Economie&Finance

100 000

VIAGOGO VA INDEMNISER 807 INTERNAUTES LÉSÉS À HAUTEUR DE 100 000 FRANCS. Après plus de six ans de procédure, la FRC a annoncé hier avoir conclu un accord avec cet acteur du marché gris dans l'événementiel. Il se traduit par des adaptations de son site, permettant que son activité d'intermédiaire soit identifiée.

SULTAN AL-JABER
Président de la COP28
«Il faut garder l'esprit de la COP28» en vie, a-t-il déclaré hier, appelant à mobiliser non pas des milliards mais «des milliers de milliards» de dollars pour financer les promesses faites à Dubaï pour limiter le réchauffement climatique.

148

PILATUS A POURSUIVI SA CROISSANCE EN 2023, LIVRANT 148 AVIONS, a indiqué hier le constructeur aéronautique nidwaldien. Le chiffre d'affaires a progressé de 10% à 1,48 milliard de francs, tandis que le résultat opérationnel a enflé de 6% à 240 millions.

SMI 11456,96 +0,51%	↑	Dollar/franc	0,8806 ↓
		Euro/franc	0,95,24 ↑
Euro Stoxx 50 4760,28 -0,06%	↓	Euro/dollar	1,0814 ↑
		Livre st./franc	1,1134 ↑
FTSE 100 7719,21 -0,12%	↓	Baril Brent/dollar	82,48 ↓
		Once d'or/dollar	2027 ↑

«L'hydre n'a perdu que quelques têtes»

CYBERCRIMINALITÉ Le groupe de hackers LockBit, présenté comme «le plus nuisible» au monde et responsable de 25% des attaques par rançongiciel, a été ciblé par une action internationale à laquelle la Suisse a participé. Deux experts analysent cette affaire hors norme

ANOUCH SEYDTAGHIA
𝕏 @Anouch

LockBit, ce nom ne dit rien à la majorité de la population. Mais c'est le cauchemar de tous les responsables de sécurité informatique. Ce groupe de hackers est l'un des plus agressifs de ces dernières années, avec des milliers de victimes à son actif. En Suisse, des cabinets médicaux neuchâtelois, le groupe Saurer ou encore les Editions Slatkine avaient été piratés par LockBit. Dans la nuit de lundi à mardi, les autorités de dix pays, dont la Suisse, ont mis ce groupe hors d'état de nuire. Mais le combat contre ces pirates est très loin d'être fini, comme l'expliquent deux experts en cybersécurité au *Temps*: Frédéric Bourla, responsable chez Orange Cyberdefense Suisse et Steven Meyer, directeur de la société de cybersécurité Zendata.

Qui est LockBit?

Un spécialiste des attaques par *ransomware* (ou rançongiciels), ces logiciels qui permettent de pénétrer dans les systèmes informatiques des victimes, de chiffrer les données et de les exfiltrer. Le groupe de hackers serait responsable à lui seul de 25% des attaques par *ransomware* dans le monde devant un autre groupe, BlackCat (8,5%). Le Ministère américain de la justice (DoJ) avait qualifié le rançongiciel LockBit de «plus actif et plus destructeur des variants dans le monde». Sur sol américain, le groupe aurait mené plus de 1700 attaques depuis 2020, récoltant 91 millions de dollars de rançons au total. Boeing, des hôpitaux français ou encore l'établissement chinois ICBC, la plus grande banque du monde, ont été victimes de LockBit.

Les attaques provenaient du groupe de hackers lui-même, mais aussi de sous-groupes affiliés qui utilisaient ses logiciels pour viser d'autres cibles. En échange, ces sous-groupes versaient une commission à LockBit. C'est donc une véritable industrie.

Que s'est-il passé?

Une dizaine de pays, dont la Suisse, ont mené une action conjointe pour infiltrer le réseau de LockBit et prendre le contrôle d'une partie de ses infrastructures. «Fedpol a assuré la coordination avec les autorités concernées pour garantir l'échange d'informations au niveau national et international», indique au *Temps* un porte-parole de l'Office fédéral de la police. Les autorités zurichoises ont aussi participé.

«La totalité de leur entreprise criminelle a été comprise», a affirmé la NCA, l'agence de lutte contre la criminalité britannique. Il s'agit d'une opération de «contre-piratage». «Les forces de l'ordre ont exploité une vulnérabilité dans le traitement des archives des différents serveurs sur lesquels le groupe cybercriminel hébergeait ses sites sur le réseau Tor. Plus d'une vingtaine de sites initialement anonymisés par le réseau Tor sont tombés aux mains des forces de l'ordre. Ce sont sur ces sites vitrines que des extraits des données volées sont publiés par des partenaires de LockBit», détaille Frédéric Bourla.

Steven Meyer complète: «Il y a encore une certaine partie de leur infrastructure qui fonctionne, comme un système de chat interne, mais c'est marginal. Donc concrètement, quasiment tout est tombé. Il semblerait que le code source, les clés de cryptage, la liste des victimes, les chats avec les victimes, les demandes de rançon, la plateforme pour les affiliés, etc., sont tombés. Il n'y a par contre pas eu d'indication de saisie de cryptomonnaie…»

Quel est l'impact de cette contre-attaque?

Selon Frédéric Bourla, «c'est clairement un coup dur pour LockBit et pour ses affiliés. Europol a potentiellement récupéré 1000 clés de déchiffrement [pour récupérer l'accès à des données chiffrées, ndlr], ce qui occasionnera un sévère manque à gagner pour l'ensemble de ces cybercriminels, sans compter les potentielles arrestations qui découleront de l'analyse forensique desdits serveurs compromis.» Mais la plupart des membres de LockBit étant a priori en Russie, des arrestations sont peu probables, d'autant que leur identité n'est pas connue.

«Pour LockBit, c'est une énorme perte de réputation, et les forces de l'ordre capitalisent là-dessus»

STEVEN MEYER, DIRECTEUR DE ZENDATA

«Le groupe de hackers pourra sans doute restaurer ses sauvegardes sur le darkweb»

FRÉDÉRIC BOURLA, RESPONSABLE CHEZ ORANGE CYBERDEFENSE SUISSE

Steven Meyer note qu'il y a dans l'immédiat «une énorme perte de réputation, et les forces de l'ordre capitalisent là-dessus. Elles travaillent pour effriter la confiance établie entre l'équipe de LockBit et les affiliés. Si la plateforme ne fonctionne pas bien, si en l'utilisant on n'est pas payé, ou encore pire, si les forces de l'ordre arrivent à identifier la vraie identité des affiliés, alors les criminels ne vont plus utiliser la plateforme. C'est donc important pour la police de faire peur, de semer le doute et d'enlever la confiance qui existe.»

Le directeur de Zendata ajoute que l'action des polices «interrompt aussi le business. Le marché des RaaS – soit des «ransomware as a service» – est très concurrentiel, avec plus de 60 groupes différents; les affiliés vont donc très rapidement aller voir ailleurs.» A noter que LockBit a reconnu mardi avoir été ciblé par le FBI.

LockBit est-il mort?

Sans doute pas. «Ce groupe est très bon techniquement. Ses membres vont pouvoir remonter en tout cas une partie de leur infrastructure, mais, s'ils doivent recommencer le développement de leur code, ça va leur prendre beaucoup de temps. Peut-être plusieurs mois. On peut s'attendre à ce que l'équipe change le nom du groupe et recommence tout à zéro», estime Steven Meyer.

De son côté, Frédéric Bourla est tout aussi prudent. «Il y a fort à parier qu'il ne s'agira pas d'un coup d'arrêt. LockBit est une hydre qui n'a perdu que quelques têtes. Le démantèlement des *front gun servers*, c'est-à-dire les serveurs frontalement exposés, n'aura probablement que peu d'incidences sur les capacités de restauration de sauvegarde sur de nouveaux sites Tor.»

Le spécialiste d'Orange Cyberdefense Suisse fait un parallèle avec le démantèlement annoncé mi-décembre du groupe BlackCat, aussi appelé ALPHV. «Alors que 400 victimes avaient pu récupérer leurs fichiers, les cybercriminels ont ensuite pris des mesures pour sécuriser les données des 3000 autres victimes… Et de nouveaux sites ont rapidement remplacé ceux qui avaient été saisis. BlackCat reste très actif et a déjà fait 56 nouvelles victimes depuis.» ▬

CYBERESPACE

En Suisse, 2,5 millions de vulnérabilités

Le paysage internet suisse présente des lacunes en matière de sécurité. Une étude de l'infrastructure informatique connectée à l'internet public a révélé plus de 2,5 millions de vulnérabilités potentielles, en raison, par exemple, de logiciels obsolètes.

C'est la conclusion d'une étude sur le cyberespace suisse, présentée hier à l'occasion des Swiss Cyber Security Days. Pour y parvenir, la société Dreamlab Technologies a scanné à l'aide du logiciel CyObs la «surface d'attaque externe» et répertorié toutes les infrastructures informatiques connectées à internet.

Ces dernières comprennent par exemple des serveurs et des pare-feu. Au total, plus de 3,2 millions d'adresses IPv4 attribuées à la Suisse et plus de 1,8 million de domaines actifs ont été trouvés. ▬ ATS

PostFinance propose une offre de cryptomonnaies pour les particuliers

INVESTISSEMENTS La filiale bancaire de La Poste se lance sur le marché des actifs numériques, en collaboration avec la banque crypto Sygnum

GRÉGOIRE BARBEY
𝕏 @GregoireBarbey

C'est une première pour une banque d'importance systémique en Suisse. PostFinance lance une offre destinée à l'ensemble de sa clientèle dans le domaine des cryptomonnaies, disponible dès aujourd'hui. Ce sont pas moins de 2,5 millions de clients qui peuvent désormais acheter, vendre et déposer une sélection de onze actifs numériques via PostFinance. L'établissement bancaire avait annoncé en avril 2023 son intention de développer une offre spécifique pour les cryptomonnaies.

«C'est une excellente nouvelle pour l'adoption des cryptomonnaies auprès des particuliers», se réjouit Jérôme Bailly, vice-président de la Crypto Valley Association. C'est selon lui un signal majeur pour l'industrie bancaire, tant en Suisse qu'à l'étranger. «Nous espérons que cela incite d'autres banques de détail et privées d'envergure à suivre le mouvement», précise l'intéressé. Il voit dans l'annonce de PostFinance une preuve supplémentaire que la Suisse est toujours en tête de l'adoption des cryptomonnaies sur le plan mondial.

A qui s'adresse l'offre?

Contactée, PostFinance indique que seules des personnes physiques ayant une résidence fiscale en Suisse peuvent bénéficier de l'offre.

Quelles sont les cryptomonnaies proposées?

Bitcoin, Ethereum, Aave, Cosmos, Bitcoin Cash, Compound, Chainlink, Litecoin, Polygon, Uniswap et Tezos.

A la demande du *Temps*, PostFinance a précisé son choix par écrit: «Notre offre couvre dès le début les cryptomonnaies les plus importantes selon la capitalisation boursière et la liquidité du marché. PostFinance peut et va développer son offre en permanence afin de réagir aux changements de comportement du marché et/ou des clients.»

Comment fonctionne l'offre?

L'offre de PostFinance est proposée en collaboration avec la banque crypto Sygnum, basée à Zurich. Cette dernière a développé une plateforme qui permet à d'autres banques de fournir à leurs clients des services d'achat, de vente et de dépôt en passant par Sygnum. PostFinance a donc intégré ces fonctionnalités au sein de son application mobile, ainsi que sur sa plateforme de banque en ligne (e-finance).

«L'avantage de cette offre, c'est qu'elle permet aux établissements de tester le marché sans devoir en supporter tous les coûts de développement et en limitant leurs risques», analyse Jérôme Bailly. C'est donc Sygnum qui réalise de son côté les opérations de négoce en cryptomonnaies, et qui se charge de la conservation des actifs numériques pour le compte de PostFinance. Plusieurs observateurs estiment qu'il s'agit d'une entrée par la petite porte, mais qu'à terme, l'établissement pourrait rapatrier l'activité en interne si les résultats sont convaincants.

Que propose PostFinance?

L'achat, la vente et le dépôt d'une sélection de onze cryptomonnaies parmi la trentaine proposée par la plateforme de Sygnum. PostFinance met en avant la sécurité des investisseurs parmi les avantages de son offre. En effet, contrairement à d'autres intermédiaires financiers, les cryptomonnaies ne figurent pas au bilan de la banque, ce qui signifie que les particuliers sont protégés en cas de faillite.

Par ailleurs, la détention de cryptomonnaies par le biais d'un portefeuille numérique (*wallet*) implique une grande responsabilité de la part des utilisateurs. La perte de la clé privée (le code cryptographique qui permet d'accéder au portefeuille) va de pair avec la perte définitive des cryptomonnaies associées. Les utilisateurs de PostFinance qui égarent leurs identifiants pour accéder aux services de l'établissement ont la possibilité de les récupérer en contactant la banque.

Les clients de PostFinance peuvent aussi mettre en place un plan d'épargne en cryptomonnaies dès 50 dollars, et effectuer des achats récurrents. Par ailleurs, la banque a mis en place sur son site web des informations destinées aux clients désireux d'acquérir des actifs numériques mais qui n'ont pas encore de connaissances dans le domaine.

Faut-il y voir une révolution?

Non. Comme le rappelle Sygnum sur son site web, quelque 15 banques ont déjà recours à sa plateforme pour proposer à leurs clients des services dans le domaine des cryptomonnaies. C'est le cas de plusieurs banques privées et banques cantonales. PostFinance est néanmoins la première banque de détail d'envergure à se lancer sur ce marché. C'est le signe que les cryptomonnaies intéressent de plus en plus d'acteurs institutionnels.

A noter que La Poste s'était déjà illustrée par le passé auprès des amateurs d'actifs numériques en proposant en novembre 2021 une série de timbres exclusifs reposant sur des certificats numériques (NFT). Elle a depuis créé deux éditions supplémentaires. L'offre de PostFinance dans les cryptomonnaies pourrait bien être observée de près à l'international. ▬