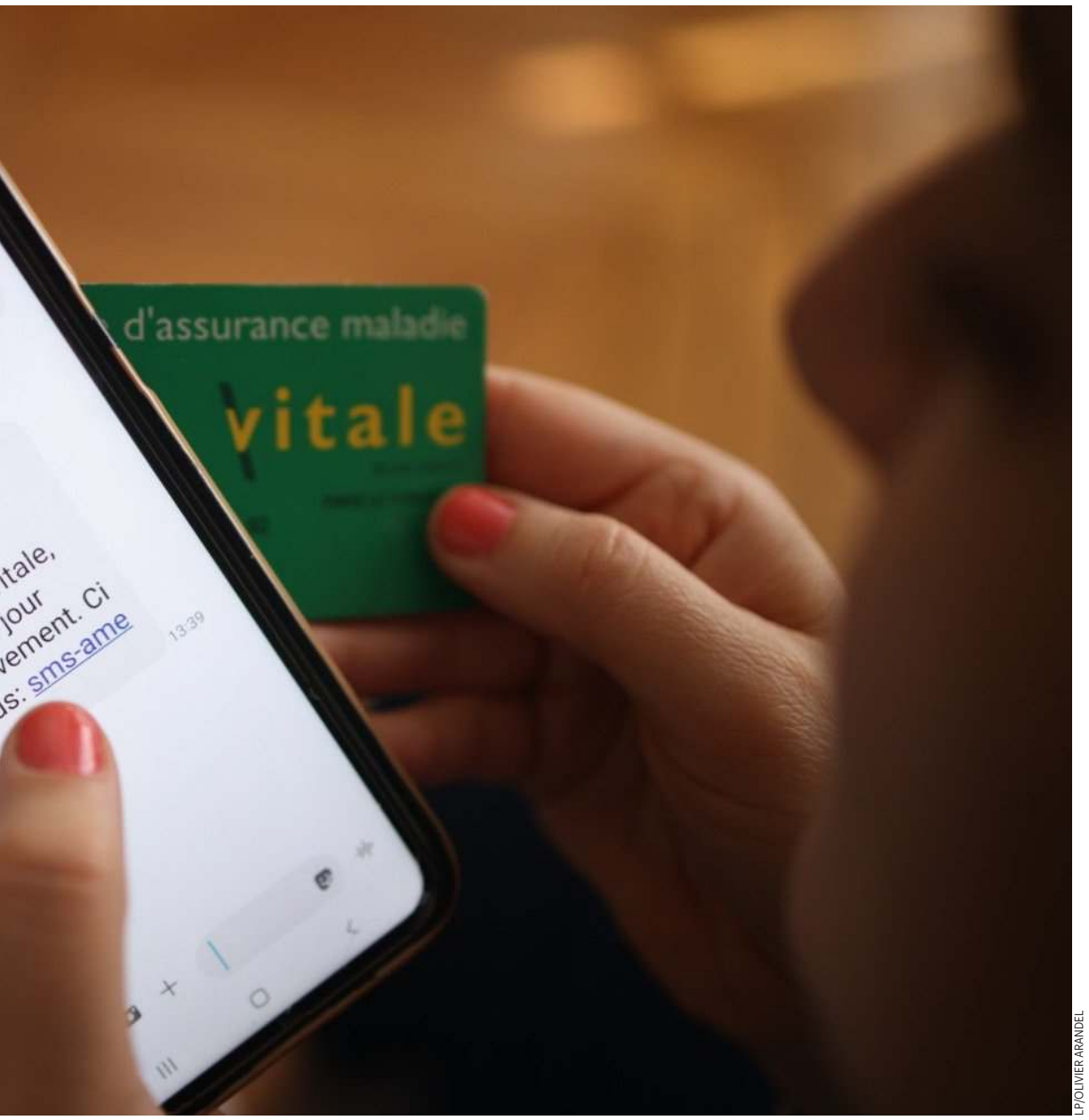

LP/OLIVIER ARANDEL

time d'une ouverture de crédit à la consommation à son nom, s'est ainsi vu délester de la somme de près de 20 000 €. « Et dès lors que les opérations sont validées par les victimes elles-mêmes, elles ne seront pas remboursées », prévient le commissaire Charlotte Huntz, cheffe par intérim de la ST de Paris, qui appelle « à la plus grande vigilance ». Selon la commissaire, les profils des victimes sont très disparates. « Vous pouvez avoir une dame âgée incapable de se servir d'un ordinateur, comme un avocat ou un jeune très à l'aise avec les nouvelles technologies… Tout le monde peut se faire piéger par ces escroqueries particulièrement bien ficelées, montées par des équipes parfois très structurées. »

D'anciens cambrioleurs reconvertis dans les arnaques

L'exploitation des images de vidéoprotection des magasins où les achats frauduleux seront effectués, mais aussi des caméras de la Ville de Paris, de la téléphonie, et des comptes bancaires utilisés pour réceptionner les virements frauduleux, mettront les enquêteurs sur les traces d'une bande originaire des XXe et XIe arrondissements. « Ce sont des amis de quartier », glisse une source proche de l'enquête. Pour la plupart, des délinquants déjà connus des services de police pour des vols avec violence et des cambriolages, qui ont flairé la bonne affaire en se lançant dans cette juteuse escroquerie.

Tête de réseau, logisticien, faux banquier, coursier… chaque protagoniste avait son rôle bien défini. Les escrocs recrutaient par « appels d'offres » sur Snapchat ou Telegram des gens qui acceptaient de réceptionner des virements frauduleux, contre rétribution, soit directement sur leur compte bancaire, soit en ouvrant un compte « fantôme ». Ils étaient capables de réaliser des fausses copies de cartes d'identité, utilisées pour récupérer les achats effectués sur l'e-commerce.

Le 22 novembre 2022, un coup de filet est organisé. Six suspects sont interpellés à Paris et en banlieue parisienne, dont le cerveau présumé de l'équipe, Gora S., un loueur de voitures déjà connu pour des faits d'escroquerie et de cambriolage. Seul le faux banquier présumé, en fuite au Maroc, a pu échapper à l'interpellation. En garde à vue, « ils nient les faits ou les minimisent ». Tous présentent des trains de vie bien au-dessus de leurs revenus officiels.

Contacté, l'avocat d'un logisticien présumé, Me Dylan Slama, a dénoncé un « dossier qui ne fait pas la démonstration claire de la culpabilité de [son] client ».

** Le prénom a été changé.*

> **Dès lors que les opérations sont validées par les victimes elles-mêmes, elles ne seront pas remboursées**
>
> **Charlotte Huntz,** cheffe par intérim de la sûreté territoriale (ST) de Paris

VIGILANCE | Ce type d'escroquerie « n'a jamais faibli depuis 2021 »

AMELI, impôts, Netflix, PayPal, Colissimo, Leboncoin, CAF… Les phishings ou hameçonnages par SMS ne connaissent pas la crise. Depuis plusieurs années, ces tentatives d'arnaques pullulent, avec des cyberpirates qui redoublent d'ingéniosité. Jean-Jacques Latour, directeur de l'expertise cybersécurité de Cybermalvaillance, la plateforme gouvernementale de prévention et d'assistance aux victimes, fait le point.

DR

Jean-Jacques Latour, expert en cybercriminalité.

Le phishing Ameli était un « hit » de l'année 2022. Quels sont les hameçonnages en vogue actuellement ?

JEAN-JACQUES LATOUR. Le phishing Ameli a connu une forte résurgence en décembre 2021. Il a été incessant pendant toute l'année 2022. Et il n'a, depuis, jamais faibli. On en repère encore aujourd'hui cinq à dix par jour, avec nos petits moyens. Ce qui est inquiétant, car ce sont des hameçonnages que l'on a l'habitude de voir par vagues : ça part et ça revient, car les cybercriminels surfent sur l'actualité. Mettre à jour sa carte Vitale en arrivant sur une nouvelle année, ça a du sens. Mi-2022, on a vu beaucoup de phishings au renouvellement de l'abonnement Netflix, ou les SMS de livraison de colis. Depuis la fin d'année 2022, nous sommes confrontés à des vagues massives d'hameçonnages à la vignette Crit'Air. Leur apparition date de septembre, en même temps que la mise en place des zones à faibles émissions (ZFE). Dans les nouveautés, on voit monter en puissance, depuis décembre, des SMS vous faisant croire que vous avez commis une infraction routière.

Tous ces phishings aboutissent-ils nécessairement à l'appel d'un faux banquier ?

On a vu le phénomène des faux banquiers prendre de l'ampleur à partir du premier semestre 2022. Mais nous avons observé aussi, notamment à la période des fêtes, le phénomène des infostealer – des « virus voleurs » – vraisemblablement opérés par des bandes organisées, qui fonctionnent depuis l'étranger. Après un clic sur le lien d'un SMS à la livraison de colis, le phishing est différent selon la marque du téléphone. Sur un Android, on vous demande de cliquer sur un lien pour suivre votre colis. Une fois que vous avez cliqué, une fenêtre s'affiche, vous demandant de faire une mise à jour de votre navigateur Chrome. Si vous cliquez sur « OK », cela vous installe un virus, qui a des fonctionnalités de vol de vos mots de passe, et qui aura donc accès à toutes vos applications. Ce virus sera même capable d'utiliser votre téléphone pour passer discrètement des appels sur des numéros surtaxés à l'étranger. Les victimes s'en rendent compte quand elles reçoivent leur facture de téléphone à quatre chiffres, avec des dépassements de forfait illimité. Sur iPhone, on vous demande de vous réauthentifier pour des raisons de sécurité à votre compte iCloud. Si vous cliquez sur « OK », vous êtes dirigé vers un faux site Apple qui vous demande votre identifiant et votre mot de passe de compte iCloud.

Comment nos coordonnées se retrouvent-elles entre les mains des escrocs ?

Nous sommes confrontés à tout un écosystème cybercriminel, nébuleux, où évoluent de petites équipes spécialisées. Vous avez des pirates qui font des collections de numéros de téléphone. Ils sont récupérés de diverses manières. Soit par des phishings précédents : si vous avez un jour donné votre numéro de téléphone lors d'un phishing, il sera intégré dans un fichier. Il va ensuite circuler entre les mains de pirates, et sera réutilisé à vie. Les numéros peuvent sinon venir de fuites de fichiers marketing. Vous vous inscrivez, par exemple, sur un site d'e-commerce et vous autorisez à communiquer vos données à des partenaires. Il se peut que, dans le lot, il y ait un partenaire véreux, qui envoie ces données à des cybercriminels. Autre possibilité : les violations de données personnelles. Je prends un exemple : à la suite du piratage d'une grande plate-forme, qui se fait voler son fichier clients, votre numéro peut se retrouver dans ces fameuses bases que l'on va trouver sur le darknet. Dernière possibilité : le scraping. Votre numéro est peut-être déjà affiché quelque part, en ligne. Sur un compte Facebook par exemple. Les pirates vont donc utiliser des programmes qui vont récupérer toutes ces données-là. Ces collections de numéros sont revendues ensuite sur des plates-formes du darknet. Les pirates qui achètent ces fichiers vont monter des kits de phishing clés en main, qu'ils revendront ensuite aux escrocs qui font du faux conseiller bancaire.

Propos recueillis par C. P.