Suricate Concept : Comment on a hacké Pokemon Go en moins de 2h…

Monir Morouche
Cofondateur de Suricate Concept

5 articles + Follow

July 24, 2016

Open Immersive Reader

- **De l'idée première, au hack.**

J'admets que le titre fait un peu racoleur.

Pour les gens de ma génération (25-35 ans au moment de la publication de cet article), Pokemon, c'est toute une institution. La simple évocation du nom fait ressurgir en nous, telle la madeleine de Proust, un univers tout entier : la douce ambiance d'une chambre d'écolier de la fin des années 90, baladeur CD dans la poche, casque sur les oreilles, et Game Boy Color à la main.

La première question qui se pose c'est : pourquoi hacker Pokemon Go ? La seconde : comment ?!

Concernant le pourquoi, il faut savoir qu'en matière de cybersécurité (qui rappelons-le est le coeur de l'activité de Suricate Concept…et non pas le jeu vidéo, quoi qu'en **disent nos collègues** ;)) nous avons tendance à penser que, là où il y a de nouvelles tendances et des usagers pour celles-ci, il y a un sujet sécu. Ici, on a quelque chose de parfaitement nouveau (la première application de réalité augmentée massivement utilisée), et en ce qui concerne les usagers, ils seraient déjà plusieurs centaines de millions…..

À l'agence (siège de la direction Suricate Concept), on aime profiter des pauses pour aborder de nouvelles idées insolites en matière de cybersécurité, d'angles d'attaques inédits (c'est à dire encore encore non démontrés ou exploités), ou encore se lancer des défis. C'est d'ailleurs l'un d'eux qui a mené à la publication de nos travaux de recherche sur **le hacking de pacemaker**.

Cette semaine, lors d'une réunion de crise, on a vu un de nos gars se comporter de façon assez étrange, se déplaçant dans la pièce en cherchant du regard (ou plutôt de celui de son smartphone) une chose qu'il semblait être

le seul à percevoir. C'est là qu'il nous a appris que, comme plusieurs millions de français, il s'était dégoté une version non officielle de l'application Pokemon Go, plusieurs jours avant sa sortie officielle en France. Sans faire plus attention à cela, nous avons repris nos discussions… mais dans les jours qui ont suivi, nous avons pu constater la propagation de l'épidémie : les zombies étaient désormais tout autour de nous, rivés sur leur mobile et à la recherches de choses qui n'étaient ni totalement d'un autre monde, ni vraiment du notre… quelque part dans "la réalité augmentée" !

En apprenant ce que cherchaient si avidement ces joueurs, on s'est tout de suite demandé (déformation professionnelle oblige…) s'ils ne pouvaient pas l'obtenir par des moyens détournés. 2h plus tard, nous avions un premier hack exploitable.

- **Le concept et ses failles**

Le concept : comme dans toute application de réalitée augmentée, le virtuel vient se plaquer à la réalité avec laquelle il s'agit d'interagir. Ici, l'ensemble est basé sur la geolocalisation, et tout particulièrement sur les déplacements.

En effet dans Pokemon Go, toute la mécanique du jeu et la progression du personnage sont basés sur ses déplacements, et la capacité du joueur à faire des kilomètres; ces derniers étant déterminés à partir de sa geolocalisation.

Et c'est là que résident les failles…

L'idée repose sur le fait d'envoyer de fausses coordonnées GPS de sorte à simuler une position différente de celle où nous sommes, ou un déplacement qui n'a pas été effectué dans la réalité.

Bien sûr, nous ne sommes pas les premiers à y avoir pensé, et bon nombre d'astuces et applications plus ou moins scam (= cyber arnaque) ont vu le jour à droite à gauche. La particularité de la plupart d'entre elles est qu'elles sont très rapidement détectées par l'application de la société éditrice, qui n'a pas attendu qu'on lui suggère pour mettre en place toute une batterie de contrôles sur les déplacements… Une détection sanctionnée par la désactivation temporaire (quelques heures) des fonctionnalités du jeu (soft ban), ou la désactivation totale du compte utilisateur.

L'idée était donc de mettre en place une émulation suffisamment proche de la réalité pour qu'elle ne puisse être détectée, ou du moins, qu'elle soit trop "équivoque" pour activer un "ban" de la part de l'application sans risquer de le faire sur un joueur innocent ayant simplement été victime d'un bug sur son smartphone.

Du coup… comment on a procédé ?

*/!\ La partie qui suit est plutôt technique et malgré un effort de vulgarisation, les non initiés sont invités à passer directement à la section "**Résultats**" /!*

La première chose à savoir est que le détail ci-dessous concerne un dispositif tournant sous Android. Nos tests ont été réalisé sur des modèles récents de Samsung et de

Sony, et sur différentes versions d'Android, dont particulièrement la 5.1.1

L'envoi de fausses coordonnées GPS est prévu nativement sous Android. Notamment à des fins de développement. Ainsi, en activant le mode dev, il est également possible d'activer l'option d'envoi de fausses coordonnées. Et donc, il suffirait ensuite d'utiliser n'importe quelle application permettant de réaliser cette soumission de coordonnées (il en existe une flopée sur le Play Store) ou encore de créer rapidement la sienne, afin d'arriver à ses fins…

- Premier hic : les développeurs de Pokemon Go ont bien évidemment songé à cela, et l'application vérifie le fait que cette option soit ou non activée. Dans le cas d'une activation, il est possible de se déplacer où l'on souhaite, cependant toutes les possibilité d'interaction du jeu sont désactivées (soft ban) et ce pour une durée allant jusqu'à plusieurs heures après désactivation de l'option, selon les déplacements "frauduleux" réalisés par le joueur.

Peu importe, on vas passer par une application qui envoie ses propres coordonnées, après tout, on n'a pas besoin d'une autorisation Android pour pouvoir le faire.

- 2nd hic : si l'application arrive bien à soumettre de fausses coordonnées, le véritable GPS quant à lui (alors même qu'il est toujours actif), continue de transmettre la vraie geoloc du smartphone. Résutat : votre personnage "clignotte", se téléportant toutes les quelques secondes entre sa véritable et sa fausse localisation. C'est ainsi que fonctionnent bon nombre d'applications de fake GPS. Et si elles fonctionnent très bien durant les quelques instants

nécessaires au fait d'envoyer un tweet, ou de poster sur Facebook l'endroit où vous n'êtes pas en réalité, ce fonctionnement n'est pas du tout adapté à une application qui travaille en temps réel et vérifie à intervalle régulier votre position. De tous les moyens que nous avons cherché pour faire bannir un joueur, c'est de loin le plus efficace... surtout s'il y a plusieurs dizaines de kilomètres entre les vraies et fausses localisations.

La seule façon de procéder est donc de pouvoir autoriser la désactivation du GPS standard, tout en envoyant de fausses coordonnées, mais sans pour autant activer l'option de fake position du mode développeur d'un Android… La question qui se pose à présent : comment faire ? Après quelques recherches, on se rend compte que cette manip est possible pour les applications dites "app system". Il suffirait donc de "copier/coller" notre application dans le bon répertoire (et en lui assignant les bons droits pour qu'elle puisse se comporter ainsi).

3ième hic : seul le "super administrateur" (user root) du smartphone est en capacité de le faire puisque les smartphones Android sont protégés contre son accès pour des raisons de sécurité. En l'occurrence, le constructeur de l'appareil…

Il va donc falloir "rooter" l'appareil (l'équivalent d'un *jailbreak*, pour Android) pour pouvoir réaliser cela.

Passons sur les différentes étapes pour procéder à cela, plus ou moins longues ou risquées selon l'appareil et la version d'Android, quand pour d'autres l'opération ne prend qu'un clic sur une application dédiée…

Ensuite, il s'agit donc d'aller copier/coller l'application et lui assigner les bons droits.

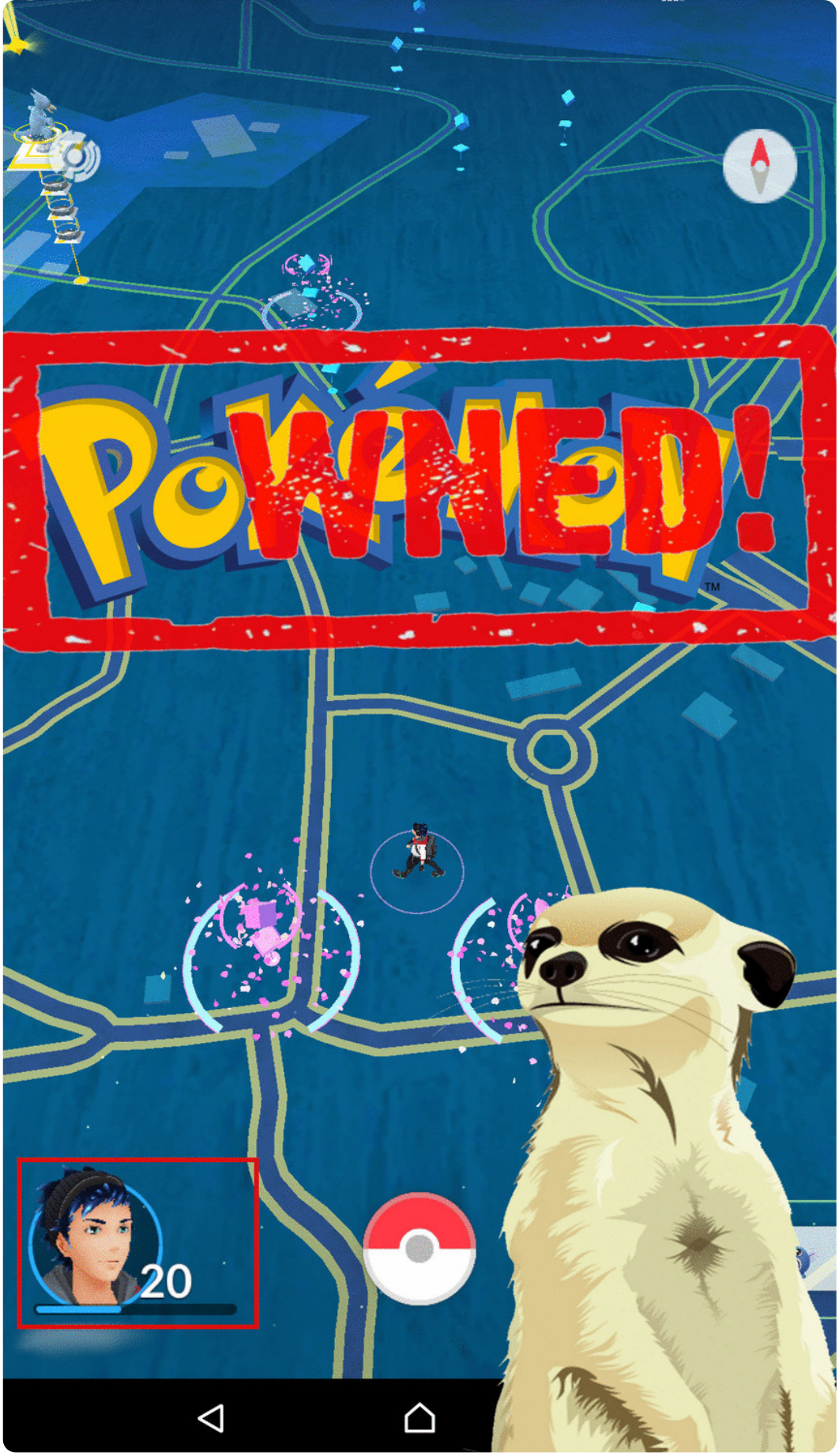
4ième hic : et pour le coup, faute à pas de chance, le premier appareil sur lequel on tombe est un Sony Xperia qui dispose d'un système empêchant l'écriture sur le répertoire system de l'appareil. Un daemon effectuant une passe toutes les secondes pour vérifier si le système permet l'écriture, et la désactive immédiatement le cas échéant…

Il nous a donc fallu trouver un script permettant à partir d'un bootloader spécifique, de pouvoir killer le process et forcer le montage de la partition en écriture.

S'en est suivi, et une fois l'application enfin installée, une bonne dizaine de tentatives différentes afin de réussir à simuler un déplacement sans se faire repérer...CF section "**Quelles parades pour ce type d'application ?"**, pour retrouver quelques exemples des sécurités auxquelles nous avons pu être confrontés.

Une fois le hack en place, il ne restait plus qu'à s'amuser...

- **Résultats**



Concrètement, la possibilité de pouvoir se déplacer librement sur toute la terre (moyennant quelques précautions), et de gagner des niveaux sans avoir même besoin de toucher à son téléphone, si ce n'est de temps en temps. En effet, l'une des principales fonctionnalités du

jeu repose sur le fait “d’incuber” des oeufs, qui éclosent une fois une certaine distance parcourue, cela ayant pour conséquence de faire prendre de l’expérience et donc des niveaux au joueur.

Par ailleurs, certains emplacements sont particulièrement prisés, sans toutefois être physiquement accessibles pour des raisons diverses (horaires d’ouvertures d’un parc, obstacles tels qu’une étendue d’eau à traverser, etc…). L’accès à ces lieux permettant également d’enrichir rapidement sa collection de nouveaux pokemons, gagnant ainsi beaucoup plus rapidement des niveaux.

Des déplacements rapides afin d’activer tous les points de contrôle d’une zone (pokéstops), pour accélérer encore son gain d’expérience.

En une demi-journée (hack inclus), un membre de l’équipe a pu atteindre le niveau 20, sans pour autant quitter son bureau et en vacant à ses occupations habituelles (traitement de ses emails, confcall, etc…); ce niveau n’étant normalement accessible qu’au bout de plusieurs semaines d’efforts, si la personne n’utilise son application que durant ses déplacements quotidiens.

- **Quelles parades possibles pour ce type d’application ?**

Alors bien sûr, cette section peut se lire dans les deux sens, et la parade de l’un fait l’opportunité de l’autre. C’est une des premières choses qu’apprend à faire le pentester : comprendre que l’existence d’une protection

nous donne des informations sur l'existence d'une faille, voir même sur comment contourner ladite protection…

Les éléments cités ci-dessous tiennent à la fois comptes des intégrations actuelles de l'application, mais également de celles possibles mais pas nécessairement encore implémentées.

- Sécurités physiques :

Cela va de soit, la meilleure des sécurités numériques reste encore celle qui est couplée à une sécurité physique. On peut envisager que les futures gros events couverts par l'application devront être validés physiquement par les personnes afin qu'elles attestent de leur présence sur place. Si cela devait se faire au travers de technologies comme le NFC (et cela est fort probable au vue de la nécessité de traiter rapidement un grand nombre d'authentification et de façon non contraignante pour l'usager), on sait d'avance que **des parades sont possibles**.

- Vérifier l'opérateur télecom :

Un usager Free Mobile connecté sur sa 3G et qui serait pourtant geolocalisé au beau milieu du Sahara, c'est suspect non ? Vérifer la disponibilité de l'opérateur sur une geolocalisation donnée nous semble plutôt pertinent.

- Suivi du gyroscope :

Un smartphone qui effectuerait de longs déplacements mais dont le gyroscope n'aurait que quelques soubresauts à l'occasion, ressemblerait plus à un appareil

confortablement posé sur un bureau qu'à un appareil secoué par une intense randonnée.

- Vérification de l'altitude :

On a tendance à l'oublier, mais des coordonnées ce ne sont pas seulement des chiffres qui indiquent qu'on est plutôt à droite ou plutôt à gauche, c'est aussi le fait de savoir si l'on est plutôt en haut ou plutôt en bas ! Or, la plupart des personnes qui tentent de simuler un déplacement ne tiennent absolument pas compte du relief. Aussi, elles vont effectuer des translations latérales en gardant la même altitude (généralement entre 0 et +100m au dessus du niveau de la mer sur la plupart des app); ce qui est quand même très suspect pour quelqu'un qui se déplace autrement qu'en drone...

- Vitesse :

À moins d'être un pilote de chasse ou un super heros, vous ne devriez pas être en capacité de vous déplacer d'un bout à l'autre du pays en quelques minutes; et si c'était le cas, vous ne devriez pas avoir une connexion internet aussi stable...

- Linéarité des déplacements :

Il vous arrive souvent de vous déplacer en parfaite ligne droite, à un rythme très régulier, comme si vous suiviez l'étoile polaire mais sans tenir compte des lois de la physique (franchissement des points d'eau et des bâtiments) ?

- Géolocalisation à partir d'autres outils que le GPS :

Votre wifi, les bluetooth beacons que vous croisez, et d'autres éléments (nous avons parlé du réseau mobile et nous pourrions également évoquer les antennes relais) permettent d'apporter plus de précision à votre geolocalisation et ils sont d'ailleurs allègrement utilisés par les GPS routiers. Si votre GPS dit que vous êtes à Tokyo mais que votre livebox dit que vous êtes toujours dans votre salon, méfiez-vous ! car l'un des deux ment très probablement…

- Fréquence des arrêts :

Contrairement à une sonde spatiale, un humain doit s'arrêter régulièrement, ne serait-ce que pour des raisons physiologiques… Si votre GPS indique un mouvement permanent, plusieurs dizaines d'heures durant, c'est qu'il est sûrement à la dérive sur un bâteau...

- Précision dans la géolocalisation :

Chaque recalcul des coordonnées donne un résultat différent. Avec un simple smartphone (même haut de gamme), il n'est pas possible d'atteindre une précision au delà du mètre, si vous êtes à 10m près, c'est déjà pas mal ! Si votre GPS renvoi plusieurs fois consécutives exactement la même position, c'est qu'il ne l'a sans doute pas calculée...

- Horaires de déplacements :

Si votre GPS n'a pas besoin de dormir, il n'en est pas de même pour votre corps. Si vous avez respecté scrupuleusement tous les points de contrôle ci-dessus, il y en a peut-être un que vous avez négligé : se déplacer plus

de 20h par jour, même en faisant des pauses… c'est juste pas humain.

- Fréquence d'envoi des données GPS :

Si vous êtes en déplacement (et donc dans la nature), vous ne devriez pas avoir une connexion internet aussi parfaite que chez vous. Si vous envoyez à l'application des données à un intervalle d'une régularité métronomique, assurément, vous n'êtes pas en vadrouille !

- Passage trop régulier d'une application à une autre :

Si vous switchez trop régulièrement entre une application et Pokemon GO, surtout si cela se traduit immédiatement par un mouvement de votre personnage, c'est assez suspect. L'autre application ne serait-elle pas celle qui fait bouger votre avatar ?

- Etc etc…..

Des exemples comme ça nous en avons des centaines, et cela illustre bien les difficultés, d'une part pour l'éditeur qui doit trouver des parades infaillibles (car bon nombre des comportements ci-dessus pourraient aussi survenir parfois suite à des bugs de leur appareil), d'autre part pour les développeurs qui s'adonnent au jeu du chat et de la souris avec les pirates… Nous en restons là pour ce listing, faute de pouvoir être exhaustif (et nous réserverons cela pour un consulting chez les sociétés éditrices intéressées ;))

Ce qu'il faut bien comprendre, c'est qu'il existe autant de façons de repérer un piratage que de possibilités de les rendre indétectables, et tandis que les uns doivent faire

vivre une application et sa communauté, n'ayant que l'aspect sécuritaire à l'esprit, les autres font de leurs piratages leur fond de commerce et y consacrent absolument tout leur temps, avec pour objectif de maximiser leurs revenus.

- **Conclusion**

On peut s'étonner de voir un groupement de boîtes dans la sécurité informatique, reconnues sérieuses, se lancer dans une étude (si courte soit-elle) qui a pour seul objectif de montrer qu'il est possible de tricher à un jeu vidéo.

Celui qui suit l'actualité en matière de cybersécurité se rend pourtant bien compte qu'il s'agit ici de seulement 2h de bidouilles, mais qui peuvent déjouer les protections d'une société ayant probablement investi plusieurs millions dans sa sécurité.

Et s'il n'est pas ici, une fois n'est pas coutume, question de mettre en avant un risque pour la sécurité des données de l'usager (**ou de l'usager lui-même**), on peut envisager un risque économique pour l'application, de voir proliférer des "robots" qui vont pouvoir générer très rapidement des ressources rares et prisées, bien que virtuelles, mais qui s'échangeront ensuite contre de l'argent, lui bien réel.

Pour information, et au moment de la rédaction de cet article, les revenus générés par la société éditrice de Pokemon Go sont estimés à 1,6 million d'euros par jour, alors que celle-ci n'est pas encore déployée dans la majorité des pays.

L’un de nos employés nous a d’ailleurs suggéré de revendre à pris d’or des smartphones disposant du hack, nous lui avons alors rappelé que nous n’étions pas les pirates mais bien ceux qui luttent contre eux... (on prend quand même les bitcoins :D).

Dans la foulée, un conseil aux joueurs qui, emportés par la passion se sentiraient prêts à succomber à l'appât d’un gain facile, moyennant finance ou via l’installation d’un “outil pirate” : la quasi totalité de ce qui est présent sur le web est soit un scam, soit un logiciel qui aura pour conséquence de vous faire bannir votre personnage. Que ce soit dans l'immédiat ou à l’issue du prochain correctif sécurité déployé par l’éditeur. Nous avons observé tous types de pratiques, et celles induisant un règlement de la part du joueur se traduisent systématiquement par un vol de données bancaires, un vol du compte, ou l’abonnement à des services tiers très difficiles à résilier. Concernant les méthodes gratuites, nous vous rappelons cet adage : ***When something is free, YOU are the product***…

D’ailleurs, nous rappelons à tous les joueurs français qui se sont procurés le jeu sur Internet avant sa sortie officielle en France, que le fichier qu’ils ont installé est par conséquent tout sauf officiel, et les premières versions infectées sont non seulement déjà en circulation, mais elles ont déjà fait des dizaines de milliers de victimes…

Finalement, nous demandons à tout lecteur de ne pas chercher à nous contacter afin d’avoir des renseignements sur comment mettre en oeuvre le hack sur son smartphone. Nous ne saurions cautionner cette pratique et encore moins la soutenir techniquement. L'objet de cet

article est uniquement d'informer et certainement pas d'inciter. Aussi, **merci de ne pas harceler ni la direction, ni les employés** ;)

Suricate Concept est un groupement d'entreprises et experts liés au domaine de la cybersécurité. Suricate Concept aborde les problématiques de la sécurité informatique sous différents angles, dont ses aspects techniques, humains, stratégiques ou légaux.
Régulièrement, le labo R&D de Suricate Concept publie ses travaux de recherche lors de conférences ou démonstrations publiques. On peut citer parmi les derniers travaux, la sécurité des objets médicaux connectés (démo hacking de pace-maker), la sécurité des cartes de fidélité et bancaires (démo hacking de cartes NFC/RFID), la sécurité SEO (démo hacking de référencement sous Google), etc...
Plus d'infos: **www.suricateconcept.com**

Published by

Monir Morouche
Cofondateur de Suricate Concept
Published • 7y