

On a visité le «Donjon», la forteresse de Ledger pour se prémunir des cyberattaques contre ses produits

EXCLU - Pour la première fois, un média a pu pénétrer dans l'un des lieux les plus stratégiques de Ledger : le «Donjon». Derrière ce nom, se cache une équipe de chercheurs en quête de la moindre faille de sécurité hardware et software. Maddyness vous fait visiter ce laboratoire mystérieux et confidentiel.

Temps de lecture : minute

18 novembre 2024

Il y a un mois, Ledger inaugurait son nouveau siège mondial au cœur du Marais : le «106», en référence à son adresse rue du Temple dans le III^e arrondissement de Paris. L'occasion pour la licorne tricolore de célébrer ses dix ans d'existence et d'offrir à ses salariés un nouvel outil de travail flambant neuf et ultra-moderne pour aborder les dix prochaines années dans les meilleures conditions.

Si la bâtiment de 7 500 mètres carrés compte pléthore d'espaces (café, bar, terrasses, studio de podcast, salle de gym, terrain de basket, salle de jeux...) pour offrir un cadre de travail optimal, il abrite également un lieu très confidentiel et particulièrement stratégique pour Ledger : le «Donjon». Preuve de son importance, l'étage dans lequel est situé ce «cyber-laboratoire» est en zone «orange», couleur réservée aux «développements critiques». Quant au «Donjon» en lui-même, il se trouve carrément en zone «rouge» pour des raisons évidentes de sécurité. Et à ce titre, il n'est pas possible de vous proposer un reportage photo, mais

on vous explique à quoi ressemble cet endroit méconnu et essentiel pour Ledger.

«C'est une équipe qui s'occupe de tout casser»

Dans cette forteresse aux accents numériques, pas de lutte médiévale avec des épées et des boucliers à l'horizon, mais une équipe de chercheurs qui traquent les moindres vulnérabilités dans les produits de l'entreprise tricolore, mais pas seulement, pour garantir aux utilisateurs des wallets de Ledger la meilleure sécurité possible. Créé dans la foulée de l'arrivée de Charles Guillemet, l'actuel CTO de Ledger, en 2017, le «Donjon» a une mission aussi simple que vitale : attaquer lourdement les produits de Ledger comme un hacker pour déceler toutes les failles possibles et imaginables, de manière à les corriger, pour avoir en permanence une longueur d'avance sur les cybercriminels. «*C'est une équipe qui s'occupe de tout casser*», résume avec le sourire Vincent Bouzon, en charge de la sécurité des produits et responsable du Donjon chez Ledger.

Aujourd'hui, cette équipe compte 17 collaborateurs, à raison de 60 % mobilisés sur le software et 40 % sur le hardware. «*Personne n'a le même background*», relève Vincent Bouzon, issu du monde bancaire. En effet, ce sont des profils très variés qui constituent cette «task-force» de Ledger. «*Je n'étais pas parano de base mais je ne vois plus du tout les choses de la même manière désormais ! (Rires.) Dans les wallets, il y a les mêmes composants que dans les cartes bancaires. Mais nos évolutions doivent aller plus loin que celles du monde bancaire*», observe le patron du Donjon. Pour gagner en efficacité, les équipes software et hardware sont combinées depuis six mois. Car une faille hardware peut mener à la découverte d'une faille software, et inversement.

Software et hardware

Ce dernier a deux visages : l'un assez classique qui ressemble à n'importe quel open-space d'une startup où les équipes software s'affairent devant leurs ordinateurs sur lesquels défilent un flot incessant de lignes de code ; l'autre plus scientifique avec un laboratoire où s'entassent des wallets de Ledger et d'entreprises concurrentes, des smartphones ou encore des cartes bancaires.

Dans cette partie hardware du Donjon, ces différents objets sont malmenés par une demi-douzaine d'outils pour tester les puces électroniques embarquées dans ces produits. Parmi eux, il y a notamment une sorte d'oscillogramme *«pour étudier le rythme cardiaque et la vie d'une puce»*, et le *«Silicon Toaster»*, une machine pour tester les puces électromagnétiques à l'aide du courant électrique. *«On cherche à perturber la puce pour avoir un comportement qui nous intéresse. Cela permet de détecter les failles pour que le produit soit résistant à n'importe quelle perturbation. Aucun wallet de Ledger n'a jamais été hacké»*, rappelle Vincent Bouzon. L'enjeu est de taille alors que l'entreprise française assure protéger 25 % des cryptomonnaies détenues dans le monde.

Dans ce laboratoire, des tests en tout genre sont pratiqués. Cela va d'attaques incessantes par laser, pour s'en prémunir, à des tests de température pour s'assurer que les wallets de Ledger ne livrent jamais leurs secrets à des inconnus. Mais pour arriver à un tel degré de sécurité, tout n'est pas toujours simple. *«Si on part de rien, on peut avoir besoin de six mois d'analyse pour une puce. Mais parfois, cela ne dure qu'un mois ou quelques jours si nous avons déjà un socle d'informations. En moyenne, cela prend entre deux et trois semaines»*, explique Vincent Bouzon.

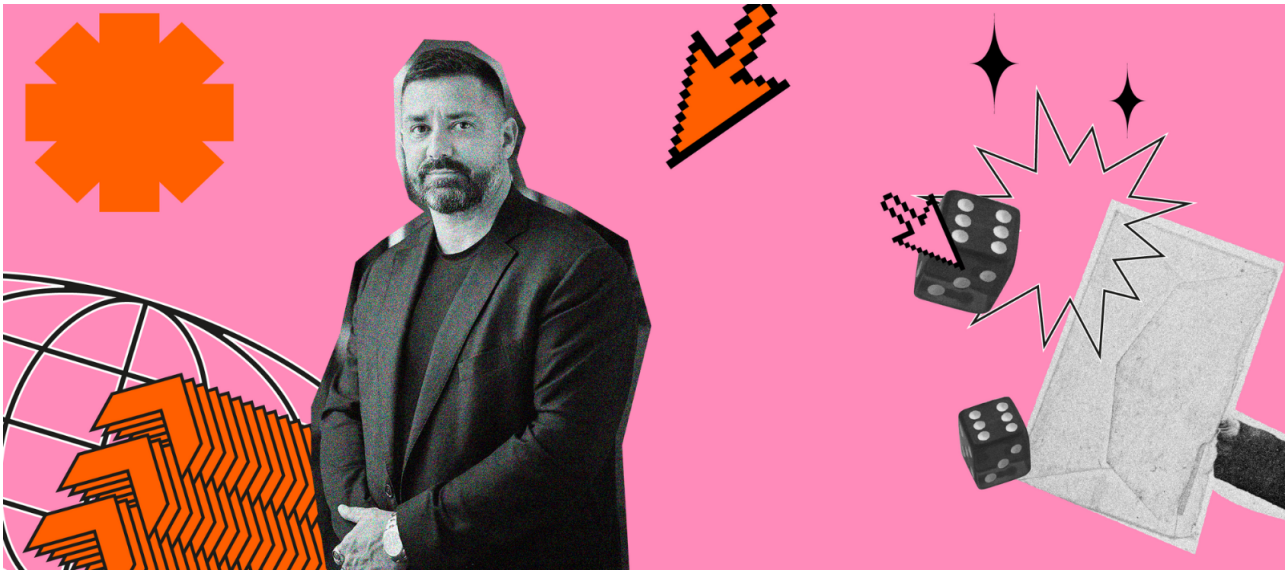
«Sécuriser l'écosystème»

A noter que les outils du Donjon sont développés et utilisés en interne, mais aussi proposés en open source à l'externe. *«La mission du Donjon n'est pas juste de sécuriser les produits de Ledger, mais de sécuriser l'écosystème. Si un autre acteur se fait hacker, il n'y a plus de confiance dans le marché. Or toute perturbation négative de l'écosystème nous impacte»*, souligne le responsable de la sécurité des produits. Avant d'ajouter : *«Tous nos produits sont certifiés par l'Anssi (Agence nationale de la sécurité des systèmes d'information, ndlr). On ne peut pas se dire qu'il y aura une faiblesse un jour. C'est notre fardeau quotidien.»* Et pour protéger ce trésor de guerre, il y a une équipe de «gouvernance de sécurité», qui s'occupe de vérifier qu'il n'y ait pas de faille en interne compromettant les découvertes et les actions du Donjon. *«Cela permet de vérifier que nos coffres forts sont solides et bien protégés»*, indique Vincent Bouzon.

Pour que cela profite à tout l'écosystème crypto, le Donjon partage toutes ses recherches en open source. Il faut dire qu'après sept ans d'existence, ce laboratoire unique en son genre s'est taillé une belle réputation. *«Historiquement, le Donjon s'est concentré sur le software, mais il y a eu beaucoup d'attaques hardware ces derniers mois. En 2025, nous allons davantage nous concentrer sur la blockchain DeFi et le Web3. C'est un univers passionnant, mais qui offre aussi de nouvelles perspectives aux hackers»*, note Vincent Bouzon. Avant de conclure : *«Il n'y a pas de magie chez Ledger, c'est juste qu'on ne fait pas de compromis sur la sécurité de nos produits.»*

Ce n'est d'ailleurs pas un hasard si des milliers de personnes se sont précipitées sur les wallets de Ledger après la faillite rocambolesque de FTX fin 2022. La licorne tricolore, qui ambitionne de devenir «la plus grande société technologique qui n'ait jamais été créée en Europe» selon son patron, Pascal Gauthier, avait alors connu *«sa meilleure journée, sa*

meilleure semaine et son meilleur mois». Et à l'heure où le bitcoin flambe à nouveau, l'intérêt pour les wallets de Ledger risque de s'en trouver renforcé.



À lire aussi

Pascal Gauthier veut faire de Ledger la plus grande entreprise technologique européenne



MADDYNEWS

La newsletter qu'il vous faut pour ne rien rater de l'actualité des startups françaises !

[JE M'INSCRIS](#)

Article écrit par Maxence Fabron