vendant le Fold 2, le fameux Galaxy Fold maquillé. Eh oui, Escobar est capable de porter des coups bas à son propre « fournisseur » ! Cette fois, c'est logiquement la société sud-coréenne qui a gagné.

Un lance-femme, pardon, un lance-flammes à 250 dollars

Californie, cette fois) dirigée par le p.-d.g. d'Escobar. C'est alors l'USA Chase Bank qui a servi avec un compte appartenant à une mystérieuse entité Maximum Intention (enregistrée dans le Wyoming par un agent « proxy ») dont on ne connaît pas les personnes derrière. Escobar affirme que ces dernières coordonnées bancaires ont été envoyées à son insu par Daniel Reitberg, qui serait le propriétaire de Maximum Intention. Même si on croit Escobar sur ce point (et on n'y est pas obligé), cela ne dissipe pas les doutes concernant la succession de comptes bancaires précédents et la société mériterait, peut-être, de figurer dans *Le Livre des Records* au titre du client refoulé d'un maximum de banques en un minimum de temps ! La solution qui semble s'imposer pour le client qui aurait encore confiance est, du coup, un paiement en cryptomonnaies (nous allons y revenir un peu plus loin…).

Escobar a finalement livré… un livre

Avant cette incursion dans le monde des *smartphones*, pour un commerce de lance-flammes (lire encadré), c'est PayPal qui avait été utilisée, plate-forme qui a coupé, elle aussi, les ponts avec Escobar, tandis que des clients se plaignaient de ne pas avoir été livrés.

Des clients lésés font état de difficultés pour obtenir remboursement de la part des intermédiaires techniques. Il se pourrait qu'Escobar ait rusé pour les tromper. Des acheteurs du Fold 1 ont, en effet, reçu par surprise un livre avec une lettre d'accompagnement informant que l'appareil promis serait remplacé sans surcoût par un Fold 2, normalement plus cher. Officiellement, la société prétend que c'était pour vérifier si les adresses de livraison étaient conformes. Mais, de fait, Escobar aurait été en mesure de prouver aux plates-formes de paiement qu'elle a envoyé des colis grâce aux numéros de suivi, même si elle ne précisait pas que les colis contenaient des livres au lieu des *smartphones* attendus.

Le Bitcoin d'Escobar

Escobar a lancé sa cryptomonnaie le dietbitcoin, abrégé en DDX. Dans un livre intitulé *Pablo Escobar's dietbitcoin*, Roberto Escobar affirme, sans apporter de preuves, que le Bitcoin est une création du gouvernement états-unien et non du mystérieux Satoshi Nakamoto. Ce qui ne le dérange visiblement pas pour en envisager un dérivé (*fork*).

Pour motiver les investisseurs, le communiqué de presse présentait Roberto Escobar comme l'un des hommes d'affaires ayant eu le plus de succès dans l'histoire de l'Humanité, avec plus de 100 milliards de dollars de profits dans sa carrière. Le chef des opérations Daniel Reitberg y déclarait : « *Tout le monde devrait écouter ces nouvelles, aller sur dietbitcoinICO.org et acheter autant de dietbitcoins qu'il en a les moyens, sa valeur sera très importante comme nous aurons un nombre identique à celui du Bitcoin, sauf que nous sommes 4000 fois moins chers pour le moment.* » C'était début 2018, bien avant de se lancer dans le commerce de *smartphones*. La valeur promotionnelle du jeton était de 2 dollars au lancement contre 50 dollars annoncés plus tard. Fin 2019 (il ne semble plus y avoir de transactions depuis), un dietbitcoin ne valait plus que 0,000009 dollar. Curieusement, il n'est pas utilisable pour payer les *smartphones* d'Escobar, contrairement à d'autres cryptomonnaies. Pas assez crédible, peut-être ? Les investisseurs ont perdu quasiment 100 %, mais la société s'est bien remplie les poches en vendant du vent.

Si des médias ont annoncé l'arrivée d'Escobar dans le monde de la cryptomonnaie, ils n'ont pas raconté la triste fin de cet épisode. Et c'est ainsi que, ce premier scam n'ayant pas été assez rendu public, Escobar a pu en lancer un second avec ses *smartphones*. ■

Roberto : tout feu, tout lance-flammes !

Lors du lancement du Fold premier du nom, Roberto Escobar a annoncé à *Digital Trends* qu'il a financé, pour un million de dollars de frais d'avocats, une action collective contre Apple visant à récupérer 30 milliards de dollars. Il reproche à la pomme que « *ce sont des escrocs* » (*sic* !), « *ils trompent les gens et vendent des téléphones sans valeur aux consommateurs, trop chers* » et il veut qu'« *Apple redistribue une partie de ses profits illégaux à la population.* » Le libre marché, l'offre et la demande, les « profits illégaux » semblaient moins le gêner quand il était dans le commerce de la drogue (et désormais des arnaques en ligne). Procédurier, l'homme poursuit aussi Elon Musk (Tesla, SpaceX…) et The Boring Company qu'il accuse de lui avoir volé son idée de lance-flammes économique ; il réclame 100 millions de dollars de dédommagement. Enfin, il y avait une procédure contre Netflix pour usage d'images non autorisé de Pablo dans la série *Narcos*, l'affaire semble s'être réglée à l'amiable à des conditions non dévoilées. Le tournage avait été endeuillé par l'assassinat d'un assistant de production ; Escobar avait dû démentir toute implication.

Une collection de sociétés

Comme nous l'avons expliqué, une myriade de sociétés satellites ont été impliquées dans le commerce de *smartphones* d'Escobar. Elle nous en cache probablement d'autres encore. Par contre, la société « balance » celles supposées de son ex-chef des opérations, Daniel Reitberg. Elle pointe du doigt notamment Quantum Blue LLC (Wyoming), ainsi que Globamente Inc, Violet Group LLC (Wyoming), Fluid Capital Markets LLC (Nevada), Vindonnus Corporate administrative & finance LLC (New York), Violet Investm Funds LP (Îles Cayman), VCAF LLP (Sainte-Croix, îles vierges des États-Unis), Innerlight Management LLC (New York), Unicitizens Inc (Californie), Unicitizens Financial Inc (Californie), Global Heavy Ltd (Grande-Bretagne), Lalaloo LLC (Floride), Adenheim Home Loans Inc (Californie), MDTB LLC (Nevada), Telford Laboratories LLC (Nevada), Reitberg Space Industries RSI. Liste, peut-être, non exhaustive. Toutes sont-elles vraiment ses sociétés ou a-t-il agi aussi en tant que prête-nom ?


SALUT!
SALUT!
BONNE ROUTE?
OUI, VRAIMENT AGRÉABLE!
ALORS, C'EST TA NOUVELLE TESLA?
OUI, UNE PURE MERVEILLE DE TECHNOLOGIE.
REGARDE-MOI CET ORDINATEUR DE BORD!
J'AI UTILISÉ LE PILOTE AUTOMATIQUE.
JE N'AI PAS VU LE TEMPS PASSER, J'AI JOUÉ SUR MON TÉLÉPHONE TOUT LE TRAJET!
MAIS C'EST SUPER DANGEREUX!
TU DEVRAIS SURVEILLER LA ROUTE AU MOINS...
ET T'AS JOUÉ À QUOI DU COUP?
REAL DRIVE 3D, J'ADORE!
TU CONNAIS?
C'EST UN SIMULATEUR DE CONDUITE AUTO SUPER RÉALISTE!
SCENARIO : ACBM

Vous avez raté les précédents numéros de Virus Info ?

Ils sont disponibles en téléchargement pour PC, Mac, iPhone/iPad, Android, etc.

Format epub, sans DRM ! (également disponibles aux formats PDF et Kindle)

http://acbm.com/ebooks.html

Le prix est variable selon les plates-formes en fonction de la commission de chacune. Mais vous pouvez acheter le fichier sur la plate-forme la moins chère, le télécharger depuis son interface Web, puis l'ouvrir ensuite sur l'appareil de votre choix, par exemple Calibre ou Vivlio (fichier de test gratuit sur notre site).