L'histoire d'un blog : KRACH.IN

Consterné par le manque de sécurité informatique que j'ai pu croiser j'ai eu envie de faire partager quelques connaissance dans le domaine du hacking.

Je me suis mis à la place d'un chef d'entreprise, d'un salarié, d'un particulier, d'un utilisateur lambda ayant pour seules connaissances informatique l'utilisation quotidienne au travail ou à la maison (souvent cantonné à bureautique + internet).
Et là je me suis rendu compte que souvent dans les médias on pouvait lire / entendre des actualités concernant tel ou tel faille permettant de portée atteinte à un système informatique, mais que ce genre d'information ne faisait que de rentrer par une oreille pour en sortir par l'autre.

J'ai donc décidé de montrer par la pratique que ce genre de dangers étaient bien réels par des démonstrations (réalisées dans le cadre d'un laboratoire montée de toutes pièces évidemment).
Il est bien plus pertinent de prendre conscience de ces dangers si on peut les matérialiser et se convaincre de leur existence dans le but de mieux se prémunir face à ces attaques.

Parmi mes articles il y avait un peu de tous, des démonstrations techniques, des actus de mise en garde, des coups de gueule, des bouts de code de programmation.
J'ai toujours fais mes articles dans un sens de mise en garde, pour porter la réflexion aux concernés, jamais je n'ai fait de tutoriel ayant pour but de porter atteinte aux systèmes automatisés de données comme on me l'a reproché.
Si un pirate malveillant avait voulu trouver des infos pour pénétrer un système, il est sûre que ce n'est pas mon blog qu'il aurait visité. Par exemple pour casser du wifi, si je tape 'crack wifi' dans Google, j'ai 'Environ 15 500 000 résultats', bref… Sachant qu'en plus dans mon article en question il manque des étapes menant à bien l'attaque.
Toujours au sujet du Wifi, le WEP est mort depuis plus de 10 ans, il y a pas si longtemps de ça des FAI livraient des box avec du WEP par défaut, pourquoi ne pas les avoir blâmé ? A cause de leur gros sous ?

La perquisition.

En septembre 2014, c'était le matin, j'étais en congés ce jour là (heureusement, ça m'aurait fais mal que ma femme et notre bébé se retrouvent face à ça), vers 9h ça toque à la porte.
Je vais ouvrir et là quatre gendarmes en civil me montrent leur carte et m'annonce qu'ils viennent perquisitionner mon domicile. Je leur demande pourquoi, et ils me répondent que c'est au sujet de mon blog qui parle de cracking.
Il sont en 'flagrant délit' étant donné que mon blog est toujours en ligne à ce moment là.
Pas le choix je les laisse entrer, ils embarquent alors mes unités centrales, PC portable, disques durs externes et clés USB.
Je précise quand même qu'ils ont été courtois et n'ont pas tout retourné comme des sauvages. Par contre aucun scellé n'a été fais sur place, ils sont parti avec le matos sous le bras et dans les poches… je ne sais pas si c'est réglo mais j'ai trouvé ça très limite d'un point de vu corruption des données entre temps…
Une fois la perquisition faite ils m'ont invité à les rejoindre à la gendarmerie pour m'auditionner, je m'y suis rendu dans la foulée.
Arrivé là bas le gendarme m'interrogeant m'a directement demandé (en off) pourquoi je n'avais pas mis de faux noms pour enregistrer mon domaine et mon serveur comme ça ils ne seraient pas venu me cueillir… \le moment WTF !\ J'ai tout simplement répondu que je ne m'étais rien d'illégal et que je n'avais aucune raison de vouloir me cacher. Ça commence fort.
La suite de l'interrogatoire se passe de la manière la plus simple, le gendarme n'est pas agressif, il est même plutôt impressionné par les compétences et m'explique qu'ils sont obligé de traiter cette plainte car elle vient d'une sorte de bot qui scanne le WEB FR et selon les contenus lève des

infractions… le blabla classique pour te mettre en confiance.
Ah si et c'est à ce moment là qu'il m'est demandé de couper mon blog.
Rien d'exceptionnel à dire en ce qui concerne l'audition, ça n'a pas durée trop longtemps (1h30~2h), sauf l'impression d'être un criminel lorsqu'on te prend toutes les empreintes possibles et qu'on te tire le portrait de face et de profil.

L'après perquisition.

Me voilà rentré chez moi, et là ça fait bizarre, plus de media center, plus de PC, encore heureux que j'ai pu garder le smartphone.
N'ayant plus la télévision chez moi (j'en avais marre des publicités et de la redevance audiovisuelle) je me suis demandé comment j'allais bien pouvoir suivre les actualités:)
Ça faisait vraiment vide, il ne restait que des écrans avec les câbles qui n'étaient plus branchés au milieu de ces espaces vides où se trouvaient les tours.

Étant donné que je bosses en tant que développeur logiciel, il m'est nécessaire d'avoir un PC, j'ai donc du lâcher 600 euros pour me prendre un PC portable en attendant ; première dépense que cela m'a engendré.

Les jours passent, les semaines aussi. Au bout d'un mois je rappel le gendarme et lui demande où en est l'analyse de mon matériel informatique. On me répond que d'autre affaires sont prioritaires sur l'analyse (comprenez les histoires de pédophilie principalement).

Un peu plus de deux mois sont passés et finalement je peux enfin aller récupérer mon matériel \0/

En définitive rien de mal sur mes ordinateurs alors je peux tout récupérer. Au passage le gendarme essaye de m'intimider en me disant que s'ils l'avaient voulu ils auraient pu garder mon matos pour ré-attribution (comprenaient pour qu'ils les gardent pour eux).

Matériel récupéré, la première chose que j'ai faite c'est d'analyser tous le hardware et le software au cas où une backdoor aurait pris place (parano quand tu nous tiens). Bon je vous rassure je n'ai rien trouvé.

La convocation.

Et voilà qu'en mars 2015 je reçois une convocation pour une CRPC pour avril 2015. J'ai donc un mois pour voir ça arriver. C'est court, et je ne suis pas du tout préparé à ce genre de merdier.
Je prends donc un avocat, c'est obligatoire pour une CRPC, et ça me coûte 400 euros pour qu'il se présente à mes côtés le jour de la CRPC.

Mon avocat m'a conseillé de refuser la CRPC et d'aller au pénal, il m'a bien expliqué que c'est un 'plaidé coupable' à la française et que c'est comme si je reconnaissais ce qui m'était reproché, mais quand j'ai vu le montant du devis, j'ai préféré aller à la CRPC et voir ce que j'allais prendre. Honnêtement je me voyais repartir avec une sorte de rappel à la loi.

Le jour de la CRPC j'apprends que le procureur veut me coller une amende et du sursis. Ouch…

Alors le passage devant le procureur à juste était le moment le plus frustrant, j'avais en face de moi un homme ayant le pouvoir de me plomber et qui avançait des arguments et comparaisons complètement farfelus, et je ne pouvais pas me risquer à le remettre dans le droit chemin sans risquer ma peine.
Il comparait le fait que je montre des techniques de hacking au fait de conduire une voiture à 250km/h alors que c'est interdit, juste pour montrer que cette vitesse peut être atteinte… si on compare vraiment à mon cas, si c'est faisable en allant sur un circuit comme moi j'ai fais mes démonstrations sur un laboratoire privé.
Ensuite il a comparé ça avec des histoires de pédophilie complètement déplacées… sérieusement c'est là que j'ai compris qu'il était 100 % à côté de la plaque sur mon cas.
Mais encore une fois, je n'ai pas voulu risqué de lui dire ses quatre vérités de crainte de me prendre

une condamnation bien salé.

Mon avocat a tout de même pu m'éviter le sursis ainsi que l'inscription au casier judiciaire. Mais j'ai quand même pris 750 euros d'amende !
Forcément j'ai accepté étant donné que c'était moins onéreux que de payer l'avocat pour aller au pénal, derrière j'ai ma femme et mon bébé auxquels je dois subvenir, et je n'ai pas un salaire de ministre, donc le choix était fait, quitte à endosser ces accusations mal-fondées.

Finalement.

J’espère en tout cas que cette histoire pourra servir à d'autres, si j'avais su que la communauté allait rebondi avec autant de vigueur sur cette histoire, j'aurais certainement essayé de m'y prendre autrement en sachant que j'aurais eu un soutien de poids.

Bonus :)

Encore une belle anecdote concernant l'administration française : lorsque je suis passé devant la juge qui a validé la peine proposée par le procureur, elle (la juge) m'a bien signifié que je pouvais aller régler l'amende dés le lendemain au Trésor Publique, que si je payé dans le mois je pourrais bénéficier de 20 % de rabais, et que c'était valable même si je payé en plusieurs fois.
Et devinez quoi, je me suis présenter pour régler l'amende une semaine après en me disant que j'allais pouvoir en finir avec tout ça et échelonner les paiements (adieu vacances d'été 2015 au passage), et bien non, j'ai appris qu'il fallait que j'attende de recevoir un papier (la décision du juge ou un truc dans le genre) et que les 20 % n'étaient pas applicable si je payais en plusieurs fois.
Car, ah oui j'ai oublié de le mentionner, il faut ajouter 127 euros pour les frais de dossier.
Donc un total de 877 euros, moins 20 % ça réduit à 701,60 euros, ce n'est pas rien.
Du coup voilà encore un exemple fabuleux, la juge affirme des choses qui s'avèrent fausses à l'autre bout, et le pire dans tout ça c'est que j'ai bouffé un RTT pour m'y rendre, y a de quoi avoir la rage !

Si quelqu'un connaît le fin mot de ce système ça m’intéresse de le savoir.