TRAQUE D'UN CYBERCASSEUR

Il soutirait des millions d'euros aux banques sans sortir de chez lui. Après presque cinq ans d'enquête dans le monde entier, la police a fini par mettre la main sur ce pirate informatique et son gang.

Romain Raffegeau

6 MARS 2018 : L'ARRESTATION

Depuis près de cinq ans, il était l'un des hommes les plus recherchés de la planète, dans le collimateur d'*Europol* et du FBI (le service de police judiciaire des États-Unis) ainsi que de nombreuses polices nationales, dont celles d'Espagne, de Taïwan, de Biélorussie, de Moldavie ou encore de Roumanie. Un inconnu qui, avec son gang, a réussi à dérober plus d'un milliard d'euros aux banques sans jamais sortir de chez lui ! Il n'a utilisé qu'une chose : son talent de programmeur pour créer des logiciels malveillants capables d'infiltrer les réseaux bancaires.
Hélas pour lui, ce 6 mars, sa carrière s'achève. La police espagnole l'arrête à Alicante, station balnéaire située à 150 km de Valence. Fernando Ruiz, chef de la cellule cybercriminalité d'Europol, a le sourire aux lèvres : il tient enfin le principal responsable du « casse du siècle ». Retour en 5 dates clés sur cette cybertraque.

VINCENT ROCHÉ POUR SVJ

#Zoom

Europol est un organisme chargé de faciliter l'échange de renseignements entre les polices européennes pour mieux lutter contre la criminalité internationale.

DÉCEMBRE 2013 : DES DISTRIBUTEURS TRÈS GÉNÉREUX

Tout commence à Kiev (Ukraine), vers la fin de l'année 2013. Dans le froid de l'hiver, les distributeurs d'une banque locale deviennent fous. Ils crachent des billets sans que l'on ait besoin d'y glisser une carte bleue ! Devant les machines, des hommes remplissent des valises avec l'argent avant de s'enfuir. Quand la banque s'en aperçoit, c'est la panique. Son directeur engage Kaspersky, une société russe spécialisée en sécurité informatique. Ses ingénieurs découvrent alors un logiciel malveillant (malware, *voir encadré ci-dessous*) sur les ordinateurs et les serveurs connectés aux distributeurs. Baptisé « Carbanak », ce malware a été installé grâce à une méthode vieille comme Internet : l'hameçonnage *(voir encadré p. 22-23)*. Les pirates ont envoyé aux salariés de la banque un e-mail contenant des documents à ouvrir d'urgence. Les employés, naïfs, ont double-cliqué sur les fichiers, ce qui a permis d'installer le logiciel espion. Une fois avertis du piratage, les experts de Kaspersky mettent rapidement à disposition des banques un outil pour savoir si le malware Carbanak est installé sur un PC. C'est facile : il suffit de vérifier la présence d'un fichier précis dans un dossier créé par le navigateur Firefox.

2014-2015 : EUROPOL CONTRE-ATTAQUE

En fait, le malware est déjà connu d'Europol sous une autre variante depuis une alerte lancée, mi-2013, par une autre banque ukrainienne. Mais, début 2014, les pirates passent à la vitesse supérieure et s'attaquent à l'Europe de l'Ouest. Europol, aidé par la fédération bancaire de l'Union européenne, convainc les banques de revoir leurs services de sécurité et de signaler dès que possible la présence de Carbanak. En deux ans, cela permet d'établir que plus d'une centaine de banques de quarante pays sont touchées ! Les enquêteurs d'Europol remontent alors aux sources du code pour l'analyser. D'une part, cette étude permet de comprendre le fonctionnement du programme. D'autre part, elle ouvre des pistes pour tenter d'identifier son auteur. On ne s'en rend pas compte, mais chaque codeur à un « style », selon l'endroit où il a appris à coder. En étudiant la manière dont il nomme ses variables ou quels outils il a utilisés, on en apprend un peu sur sa personnalité et son entourage. Exemple simple : si un programmeur tape le nom d'une variable dans un mauvais anglais, il sera facile de supposer qu'il n'est pas natif d'un pays parlant cette langue. Si le malware est codé par plusieurs personnes, chacune ayant sa manière de faire, les enquêteurs pourront également le déceler. En scrutant le dark web (la partie « obscure » d'Internet, où tous les échanges sont anonymes), on peut aussi trouver quelques indices : certains pirates n'hésitent pas à se vanter d'avoir réussi un « coup » et tentent de revendre le programme. Pas les auteurs de Carbanak, qui ont préféré faire profil bas. Au vu de leur travail, les enquêteurs d'Europol pensent que le cerveau derrière Carbanak est d'origine slave, probablement ukrainienne.

MALWARE : L'ARME DU CRIME

Un malware est un assemblage de programmes. Certains sont codés par le pirate, mais d'autres sont légaux. Cobalt, par exemple, utilise les fonctions d'un logiciel qui permet aux services de sécurité informatique de tester des attaques sur leur réseau. Sauf que le malware, lui, attaque pour de vrai ! D'autres programmes dans le malware enregistrent ce qui est tapé sur le clavier du PC, prennent des captures d'écran (ou des vidéos), récupèrent les mots de passe et envoient le tout aux pirates par une « porte dérobée », une voie de communication ouverte entre le logiciel et les pirates. Sur les versions récentes de Windows, les malwares comme Cobalt sont neutralisés, mais les banques visées avaient des versions dépassées, très vulnérables.

#Zoom

Macro : série d'instructions destinée à automatiser les tâches d'un programme (ex : « mettre en gras les noms propres » dans Word). Elle peut servir à exécuter du code malveillant.

JANVIER 2016 : DÉBUTS DE COBALT

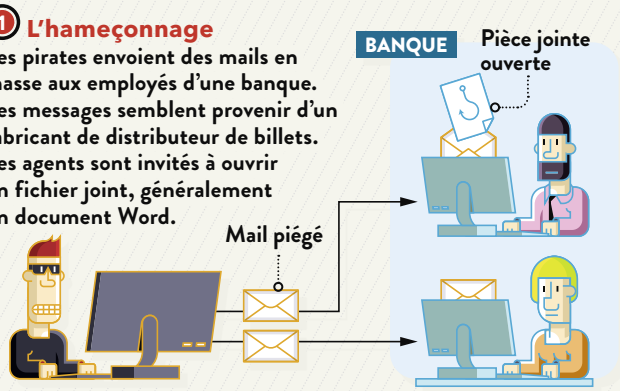
Carbanak désormais dans le collimateur d'Europol, les braqueurs ne peuvent plus agir. Il faut développer un nouveau logiciel : ce sera « Cobalt ». Puisqu'il emploie des techniques d'infiltration différentes de Carbanak, il repasse sous le radar des antivirus. Et, en plus, il est amélioré : avec Cobalt, les criminels peuvent se transférer de l'argent directement. C'est ce qu'ils expérimentent à Hong Kong et en Ukraine en mars et avril 2016, selon une autre société de sécurité informatique, Group IB. Ils choisissent un compte appartenant à une banque, augmentent virtuellement la somme déposée dessus (il suffit d'ajouter quelques zéros !) et se versent le trop-plein sur un compte à l'étranger. Celui-ci ne sert qu'à transférer l'argent sur un nouveau compte, puis est supprimé afin de ne pas laisser de traces remontant jusqu'aux pirates. La méthode permet des virements faramineux : jusqu'à 10 millions d'euros !

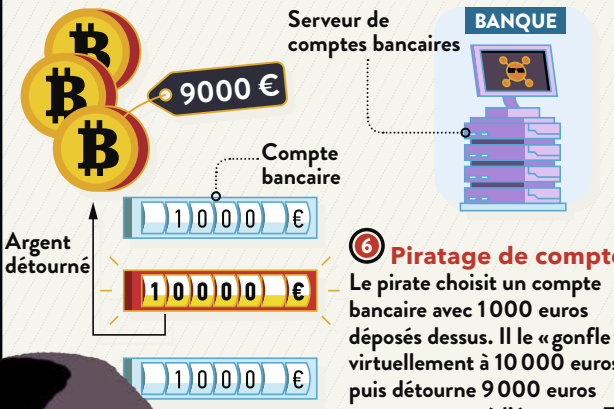
STÉPHANE JUNGERS POUR SVJ

CYBERCASSE : COMMENT ÇA MARCHE ?

1 L'hameçonnage

Les pirates envoient des mails en masse aux employés d'une banque. Les messages semblent provenir d'un fabricant de distributeur de billets. Les agents sont invités à ouvrir un fichier joint, généralement un document Word.





6 Piratage de compte

Le pirate choisit un compte bancaire avec 1 000 euros déposés dessus. Il le « gonfle » virtuellement à 10 000 euros, puis détourne 9 000 euros sur un compte à l'étranger. Et laisse les 1 000 euros de départ.

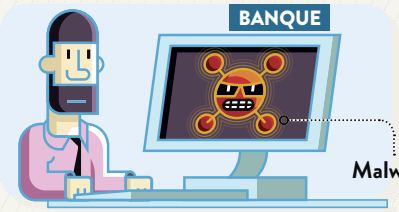
#Zoom

Un **pilote**, aussi appelé « driver », est un programme qui permet d'utiliser une carte (graphique, son…) ou un périphérique (imprimante, scanner…) sur son ordinateur.

VINCENT ROCHÉ POUR SVJ

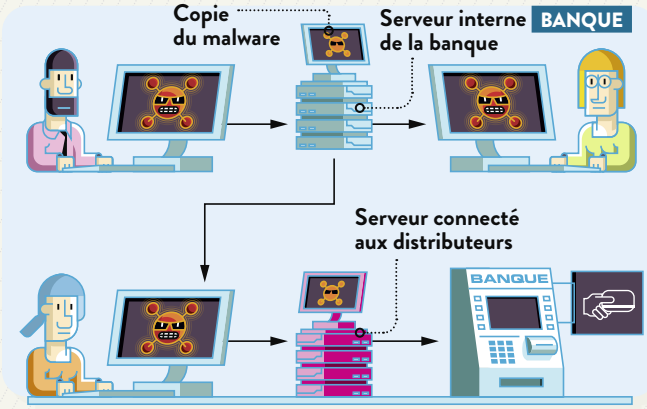
JUILLET 2016 : ATTAQUE À TAÏWAN

En plus des millions dérobés directement sur les comptes des banques, les criminels continuent de vider les distributeurs de billets. En juillet 2016, ils lancent une nouvelle attaque contre la First Commercial Bank de Taïwan. Comme à Kiev, des hommes de main sont chargés d'aller récupérer les billets devant les distributeurs. Les pirates volent deux millions d'euros en un week-end. Sauf que cette fois, la police les attend. Elle suit discrètement les porteurs de valises jusqu'à leur planque et les arrête. L'opération est payante : une large partie de l'argent est récupérée et, dans les téléphones portables des hommes de main, la police identifie un contact haut placé situé à… Alicante (Espagne).



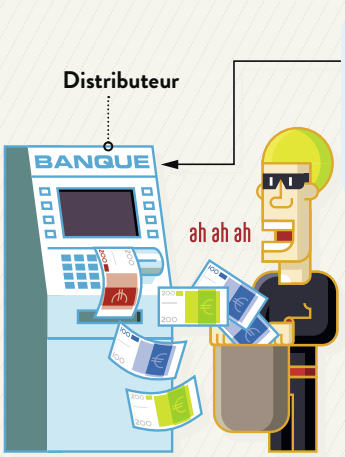
② L'infection

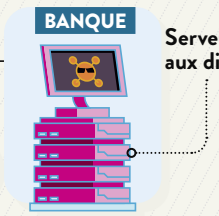
Le fichier contient une *macro* qui profite d'une faille de sécurité dans Word pour télécharger sur Internet le malware et le rendre opérant sur l'ordinateur de la victime. Le PC est infecté.



③ Survivre

La première tâche du malware est d'assurer sa «survie» : si le PC est redémarré, il ne pourra plus s'exécuter. Le programme se copie dans des dossiers comportant des fichiers toujours chargés au démarrage (par exemple, en se faisant passer pour un *pilote*). Pour toucher d'autres PC, il récupère des mots de passe qui lui donnent le droit de se copier sur des serveurs distants. Enfin, il crée une liaison pour que les pirates le commandent à distance.



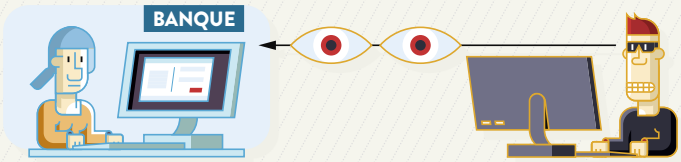


⑤ Attaque de distributeurs

Le pirate modifie le programme interne d'un distributeur bancaire. Il lui ordonne de vider les casiers de billets à une certaine heure d'un certain jour. Un complice attend devant et récupère l'argent avant de s'enfuir.

④ Espionnage

Bien installé, le malware prend des captures d'écran et les envoie, via la liaison qu'il vient d'ouvrir, aux criminels. Ceux-ci apprennent ainsi comment les employés travaillent. Ils notent à quelle heure sont mis à jour les distributeurs bancaires pour installer leur propre programme en même temps et ne pas se faire repérer. Ils surveillent aussi qui valide les opérations bancaires, afin de pouvoir simuler l'approbation d'un transfert d'argent. La surveillance peut durer des mois, après quoi deux types d'attaque peuvent être lancés.



2017 : L'ÉTAU SE RESSERRE

La piste se précise pour Europol. Maintenant qu'ils ont une adresse, la police espagnole est mise sur le coup. Carlos Yuste, inspecteur en chef spécialisé dans le cybercrime, prend en filature l'occupant du lieu. Il s'agit de Denis Katana, ou Denis Tokorenko, apparemment de nationalité ukrainienne (les enquêteurs ne confirment pas ces infos). La petite trentaine, il vit sans faire de vagues avec sa femme et son enfant dans un appartement et sort peu de chez lui. Les policiers ne le voient jamais à la plage, mais il manifeste une grande activité sur les réseaux.

Il reçoit fréquemment des visiteurs roumains ou moldaves liés au crime organisé. Afin d'obtenir davantage d'informations, Carlos Yuste ordonne des écoutes téléphoniques et découvre ainsi que Katana loue un hangar en Chine, dans lequel tournent jour et nuit des ordinateurs qui «blanchissent» l'argent volé, c'est-à-dire qu'ils le convertissent en monnaie virtuelle pour pouvoir le dépenser ni vu, ni connu. Il y a maintenant assez de preuves pour que la police puisse intervenir. Le 6 mars 2018, Denis Katana est arrêté.

APRÈS MARS 2018 : ET MAINTENANT?

Certes, le cerveau de Cobalt et Carbanak est sous les barreaux, mais il n'était pas seul. Carlos Yuste a identifié au moins trois acolytes du criminel : Illia et Alexei en Ukraine, Eugenii en Russie, qui sont toujours en fuite. Et ils sont tout autant capables d'attaquer les banques. Aujourd'hui, la menace des logiciels malveillants est l'une des plus grandes qui pèsent sur le secteur bancaire. Avec Internet, la pègre peut attaquer n'importe quelle banque, où qu'elle soit. ■

REMERCIEMENTS À BENJAMIN DELPY (CENTRE DE RECHERCHE & DÉVELOPPEMENT EN SÉCURITÉ DE LA BANQUE DE FRANCE).