Questions for Cyril

Est ce que tu peux nous en dire plus sur toi ? Qui es tu ? Que fais tu dans la vie ? Est ce que tu es marie avec des enfants, etc... ?

Je suis Cyril, j'ai 32 ans, 2 enfants, non marié. Je suis employé comme chef de projet chez un éditeur de logiciels, mais actuellement en congé sabbatique pour quelques mois.
Je suis en train de monter mon entreprise d'édition de logiciels / et de recherche en sécurité informatique. D'ailleurs, je recherche des projets et clients dans ce 2ème domaine, pour de la recherche, du consulting, ou des formations !

Quel groupe ecoutes tu en ce moment ?

Je suis fan de Muse, Linkin Park et très récemment C2C.

Qu'est ce que tu fais quand tu n'es pas derriere l'ecran de ton ordinateur ? Des passions, des hobbys ?

Je sors voir des amis, boire des bières en ville. J'aime le cinéma, j'y suis un week-end sur deux. Sinon je regarde pas mal de séries à la télévision. Je suis fan de Dr House et de Mentalist par exemple.

Durant JailbreakCon, j'ai pu m'appercevoir que tu es un mec assez humble. Qu'est ce que ca fait d'etre une rock star ?

J'ai du mal à répondre à cette question car je ne me considère vraiment pas comme une rock star !

Comment as tu commence a programmer et a hacker ?

J'ai commencé le programming très tôt. A 5 ans je recopiais déjà des programmes BASIC d'un livre de mon père sur mon ZX 81. Ensuite, j'ai écris mes propres, puis des minis jeux, des applications, etc.

Mes vrais réalisations sont sur Atari ST ou j'ai écris des demo techniques en GFA BASIC et assembleur 68k (pour les puristes: overscans, rasters, roto-zooms, etc.)

Pourquoi travailles tu sur iOS plutot qu'une autre plateforme ?

Je suis fan d'Apple, que ce soit pour les devices iOS ou les ordinateurs. J'ai par exemple un MacBook Pro et un iMac.

iOS est une version réduite d'OSX, mais tout est là. Le même plaisir d'avoir un unix comme coeur du système : jailbreaké, cela donne accès à tous les classiques GNU et opensource. Aussi, le code source du kernel XNU est disponible en ligne, et tout un

chacun peu donc lire son code à la recherche de failles éventuelles. Cela procure une fiabilité et une sécurité extrême. Trouver des failles et les exploiter devient donc un challenge important, reconnu dans le domaine.

iOS dispose aussi du catalogue d'applications mobile le plus vaste et le plus qualitatif, la review des applications par Apple augmentant naturellement le niveau. Aussi, le fait que le matériel et le logiciel soient gérés par Apple limite fortement la fragmentation de marché (les utilisateurs sont en grande majorité sur la dernière version du système, et s'oriente petit à petit vers le dernier matériel en date).

On est très loin du modèle économique d'Android, où c'est le prix qui régit le marché, et non la qualité. La fragmentation est présente à tous les niveaux : version du système, matériel, surcouches constructeurs. Un cauchemard pour les développeurs et les chercheurs en sécurité.

L'intérêt de travailler sur iOS, c'est la garantie que sont travail va toucher une grande fraction de la population, et sera pérénisé pour plusieurs années.

Que dire aussi de la qualité de l'écosystème Cydia ? Les développeurs sont talentueux (car c'est un défi aussi de modifier un système sans avoir son code source), les tweaks ingénieux, et les thèmes et modifications graphiques nombreuses.
Ce n'est pas un hasard si beaucoup des idées des tweaks sont reprises aussi bien dans iOS que dans Android.

Si je voulais devenir le prochain pod2g, quels conseils pourrais tu me donner pour commencer ?

Déjà, cela n'est pas forcément donné à tout le monde, il faut de solides connaissances dans le développement, mais aussi dans le fonctionnement d'un système d'exploitation moderne.
Pour commencer, il faut donc lire de nombreux livres et documents traitant du sujet. Les plus intéressants spécifiquement pour le hacking d'iOS sont :
- OSX Internals (Amit Singh)
- A guide to kernel exploitation - attacking the core (Enrico Perla, Massimiliano Odani)
- Mac Hacker's Handbook (Charlie Miller, Dino Dai Zovi)
- iOS Hacker's Handbook (Charlie Miller, Dino Dai Zovi & others)
Ce n'est qu'une fois que la grande partie des notions abordées dans ces livres est assimilée que l'on peut se lancer dans le jailbreaking.

Après, l'idée n'est pas le succès, l'idée est d'aider la communauté et de réaliser des outils pour elle.

Le secret est la passion.

Combien d'iPhones et d'iPads possedes tu ? Quels modeles ?

iPod 3, 4 - iPhone 4, iPhone 4S, iPad 2, iPad 3

Est-ce qu'ils sont tous jailbreakes ?

Tous mes devices sont jailbreakés sauf mes devices de tous les jours (iPhone 4S, iPad 3) ne le sont pas pour 2 raisons :
- me forcer à travailler sur le jailbreak d'iOS6
- je les utilise pour développer une application officielle, et souhaite donc qu'ils soient dans une configuration standard

Est ce que tu utilises beaucoup d'appli jailbreak ? Quels sont tes apps jailbreaks preferes, et pourquoi ?

J'en utilise peu, mais voici ma liste d'indispensables :
*- OpenSSH : pour accéder au filesystem de l'iPhone en toute simplicité, et pour la recherche en sécurité (j'ajoute ensuite tous les packages en .*cmds, .*util)*
- SBSettings : pour l'accès rapide à tous les réglages indispensables de l'iPhone
- Barrel : j'adore l'effet geek qu'il procure. Tout le monde sait au premier coup d'oeil que t'es jailbreaké
- IntelliScreenX : pour avoir son réseau social en un slide du doigt. Réalisation superbe.
- 5 icons dock : pour ajouter twitter sans supprimer les icones d'origine dans le dock.

Ou est ce que tu vois la communaute jailbreak dans 12 mois ? Sommes nous sur la bonne voie ou sommes nous dans une impasse ?

Je suis confiant pour les 6 prochains mois. Je pense sincèrement qu'iOS 6 sera jailbreaké, et que les développeurs vont continuer dans leur lancée, avec toujours plus de qualité. Les discussions sur les prochains tweaks à JailbreakCon ont ouvert de nouvelles perspectives d'amélioration d'iOS. La créativité ne va pas s'arrêter !

Vis à vis du jailbreak des versions suivantes, je ne sais pas véritablement quoi en penser. Je reste convaincu que le travail d'Apple va rendre la difficulté de la tâche telle que l'on ne pourra plus parvenir à trouver les différentes failles imparties dans un temps convenable.

Mon message à Apple : pourquoi ne pas arrêter ce combat, et ouvrir à l'utilisateur le choix d'installer des applications non signées, comme c'est le cas sur OSX ? Le faire de la bonne façon, pour limiter le piratage, mais rendre possible les tweaks ?
Je suis intimement convaincu que cela permettrait encore de gagner des parts de marché à Android, et de devenir complètement incontournable.

Quelle est la principale question que les gens te posent generalement ? Comment reponds tu a cette question ?

La question principale (sans compter les informations sur la date de release du prochain jailbreak) est comment commencer / aider. Ma réponse est toujours la même :

lire iOS Hacker's Handbook. Le problème est que les gens ne se rendent pas forcément compte de la difficulté. Ils pensent qu'il s'agit simplement d'installer une application sur le device et c'est fini !

Certaines personnes vendent leurs exploits. N'as tu jamais pense a tirer profit de ton travail ? Pourquoi ?

Ma réponse est liée à celle de la question suivante. Je souhaite toucher le maximum de personnes avec mon travail, c'est ce qui me passionne. Faire payer de quelques manières que ce soit le jailbreak le ferait imploser de lui même, le rendant inétéressant aux yeux de tous.

Si l'argent n'est pas ta source de motivation principale, qu'est ce qui te motive ?

Ce qui me motive, c'est le mass market, toucher avec un logiciel un maximum de personnes. Qu'est-ce qui pourrait être plus motivant alors qu'un jailbreak, téléchargé à des millions d'exemplaires ?

Il y a moyen de faire un don a la Chronic Dev Team, est ce que cet argent est distribue equitablement ? As tu donc deja tire profit de ton travail ?

- ne souhaite pas répondre à cette question -

Il semble que tu sois le principal responsable du dernier jailbreak, pourtant le jailbreak a ete presente sous l'efigie de la Chronic Dev Team. Tu n'as pas l'impression que tu te fais voler la vedette quelque part ?

La « Chronic Dev Team » n'est presque pour rien dans les 2 derniers jailbreaks. Les personnes ayant véritablement contribué sont, par ordre alphabétique : @MuscleNerd, @pimskeks, @planetbeing, @saurik.

Par contre, l'infrastructure dont dispose la « Chronic Dev Team » (serveurs WEB, IRC, etc.) a permis le travail en équipe et la release dans de bonnes conditions.

Les membres de cette équipe sont mes amis, et c'est grâce à notre collaboration passée que j'ai pu acquérir les connaissances nécessaires. J'entretiens donc une bonne entente avec eux, et c'est pour cette raison que j'ai souhaité qu'ils soient tout de même mis sur le devant de la scène.

J'avoue toutefois qu'entendre que le jailbreak a été réalisé par la « Chronic Dev Team » me fait bondir, et que c'est une des raisons qui m'ont poussé ces derniers mois à m'en éloigner.

Heureusement qu'une grande partie des gens ne sont pas dupes, et me suivent sous twitter, c'est mon moteur !

Que penses tu d'i0nic qui nous taquine sans arret avec un nouveau jailbreak alors qu'on sait qu'il ne le lancera surement jamais au public ?

C'est assez déprimant, il prend souvent un malin plaisir à créer des « trolls ». D'un autre point de vue, je pense que cela lui permet de renforcer son buisness. Je suis donc partagé !

Tu as recemment dit que tu ne travaillais pas sur un jailbreak pour iOS 6. Y a t'il une chance que tu changes d'avis ? Si oui, qu'est ce qui te ferait changer d'avis ?

Il y a une véritable chance que je change d'avis, d'ailleur j'ai déjà passé quelques heures depuis WWJC, mais je manque toujours cruellement de temps.

Ce qui me pousse ? Travailler avec @planetbeing. Il est toujours plein de bonnes idées, et cela monte le niveau.

Est ce que tu ressens une certaine pression des utilisateurs de jailbreak ? Il semble que toute la communaute repose en fait sur toi et une poignee d'autres hackers.

Je ressens une forte pression oui, mais je crois qu'une bonne partie de mes followers comprennent que cela n'est pas notre travail, et que l'on fait de notre mieux pour concillier travail, vie personnelle, et jailbreak.

J'ai souvent des mentions positives sur twitter, me disant de ralentir, que l'on a le temps, qu'il faut peut être attendre iOS 6.1, etc.

Je me raccroche à ça.

A JailbreakCon, tu as dit qu'il n'y avait pas assez de hackers qui travaillent a trouver des exploits. Comment penses tu que la communaute jailbreak pourrait en quelques sortes "recruter" des hackers ? Comment concentrer tous les efforts et etre sur que tout le monde travaille ensemble au lieu de travailler chacun dans son coin ?

J'y ai beaucoup réfléchi à JailbreakCon. Recruter des personnes pour aider n'est pas une tâche facile, car le profil :
- doit être passioné par iOS / OSX
- doit être un hacker de talent
- doit avoir du temps à consacrer à cette tâche
- ne doit pas faire partie d'une entreprise de recherche en sécurité, car il pourrait alors utiliser notre travail à d'autres fins
- doit être loyal et ne doit pas chercher la popularité à tout prix, car le risque est alors qu'il divulgue des informations crutiales permettant à Apple de fixer les failles avant la release du jailbreak

Je pense que le meilleur endroit pour rencontrer ces profils est à HITB par exemple, car les personnes assistant à ce type de conférence sont assurément talentueuses. Ensuite je crois que c'est une question de « feeling », le contact physique est donc bien venu. J'ai dors et déjà créé un channel IRC vers lequel j'inviterai les profils que je trouverai intéressants, de façon à identifier les bonne personnes, sur des travaux concrets.

Tous les yeux sont actuellement rivés sur toi. Tu as un profil qui interesse surement beaucoup d'entreprises, y compris Apple. Est-ce qu'Apple t'as deja contacte pour t'offrir un travail. Est ce que tu serais interesse de travailler pour Apple (ou une autre grande entreprise), ou est-ce que tu prefererais garder ton independance ?

Nous avons en effet plusieurs fois discuté avec Apple au sujet d'un poste éventuel, mais la réalité fait que cela ne sera pas possible. En effet, je ne peux pas quitter la France pour rester proche de ma famille, et mon choix de parcours en tant que chef d'entreprise est complètement contraire à travailler comme employé Apple. A suivre donc, l'année 2013 sera décisive pour moi professionnellement !

Chpwn a recemment montre un jailbreak sur iPhone 5 iOS 6. Est ce que tu peux nous expliquer ce qu'il a fait (sans en reveler de trop bien sur). Est ce que c'est une bonne base de depart pour un jailbreak pour iOS 6 ?

Pour faire simple, ce «jailbreak» utilise comme moyen d'injection le fait d'avoir un certificat développeur. D'autre part, il n'applique pas les modifications au kernel pour que le jailbreak soit complet, d'où sa dénomination de «failbreak».
C'est une très bonne base car cela permet aux chercheurs en sécurité d'avoir accès au filesystem, de modifier n'importe quel fichier d'iOS et d'exécuter du code non signé, en root.
Par contre, aucune des techniques empoyées par ce «failbreak» ne peut être utilisée dans un jailbreak publique.

Si tu n'es pas en train de travailler sur un jailbreak, peux tu nous parler de ce que tu fais en ce moment ?

Comme évoqué plus haut, le temps me manque, car je crée mon entreprise et travaille activement sur un logiciel. Mes revenus futurs (étant en congé sabbatique, je n'en ai plus!) dépendent de ce travail, donc je m'y consacre à 100%.

Est ce que tu as quelque chose a ajouter ? Quelque chose ou un message que tu voudrais faire passer ?

J'ai deux messages :
- *le premier à mes followers, que je remercie pour leur patience et leur support. Je ne peux pas leur garantir de travailler sur un jailbreak dans les jours à venir, mais que dès que le temps me le permettra, je serai de retour.*
- le 2ème à Apple, car j'ai été déçu de l'iPhone 5, qui n'a aucune valeur ajoutée significative par rapport à l'iPhone 4S (surtout en France, où l'on a pas de support 4G

LTE). Je ne retrouve pas l'innovation dans ce produit qu'il y avait dans les précédents. Il faut prendre des risques, ajouter des nouveaux composants améliorant l'interactivité. Pourquoi pas un écran tactile en relief ? Je suis inquiet de l'avenir, surtout avec ce système d'exploitation fermé et la pression exercée par Android.

Peux tu nous raconter une journee typique dans la vie de pod2g ?

Une journée typique ces derniers mois : réveil, recherche en développement, déjeuner, développement logiciel, souper, communication, développement logiciel et ce jusqu'à 3h du matin ! 99% de travail en somme.