L'impact économique de la cyber-criminalité : pas de ralentissement en vue

La cybercriminalité coûte désormais au monde entier près de 600 milliards de dollars, soit 0,8 % du PNB mondial, selon le nouveau rapport publié par le Center for Strategic and International Studies (CSIS) et McAfee, ***The Economic Impact of Cybercrime: No Slowing Down*** (L'impact économique de la cybercriminalité : pas de ralentissement en vue). Prévu pour le 21 février, il propose une analyse actualisée par rapport à l'édition 2014, qui évaluait les pertes mondiales à près de 500 milliards, ou 0,7 % du produit mondial.

Replaçons cette statistique en contexte : elle représente un montant supérieur au revenu de la plupart des pays, à quelques exceptions près. En outre, si l'on considère son coût par rapport à l'économie Internet mondiale (4,2 mille milliards en 2016), la cybercriminalité peut être considérée comme une taxe sur la croissance de 14 %[1].

La cybercriminalité est le troisième plus grand fléau économique[2] dans le monde, derrière la corruption dans le secteur public et le trafic de stupéfiants. En voici les raisons :

- **Elle touche tout le monde :** Près de deux tiers des personnes qui utilisent des services en ligne (plus de deux milliards d'individus) ont été victimes d'un vol ou d'une compromission de leurs données.
- **Des risques faibles pour des gains élevés :** La probabilité d'arrestation ou d'incarcération est faible. Aucun des auteurs des violations de données les plus médiatisées n'a été poursuivi en justice. Les forces de l'ordre redoublent d'efforts, mais de nombreux cybercriminels opèrent en dehors de leur juridiction.

Le rapport attribue la croissance des crimes informatiques (100 milliards de dollars) à l'adoption rapide de nouvelles technologies, à l'accès aisé aux filières cybercriminelles (notamment aux centres cybercriminels en expansion) et à la sophistication financière croissante des pirates informatiques de haut vol.

Si l'on considère son coût par rapport à l'économie Internet mondiale (4,2 mille milliards en 2016), la cybercriminalité peut être considérée comme une taxe sur la croissance de 14 %[1].

Gardez le contact

Principales observations

- Le ransomware, ou logiciel de demande de rançon, est l'outil qui connaît la croissance la plus rapide. Internet abrite en effet plus de 6 000 places de marché criminelles proposant des services et produits de ransomware. De plus, le Ransomware-as-a-Service connaît une popularité croissante.
- La cybercriminalité sous forme de service gagne en sophistication, avec des marchés florissants offrant un large choix d'outils et de services — notamment des kits d'exploit, des logiciels malveillants personnalisés et des locations de botnets.
- Pour échapper aux autorités, la plupart des transactions de la communauté cybercriminelle se passent sur le Dark Web, où l'anonymat et les cryptomonnaies (p. ex. le réseau Tor et le bitcoin) empêchent l'identification des pirates.
- Parmi les logiciels malveillants les plus populaires mis en vente sur le Web clandestin, l'on trouve des injections de code HTML, des kits d'exploits et des services IaaS (Infrastructure-as-a-Service), notamment l'hébergement hypersécurisé et les locations de botnets.
- Le vol de capital intellectuel représente au moins un quart du coût de la cybercriminalité, sans compter les risques pour la sécurité nationale lorsqu'il concerne des technologies militaires.

Activités cybercriminelles

Le rapport ne tente pas d'évaluer le coût de toutes les activités malveillantes sur Internet. Il se concentre plutôt sur l'accès illicite des criminels à l'ordinateur ou au réseau d'une victime. Parmi les activités cybercriminelles identifiées par les auteurs :

- Perte de capital intellectuel et d'informations métier confidentielles
- Délits financiers et fraudes en ligne, souvent rendus possibles par le vol préalable d'informations d'identification personnelle
- Manipulation financière visant des sociétés cotées en bourse
- Coûts d'opportunité, y compris les interruptions de service et de production, ou la perte de confiance dans les activités en ligne
- Coûts associés à la sécurisation des réseaux, à la souscription de cyberassurances et à la reprise des activités après une cyberattaque
- Risque d'atteinte à la réputation et de responsabilité civile pour la société touchée et sa marque

La menace la plus redoutable

Le ransomware n'épargne personne, ni les particuliers, ni les grandes entreprises. Une grande partie des victimes cèdent au chantage et paient la somme exigée.

La cybercriminalité est le troisième plus grand fléau économique[2] dans le monde, derrière la corruption dans le secteur public et le trafic de stupéfiants.

D'après le FBI, les rançons payées s'élèvent à 209 millions de dollars pour le premier trimestre 2016, contre 24 millions de dollars pour toute l'année 2015[3]. Plusieurs raisons expliquent la croissance fulgurante[4] du ransomware :

- Disponibilité des kits de ransomware sur le Web clandestin : plus de 6 000 places de marché criminelles en ligne offrent près de 45 000 produits et services différents
- Plates-formes RaaS (Ransomware-as-a-Service) qui offrent aux auteurs de ransomware la possibilité d'étendre leurs activités en vendant leur code à la communauté criminelle et en touchant une part des rançons perçues
- Vers de ransomware, comme WannaCry, capables de se propager à tout le réseau et de bloquer un grand nombre d'ordinateurs

Parmi les autres tendances attendues des ransomwares, citons les fonctionnalités d'exfiltration des données et les attaques contre les équipements mobiles et l'Internet de objets (IoT), dont la sécurité laisse souvent à désirer.

La cybercriminalité dans le monde

Le rapport se penche sur la cybercriminalité en Amérique du Nord, en Europe, en Asie centrale, en Asie du Sud-Est et dans la région Pacifique, en Amérique latine et dans les Caraïbes, en Afrique sub-saharienne, en Afrique du Nord et au Moyen-Orient. Les résultats du rapport suggèrent que le coût de la cybercriminalité varie selon les régions et le niveau de cybersécurité de chaque pays. Ce dernier est mesuré à l'aide des principaux indicateurs suivants : mesures légales, techniques et organisationnelles, développement de moyens d'action et coopération.

Les résultats sont classés comme suit : les pays de haut niveau avec une économie numérique et une cybersécurité évoluées ; les pays de niveau intermédiaire dont l'économie numérique et la cybersécurité sont en cours de développement ; et enfin ceux dont l'économie numérique et la cybersécurité sont encore au stade embryonnaire. Comme l'on peut s'y attendre, les États plus riches subissent des pertes plus élevées. Les plus touchés sont les pays de niveau intermédiaire.

- **Allemagne :** Le pays héberge l'économie Internet souterraine la plus sophistiquée de l'Union européenne.
- **Brésil :** Il représente la deuxième source majeure de cyberattaques et la troisième cible la plus touchée.
- **Émirats arabes unis :** Il s'agit du deuxième pays le plus ciblé et dont le coût de la cybercriminalité est estimé à 1,4 milliard de dollars par an.
- **Japon :** Jusqu'il y a peu protégé contre la cybercriminalité par la barrière linguistique et l'absence d'infrastructure pour le blanchiment d'argent, le Japon a connu une augmentation des attaques, surtout celles lancées contre les banques.
- **Royaume-Uni :** Les fraudes en ligne et la cybercriminalité représentent près de la moitié de l'ensemble des activités criminelles, avec plus de 5,5 millions de délits chaque année.

Le rapport attribue la croissance des crimes informatiques (100 milliards de dollars) à l'adoption rapide de nouvelles technologies, à l'accès aisé aux filières cybercriminelles et à la sophistication financière croissante des pirates informatiques de haut vol.

Conclusion et recommandations

Si l'analyse réalisée par le CSIS et McAfee se concentre sur les coûts de la cybercriminalité, les entreprises et les États peuvent prendre plusieurs mesures pour réduire leurs pertes :

- Implémentation systématique de mesures de sécurité essentielles, p. ex. la mise à jour régulière des logiciels de sécurité, l'application de correctifs, le choix d'architectures de sécurité ouvertes ainsi que des investissements dans des systèmes de défense avancés couvrant l'ensemble de l'infrastructure, des terminaux au cloud
- Coopération internationale accrue des forces de l'ordre nationales et du secteur privé, et investissement dans des ressources d'investigation, surtout dans les pays en développement
- Modernisation des processus actuels, par exemple le traité d'entraide judiciaire (TEJ) qui permet aux gouvernements de solliciter l'aide d'autres États dans les enquêtes cybercriminelles et la collecte de preuves
- Processus optimisé pour la collecte de données agrégées par les autorités nationales
- Normalisation des informations sur les menaces et coordination des exigences de cybersécurité pour améliorer la sécurité dans des secteurs critiques comme la finance
- Adoption accélérée de traités comme la Convention de Budapest qui définit les responsabilités des États en matière de coopération et d'application des lois sur la cybercriminalité
- Imposition de sanctions temporaires ou d'autres mesures à l'encontre des gouvernements qui ne luttent pas comme il se doit contre la cybercriminalité

À propos de McAfee

McAfee est l'une des plus grandes entreprises de cybersécurité indépendantes au monde. Convaincue de l'efficacité de la collaboration, McAfee met au point des solutions pour entreprises et particuliers qui contribuent à un monde plus sûr. **www.mcafee.com/fr**

1. https://www.bcg.com/documents/file100409.pdf
2. www.imf.org/external/pubs/ft/sdn/2016/sdn1605.pdf
3. Max Metzger. « FBI says Ransomware soon becoming a billion dollar business » (D'après le FBI, le business des ransomwares va bientôt atteindre le miilliard de dollars). SC Media UK, 10 janvier 2017. https://www.scmagazineuk.com/fbi-says-ransomware-soon-becoming-a-billion-dollar-business/article/630615/
4. « McAfee Labs - Rapport sur le paysage des menaces », McAfee, décembre 2017

McAfee
Together is power.

11-13 Cours Valmy - La Défense 7
92800 Puteaux, France
+33 1 4762 5600
www.mcafee.com/fr