ques, ’amateurisme

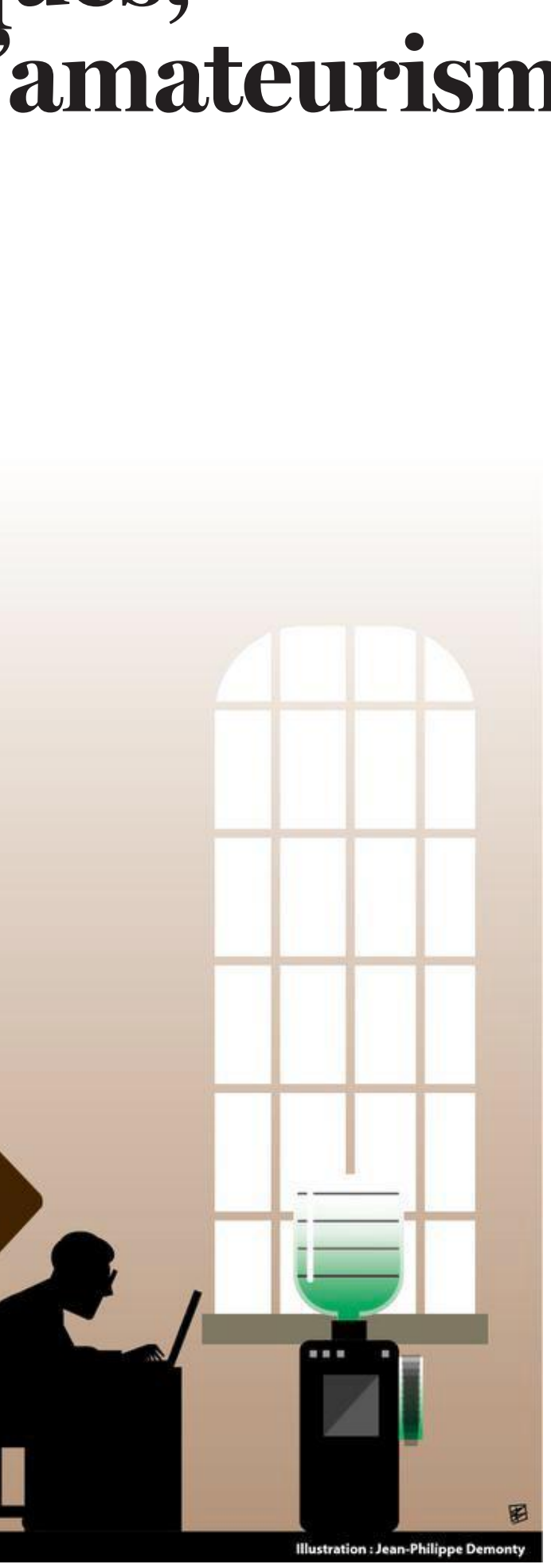
Illustration : Jean-Philippe Demonty

Lexique du flibustier

Phishing Contraction de *fishing* (pêcher) et de *phreaking* (piratage téléphonique), le terme désigne le fait de tenter de récupérer des identifiants et mots de passe afin d’accéder à un système. Dans la majorité des cas, ce sont les coordonnées bancaires qui sont visées, mais la pratique peut aussi servir à usurper l’identité d’un internaute. Il s’agit souvent de mails frauduleux poussant la personne qui les reçoit à divulguer des informations sensibles.
Malware Il s’agit d’un programme malveillant installé sur un ordinateur ou un objet connecté. Soit le logiciel récolte des données sensibles, soit il compromet la sécurité de la machine sur laquelle il est installé. Un *malware* peut, par exemple, permettre aux pirates d’accéder à l’ensemble du réseau auquel la machine est connectée. Il peut également diffuser de la publicité non autorisée.
Ransomware Le *ransomware* est une forme de *malware* qui s’attaque particulièrement aux données contenues sur la machine. Il bloque l’accès à l’appareil et, souvent, vole et crypte les données. Pour retrouver l’accès à l’ensemble de sa machine, la victime est invitée à effectuer un paiement. Sans quoi les données sont détruites ou, le plus souvent, revendues sur le dark web.
Dark web Le dark web est une portion d’internet à laquelle on ne peut pas accéder avec un navigateur internet standard comme Chrome ou Firefox. Cette difficulté d’accès offre une discrétion appréciée par les groupes criminels et permet au dark web de s’imposer comme le lieu privilégié d’échange de biens et de services prohibés.
Attaque DDoS Acronyme anglophone d’« attaque par déni de service ». Le principe est simple : bombarder un serveur afin de le surcharger en demandes inutiles. En le saturant ainsi, le système, qui ne dispose plus d’assez de mémoire, de force de calcul ou même de bande passante, finit par être mis hors service. Pour un site de vente en ligne ou une ligne de production, l’impact commercial peut être énorme, ainsi que l’impact sur l’image de l’entreprise.
Faille zero-day Une faille *zero-day* est une faille de sécurité informatique dont le développeur du logiciel n’a pas connaissance. Cette faille peut donc prendre un certain temps avant d’être colmatée et permet aux pirates de l’exploiter incognito. TH.CA

l’expert « La cybercriminalité est le plus souvent évanescente et agile »

Pas simple pour les autorités belges d’interpeller un groupe russe qui lance une attaque sur une entreprise belge depuis des machines chinoises et retire l’argent de la rançon en Lituanie

TH. CA

Michaël Dantinne donne les cours de criminalité organisée et de crime et nouvelles technologies à l’ULiège. Pour lui, les deux univers partagent des points communs, mais leurs modèles d’organisation diffèrent.

Le modèle de fonctionnement des cybercriminels est-il comparable à celui du crime organisé ?
Ils me semblent assez différents. Il est assez rare de trouver des groupes qui gèrent tout de A à Z, depuis la création du *malware* jusqu’à l’encaissement et le blanchiment des cryptomonnaies versées par les victimes. La chaîne demande énormément de profils très spécialisés. On retrouve donc énormément de cybercriminels sur les forums du *dark web* qui offrent leurs services comme free-lances. Il y a ceux qui mettent à disposition leur capacité à blanchir l’argent, d’autres qui sont spécialisés dans la négociation ; certains ne font que livrer le virus. Les profils sont extrêmement diversifiés.
Par ailleurs, il y a rarement de composante ethnique ou culturelle comme dans les mafias, qui travaillent généralement en famille avec un lien de confiance très fort. Cette confiance est moins présente dans les groupes cybercriminels.

On est donc face à un écosystème de prestataires de services ?
Oui, complètement. L’actualité nous donne un exemple symptomatique de cette structuration : il y a quelques semaines, un jeune homme de 20 ans a été interpellé dans le Namurois après une enquête menée par le FBI et les enquêteurs de la Computer Crime Unit. Il est soupçonné d’avoir mis à disposition de ses clients un service d’attaques DDoS clé sur porte. Il proposait donc de faire planter des sites et des infrastructures en ligne. Le monde des cybercriminels est composé d’une myriade de profils comme celui-ci : très spécialisés et qui opèrent comme des petits indépendants en vendant les attaques comme un service.

Un contre-exemple de la difficulté qu’éprouvent les autorités à appréhender les pirates…
Effectivement, ces structures sont le plus souvent évanescentes et agiles. Elles se font et se défont selon les missions. Cela a l’avantage, par rapport au crime organisé traditionnel, d’être beaucoup plus difficile à détecter par les autorités. Plus les pirates disposent de technologies avancées, plus ils peuvent mettre de la distance entre eux et leurs victimes. Bien souvent, les différents opérateurs sont, en plus, répartis sur l’ensemble du globe. Le lien entre les membres est donc moins fort que dans le crime organisé traditionnel, mais ils sont aussi bien plus insaisissables. Pas simple pour les autorités belges d’interpeller un groupe russe qui lance une attaque sur une entreprise belge depuis des machines chinoises et retire l’argent de la rançon en Lituanie. Une structure pyramidale, fixe, est plus simple à identifier et il est plus facile d’appréhender ses membres. En outre, il est très difficile d’évaluer l’ampleur du phénomène, bien qu’il semble être en forte augmentation. Car la plupart des entreprises touchées préfèrent ne pas ébruiter l’attaque dont elles ont été victimes. Et les criminels restent, bien entendu, les plus discrets possible.

erguérilleros contre la Russie ?

sont connus, mais ne sont pas inquiétés. »

Pire, ils sont, avec d’autres, plus actifs que jamais. Et les attaques contre l’Ukraine ne cessent de se poursuivre : « Nous avons observé trois fois plus d’attaques sur les réseaux ukrainiens qu’à la même époque l’an dernier », analyse Hyppönen. « Pourtant, les infrastructures tiennent, le pays dispose toujours d’électricité, de connexion à internet, etc. Si le pays tient bon aussi héroïquement, c’est grâce à son entraînement. Cela fait quelques années que l’Ukraine se défend contre les attaques. En 2017, NotPetya, un *ransomware* particulièrement virulent, a frappé le pays et son économie de plein fouet avant de se répandre dans le monde entier. Aujourd’hui, il devient évident que NotPetya n’était pas un simple *ransomware* destiné à extorquer ses victimes, mais une arme mise au point par la Russie pour paralyser le pays. Un coup de semonce, voire, déjà, un acte de guerre. »

L’expert estime en outre que, traditionnellement, de nombreuses attaques sont planifiées depuis l’Ukraine, mais que ces dernières ont drastiquement chuté depuis le début de l’invasion militaire russe : « De nombreux pirates mènent sans doute une cyberguérilla sans merci à la Russie et participent activement à la défense des infrastructures en ligne de leur pays. Cela explique qu’ils soient moins actifs dans leurs activités habituelles. »

Les experts ne sont pas unanimes
Le professeur Axel Legay est circonspect face à cette analyse : « Tout d’abord, il convient de rappeler que les plus belles attaques sont celles qui ne se voient pas. Ce n’est pas parce que l’on détecte moins d’attaques qu’elles sont effectivement moins nombreuses. Ensuite, il ne faut pas oublier que la morale des hackers est à géométrie variable. Beaucoup se considèrent comme des mercenaires et se vendent aux plus offrants. Ils ne s’embarrassent pas de considérations géopolitiques. Certains se sont donc ralliés à la Russie sans se poser trop de questions tandis que d’autres se sont sans doute déplacés et poursuivent leurs attaques vers le reste du monde depuis d’autres pays. Enfin, si des attaques sont parties d’Ukraine ces derniers mois, il se pourrait que l’on ne s’en rende compte que dans plusieurs années. Si l’Ukraine résiste tant bien que mal, c’est, d’une part, parce qu’elle se prépare à ce genre d’attaques depuis des années et, d’autre part, parce qu’elle profite d’une très grosse aide américaine : de la part du gouvernement, mais aussi d’entreprises comme Google ou Microsoft qui avertissent les autorités dès qu’ils détectent une tentative d’intrusion. »

Les pirates informatiques sont plus actifs que jamais. Et les attaques contre l’Ukraine ne cessent de se poursuivre

Le professeur Laurent Mathy émet lui aussi quelques doutes quant à cette thèse des pirates défenseurs : « Une des spécificités de la criminalité en ligne est qu’il est très difficile de déterminer son origine. La plupart des attaques proviennent de *bots* (un agent logiciel automatique ou semi-automatique qui interagit avec des serveurs informatiques – NDLR) disséminés sur l’ensemble de la planète. Impossible donc de dire aujourd’hui si des attaques sont menées depuis l’Ukraine ou non. C’est aussi la raison pour laquelle il est très ardu de lier des attaques avec les autorités d’un Etat qui, sachant que l’on ne pourra pas remonter jusqu’à eux, ne se privent pas d’attaquer pour déstabiliser d’autres pays ou, simplement, s’entraîner. »