L'Ukraine cyberharcelée

INGÉRENCES RUSSES 2|6 « Le Monde » publie une série d'articles sur la manière dont la Russie étend ses réseaux et son influence à l'étranger. Aujourd'hui, les attaques informatiques incessantes de Moscou contre Kiev

KIEV - *envoyé spécial*

Les locaux de l'entreprise ukrainienne Linkos – de hauts bâtiments de tôle hérissés de blocs de climatisation – se dressent de part et d'autre d'un parking où se côtoient des Lada hors d'âge et des tout-terrain rutilants. Pour les trouver, au nord de Kiev, il faut se perdre sous une voie rapide, puis franchir les voies d'un chemin de fer désaffecté. Le 27 juin 2017, lorsque la patronne de cette société, Olesya Linnik, est arrivée au travail, elle ne se doutait pas que sa modeste entreprise, qui développe un logiciel de comptabilité, était sur le point de devenir la première victime d'une agression numérique contre son pays. Depuis plusieurs mois, des pirates informatiques rôdaient dans son réseau. En toute discrétion, ils avaient dissimulé un programme virulent à l'intérieur du principal logiciel produit ici, utilisé par des centaines de milliers d'entreprises à travers le pays.

Ce 27 juin, les hackeurs décident d'activer leur charge. Peu après 13 heures, la plupart des ordinateurs des salariés cessent de fonctionner, comme presque tous ceux des utilisateurs du logiciel de Linkos. Cette société devient le patient « zéro » d'une épidémie nationale : capable de se répliquer à grande vitesse, ce virus, baptisé NotPetya – nouvelle forme d'un autre virus moins dangereux appelé Petya –, paralyse une trentaine de banques. Des supermarchés et des stations-service sont à l'arrêt, des distributeurs de billets hors service. Même les capteurs automatiques de radioactivité de Tchernobyl, à cent kilomètres au nord de Kiev, sont désactivés. La nuit n'est pas encore tombée que l'Ukraine a déjà perdu un demi-point de PIB. Bientôt, l'infection dépasse la frontière pour atteindre des dizaines de pays. Au total, elle provoquera 10 milliards de dollars de dégâts dans le monde entier.

Selon un décompte fourni récemment au *Monde* par le premier ministre ukrainien, Volodymyr Hroïsman, environ 10 % des ordinateurs des entreprises du pays ont été détruits à cette occasion, 1 500 compagnies et organisations se sont signalées comme victimes. Un bilan vraisemblablement sous-estimé selon la firme spécialisée Information Systems Security Partners (ISSP), qui a étudié de près les dégâts et y a vu une *« cyber-invasion massive et coordonnée »*. Huit mois plus tard, les Etats-Unis et leurs plus proches alliés ont conforté le diagnostic de la plupart des analystes et observateurs : la Russie est responsable de *« la cyberattaque la plus destructrice et coûteuse de l'histoire »*.

UN PAYS « PRIS PAR SURPRISE »

Près de deux ans après l'attaque, Mme Linnik en relativise les conséquences. *« Personne n'est mort à cause de NotPetya,* rappelle la patronne de Linkos. *Le vrai conflit est à l'est du pays. Là, il y a des jeunes garçons qui meurent. »* NotPetya est pourtant bien l'épisode le plus marquant d'une guérilla informatique lancinante contre l'Ukraine depuis 2014. L'élément déclencheur en a été la crise de la fin 2013 en Ukraine et les manifestations sanglantes de la place Maïdan, à Kiev. A l'époque, le président prorusse Viktor Ianoukovitch renonce à un accord de rapprochement avec l'Union européenne. De nombreux Ukrainiens descendent dans la rue, et Maïdan devient l'épicentre d'un mouvement de protestation qui durera de longues semaines et fera des dizaines de morts. Ianoukovitch a beau fuir en Russie, le pays est déstabilisé. Fin février, des soldats prorusses envahissent la Crimée, une péninsule ukrainienne que la Russie finira par annexer. Un conflit éclate dans l'est de l'Ukraine entre l'armée nationale et des soldats séparatistes ; il fera des dizaines de milliers de morts.

Le feu informatique qui a accompagné cette crise – plusieurs centaines d'actions au total – *« a pris notre pays par surprise »*, admet aujourd'hui Oleksandr Klymchuk, chef du département cyber du SBU, les services de renseignement ukrainiens. Aucune preuve formelle de l'implication russe dans ces opérations ciblées n'a été apportée : dans le cyberespace, les preuves sont rares, trompeuses, et la dénonciation n'est jamais dénuée d'arrière-pensées, surtout en Ukraine. Mais un épais faisceau d'indices techniques pointe vers la Russie, la seule à avoir intérêt à éprouver de la sorte les réseaux ukrainiens.

« Notre pays est un terrain d'essai pour leurs cyberarmes, qu'ils combinent avec une guerre de l'information et une guerre traditionnelle », analyse Victor Zhora, vétéran ukrainien de la cybersécurité. Siim Alataly, chercheur au centre de recherche de l'OTAN sur la cyberdéfense, à Tallinn (Estonie), confirme : *« En Ukraine, la Russie teste des concepts, des capacités. C'est l'endroit parfait pour comprendre comment opèrent les Russes. »*

Valerii Striganov, le responsable informatique de la commission électorale, l'instance chargée de l'organisation des élections en Ukraine, se rappelle parfaitement le premier signe du basculement de son pays dans ce conflit d'un genre particulier. Il remonte à l'élection présidentielle anticipée de 2014, qui devait désigner un successeur à Viktor Ianoukovitch, après le bain de sang de Maïdan. Le 21 mai 2014 au matin, moins de quatre jours avant le scrutin, les équipes de la commission découvrent que des pirates ont détruit, pendant la nuit, le système censé afficher les résultats sur son site. Les autorités comprennent vite que le but n'est pas de modifier le scrutin – impossible, les votes étant décomptés sur papier. Il s'agit plutôt, raconte M. Striganov, *« de diminuer la confiance dans le système électoral »*, juste avant un vote crucial.

Les experts sont confortés dans leur analyse le jour du scrutin quand un déluge de connexions s'abat sur le site, le rendant un temps inaccessible. Puis, douze minutes avant la fermeture des bureaux de vote, les pirates parviennent à modifier une page annexe où ils annoncent la victoire de l'ultranationaliste Dmytro Iaroch. Cette page a beau être inaccessible pour les internautes, l'information est reprise immédiatement par certaines chaînes de télévision russes. A l'évidence, les journalistes avaient été prévenus. Les autorités ukrainiennes y voient la preuve de l'implication de Moscou dans cette opération de déstabilisation. D'autant plus que le groupe de hackeurs qui l'a revendiquée, CyberBerkut, les harcèle depuis le début des tensions avec la Russie. Des traces d'autres groupes de pirates russes bien connus auraient également été décelées dans le réseau de la commission électorale.

Si les conséquences de ce raid restent limitées, il préfigure un cyberespace de plus en plus irrespirable pour l'Ukraine. Ainsi, en octobre 2015, le plus grand groupe de médias du pays, Starlight Media, et la chaîne de télévision TRK sont à leur tour ciblés à la veille des élections locales. Des dizaines de postes informatiques et de serveurs sont bons pour la casse. Un procédé étrangement similaire à ce qui surviendra, quelques mois plus tard, dans les locaux parisiens de la chaîne française TV5 Monde, où des traces d'un groupe de pirates travaillant pour le Kremlin ont ensuite été découvertes...

Un autre cap est franchi deux jours avant Noël de la même année, dans l'ouest de l'Ukraine. Les techniciens d'une compagnie régionale de distribution d'électricité voient sur leur écran des hackeurs prendre le contrôle de plusieurs coupe-circuits dans un transformateur. En trois clics, des dizaines de milliers de foyers sont plongés dans le noir. Le même procédé se répète dans deux autres firmes. Pour Oleh Derevianko, le PDG d'ISSP, qui a passé ces dernières années sur la « ligne de front » de cette cyberguerre, il s'agit d'une date charnière. C'est la première fois, explique-t-il au *Monde*, qu'une attaque purement informatique a causé des dégâts physiques.

L'année suivante, à la même période et dans le même froid hivernal, des pirates répètent l'opération. Pendant une demi-heure, des parties entières de Kiev se retrouvent privées d'électricité. Les dégâts sont limités, mais les experts sont formels : les assaillants ont mis au point une véritable arme, capable de « parler » aux systèmes industriels et d'être réutilisée contre n'importe quelle usine, n'importe où dans le monde.

En Ukraine, les attaques surviennent souvent par vagues. Peu avant la deuxième menée contre le réseau électrique, en décembre 2016, les pirates décident de viser cette fois l'Etat. Leur cible : des ministères. *« Tous les ordinateurs du ministère des finances ont été détruits. Cela aurait pu être catastrophique »*, explique Dmytro Shimkiv, ex-conseiller du président Petro Porochenko sur les questions de cybersécurité. *« Il y avait*

un risque que les fonctionnaires ne reçoivent pas leur salaire, que les retraités ne touchent pas leur pension », renchérit M. Derevianko.

MUSCLER LES PROTECTIONS

Dans l'arsenal russe de la guerre hybride, les agressions numériques côtoient la propagande et poursuivent le même but. *« C'est le plus court chemin vers le cerveau de l'électeur »*, résume Konstantin Korsun, ancien agent du SBU et spécialiste de sécurité informatique. *« La Russie doit prouver deux choses à la population ukrainienne et au reste du monde : que l'Ukraine est un pays divisé et que son Etat est en faillite »*, résume le diplomate ukrainien Dmytro Kuleba, chargé de la communication de son pays au pire de la crise avec Moscou. *« Le principal but est de déstabiliser. Lors de chaque cyberoffensive sont lancées des opérations informationnelles destinées à montrer que les autorités sont incapables de gérer le pays »*, confirme Oleksandr Klymchuk, l'officier du SBU. Les assauts contre l'Ukraine permettent aussi aux Russes d'envoyer un message au monde entier sur leurs capacités informatiques, surtout lorsqu'il est question de réseaux électriques ou de destruction pure et simple de systèmes informatiques.

Après quatre années marquées par une succession rapide d'attaques, 2018 a été plus calme. Cela peut s'expliquer par les mesures prises par l'Ukraine et ses alliés. Kiev a adopté une loi censée mieux organiser sa défense dans ce domaine. Les Etats-Unis ont dépêché une escouade de spécialistes pour comprendre les offensives contre le réseau électrique, et plusieurs organisations internationales, dont l'Organisation pour la sécurité et la coopération en Europe et l'OTAN, collaborent avec l'Ukraine pour muscler ses protections.

Du chemin a été parcouru mais, de l'avis de tous les spécialistes, ce pays continue de prêter le flanc aux attaques. Ainsi, en 2018, un logiciel malveillant y a été repéré à temps. Selon ses découvreurs, il aurait pu *« couper l'accès à Internet de centaines de milliers de personnes »*. Les autorités locales et plusieurs experts ont également affirmé au *Monde* avoir récemment désamorcé d'autres attaques d'ampleur. Une menace sur les réseaux électriques, attribuée à un groupe de pirate surnommé GreyEnergy, a notamment été déjouée. *« Il y a beaucoup d'infrastructures critiques* [réseaux d'eau, de gaz, d'électricité...] *où la sécurité n'est pas optimale et où de nombreux scénarios sont possibles »*, pronostique Oleg Bondarenko, pilier de l'industrie de la cybersécurité en Ukraine et directeur de recherche pour l'entreprise américaine FireEye. Dmytro Shimkiv, l'ex-conseiller de M. Porochenko, confirme ces craintes : *« Ce qui m'inquiète, c'est la sécurité des infrastructures critiques. La tempête approche. »* ■

MARTIN UNTERSINGER

Prochain article : *l'Estonie, une république sous influence*

« EN UKRAINE, LA RUSSIE TESTE DES CONCEPTS, DES CAPACITÉS. C'EST L'ENDROIT PARFAIT POUR COMPRENDRE COMMENT OPÈRENT LES RUSSES »

SIIM ALATALY
centre de recherche de l'OTAN sur la cyberdéfense