ONUDC
Office des Nations Unies contre la drogue et le crime

COVID-19 RIPOSTE

Vienne, le 14 Avril 2020

CYBERCRIMINALITÉ ET COVID19 : Risques et Réponses

PRINCIPALES EVALUATIONS

- **La cybercriminalité évolue et est en pleine expansion dans le contexte de lala pandémie du COVID19.** La fraude en ligne, l'extorsion de fonds et les abus sexuels d'enfants en ligne ciblent des individus, alors que les rançongiciels, compromettent essentiellement les systèmes, y compris ceux des hôpitaux. Alors que Les gouvernements continuent d'être la cible de logiciels malveillants, la propagation croissante de la désinformation et des informations erronées continuera à semer la confusion dans l'esprit du public et à saper la réponse scientifique.
- **Le télétravail a augmenté le nombre de victimes potentielles de la cybercriminalité. Les personnes prennent de plus grands risques en ligne à la maison, exposant ainsi par inadvertance le système informatique des entreprises aux cybercriminels.** Le hameçonnage continue de permettre aux criminels et aux autres spécialistes, un accès malveillant à des systèmes critiques.
- **Le nombre d'agents des forces de l'ordre spécialisés dans la lutte contre la cybercriminalité sera réduit pendant la majeure partie de l'année 2020. La cybercriminalité augmentera à court terme, et les victimes seront probablement confrontées à des retards dans l'obtention de la justice.** Les cybercriminels exploiteront les lacunes opérationnelles visibles. Contre toute attente, cela créera des opportunités tactiques et stratégiques en matière d'application de la loi.
-

Contexte

1 . Ce briefing donne un bref aperçu des menaces de cybercriminalité dans le contexte de la pandémie de COVID19. Il a été élaboré à partir de comptes rendus confidentiels obtenus des services d'application de la loi de l'ONUDC, de partenaires des gouvernements, des ONG, des universités, des médias, des sources publiques et du secteur privé dans le monde entier, au début du mois d'avril 2020. Des recommandations sont formulées à la fin de chaque section thématique.

Tableau de la Menace : évolution, accroissement et exploitation

2. Des mesures globales de distanciation sociale sont maintenant en place dans le monde entier. Cela a mené à une augmentation significative de l'utilisation des technologies de communication en ligne par les autorités publiques, les entreprises comme les particuliers. Nombreux sont ceux qui ne sont pas familiers avec l'utilisation des technologies en ligne à ce stade. Cela offre aux cybercriminels la possibilité d'exploiter un vaste réseau de cibles attrayantes et vulnérables. Si l'on ajoute à cela

l'enseignement et le travail à distance, il existe davantage d'utilisateurs de l'Internet, qui sont moins bien informés des menaces et sont susceptibles de prendre plus de risques en ligne à la maison, qu'au travail ou à l'école.

3. Les cybercriminels ont fait évoluer leur criminalité de sorte à exploiter les nuances sociales, juridiques et psychologiques associées au COVID19. Les délinquants sexuels en ligne ciblent de manière proactive les enfants confinés qu'ils soient de nouveaux utilisateurs d'internet ou plus habitués. en. Il s'agit notamment des délinquants qui cherchent à préparer[1] et à extorquer des faveurs sexuelles d'enfants pris individuellement[2], jusqu'à une infiltration plus large dans les cours en ligne[3] désormais appelée « Zoom-bombing ».

4. Les cybercriminels exploitent de plus en plus la peur liée au virus COVID19 : ils proposent de faux remèdes à la vente sur Internet et fraudent en vendant des désinfectants pour les mains et des équipements de protection individuelle (EPI), des médicaments ou des produits d'hygiène inexistants. Les autres fraudes comprennent l'offre de services tels que des conseils en investissement douteux (y compris dans les crypto-monnaies) et des conseils et diagnostics médicaux erronés. Un important site de pornographie en ligne a proposé un abonnement gratuit aux utilisateurs d'un pays, augmentant ainsi les risques de téléchargement de logiciels malveillants et de sextorsion.

5. Les personnes âgées, qui sont souvent moins sensibilisées aux risques en ligne, sont particulièrement ciblées par les cybercriminels pour télécharger, faire suivre des liens infectés par des rançongiciels à travers des spams sur le COVID19 et diffuser des informations erronées à leurs amis et à leur famille. Les cybercriminels continuent de chercher à extorquer leurs victimes en prétendant connaître – et révéler - l'utilisation présumée de la pornographie en ligne par la victime.

6. Le Business Email Compromise[4] (comptes de courrier électronique compromis par le hameçonnage qui se font passer pour un haut fonctionnaire de l'organisation cible) continue de recourir à l'ingénierie sociale, renforcée par l'urgence accrue de la pandémie, pour encourager le mouvement de fonds vers une banque criminelle, un compte en devises ou un compte en crypto-monnaies, ou est utilisé pour obtenir des données sensibles à des fins malveillantes, y compris l'espionnage.

7. Les forums Darknet continuent de vendre des données compromises – y compris celles de hauts responsables et de célébrités. Les criminels qui sont nouveaux dans la « cybercriminalité » recherchent des conseils auprès d'autres criminels sur la meilleure façon d'exploiter la pandémie COVID19 à des fins lucratives. Certains cybercriminels ont cherché à dissuader d'autres cybercriminels de cibler les hôpitaux et les laboratoires de test de vaccins par des attaques par Déni de Service Distribué (DDoS) et par des *rançongiciels*. Les pédophiles prédateurs continuent à discuter pour savoir quels sites de réseaux sociaux et de partage de photos sont susceptibles de leur donner plus facilement accès à des enfants à abuser. Les délinquants continuent également de discuter de la meilleure façon d'identifier et échapper aux agents de police infiltrés en ligne.

8. En plus des cybercriminels traditionnels, des groupes de Menace Persistante Avancée (*Advanced Persistent Threat (APT)* continuent d'évoluer et d'exploiter la pandémie. Les APT continuent de cibler les infrastructures critiques nationales, notamment les hôpitaux et les laboratoires de développement de vaccins, par des attaques par logiciels malveillants, par des rançongiciels et par DDoS. La motivation de ces attaques n'est pas simplement basée sur le profit, car les logiciels malveillants donnent souvent accès à des identifiants de connexion et à d'autres informations sensibles ayant une valeur de renseignement.

9. Le succès d'une grande partie de la cybercriminalité liée au COVID19 repose sur les attaques de hameçonnage par courrier électronique comme vecteur initial d'infection. Lorsqu'une personne clique sur un lien ou un document, le compte est compromis. La compromission peut être visible pour la victime mais, le plus souvent, elle est dissimulée et permet au criminel d'établir et de maintenir un accès à long terme au compte, à l'organisation et aux système informatique qui y sont relatifs. Outre la collecte d'informations sensibles, l'acteur APT peut altérer des sites web, modifier le détail de

[1] https://www.esafety.gov.au/parents/big-issues/unwanted-contact

[2] https://www.esafety.gov.au/key-issues/image-based-abuse/take-action/deal-with-sextortion

[3] https://tcrn.ch/3buz3gW

[4] https://www.trendmicro.com/vinfo/us/security/definition/business-email-compromise-(bec)

documents, supprimer des données et diffuser des informations erronées.

10. **L'ONUDC recommande aux gouvernements et au secteur privé de multiplier des campagnes de sensibilisation du public qui soient culturellement adaptées et faciles à comprendre. Les hotlines (numéros d'urgence) de signalement anonyme d'abus sexuels d'enfants en ligne sont une facette essentielle de la réponse. Nous recommandons également de continuer à appliquer rigoureusement les mises à jour de sécurité et de faire régulièrement la sauvegardes des informations.**

Réduction de la capacité d'application de la loi et de résilience de la société

11. Dans de nombreux pays, le personnel de police spécialisé dans la lutte contre la cybercriminalité a été détourné des enquêtes sur les infractions de cybercriminalité pour soutenir les mesures gouvernementales contre l'épidémie de COVID19 telles que la mise en quarantaine. Des fonctionnaires spécialistes sont également tombés malades. Les capacités devraient encore se réduire dans les semaines à venir, réduisant ainsi la capacité des États à faire face aux nouvelles menaces croissantes de la cybercriminalité.

12. Dans plusieurs pays, les procédures d'enquête et les procédures judiciaires sont perturbées par la nécessité de mener ces activités en personne, ce qui n'est pas possible en raison des mesures de santé publique locales. D'autres pays ont rapidement adoptés des procédures judiciaires en ligne.

13. La désinformation et les informations erronées concernant le virus continuent de se propager, essentiellement par le biais des réseaux sociaux et des services de messagerie cryptés. Les entreprises promotrices des réseaux sociaux, également confrontées au travail à distance, luttent pour faire face à la quantité d'informations erronées, à la manière d'appliquer systématiquement les politiques internes et à l'impact de la législation locale.

14. La désinformation et les attaques contre les Infrastructures critiques nationales sapent la confiance du public et réduisent l'efficacité des mesures de sécurité publique.

15. **L'ONUDC recommande que les procédures judiciaires se poursuivent en ligne lorsque cela est possible, tout en veillant à ce que les normes et standards internationaux, le respect de la légalité et la primauté du droit soient maintenus.**

16. **Nous recommandons également que les entreprises promotrices des médias sociaux déploient davantage d'efforts pour contrer la propagation de l'« infodémie » COVID19, tout en protégeant la liberté d'expression. La science basée sur des faits doit être au cœur de la réponse au COVID19 – nous avons tous un rôle crucial à jouer à cet égard.**

Analyse

a. *La pandémie de COVID19 pose un défi mondial sans précédent à l'ensemble de la société. Nombreux sont ceux qui ont transféré leurs activités physiques vers des opérations en ligne, tout comme les criminels. La cybercriminalité devenant de plus en plus complexe et les victimes de plus en plus nombreuses, les forces de l'ordre de certains pays sont orientées vers d'autres fonctions. L'impact économique de COVID19 ajoute une couche de complexité supplémentaire pour le public et pour le gouvernement. Une tempête parfaite de cybercriminalité potentielle se déclare.*

b. *Si la crise de COVID19 et les menaces de cybercriminalité liées à cette crise sont mondiales, les réponses doivent également l'être : la lutte contre la cybercriminalité dans une juridiction donnée réduit les risques partout dans le monde. Des informations sur de nouvelles menaces et de nouveaux types de criminalité comme l'analyse COVID19 d'Europol (Europol's COVID19 analysis) et l Évaluation de la Cyber menace par INTERPOL (INTERPOL's Cyber Threat Assessment) doivent continuer à être partagées au niveau international sans délai.* Les *hotlines (numéros d'urgence) pour le signalement des abus sexuels d'enfants en ligne sont un outil essentiel pour permettre au public de contrer la menace.*

c. *Compte tenu de la pression probable sur les forces de l'ordre, proactives comme réactives, nous estimons que la capacité à enquêter activement sur la cybercriminalité sera mise à l'épreuve à court terme – en particulier dans les pays dont les ressources étaient limitées avant la pandémie. Les*

cybercriminels, y compris les groupes APT, continueront à exploiter cette situation. Il convient de renforcer la communication au public des arrestations réussies ou des perturbations au sein des cybercriminels qui ont cherché à exploiter la crise actuelle. Des opérations ayant un grand impact, comme le récent démantèlement, par les Pays-Bas, de quinze opérateurs de DDoS en une semaine[5], contribuent à montrer l'impact visible et à rappeler aux cybercriminels que les opérations se poursuivent partout dans le monde. Les opérations proactives d'infiltration en ligne contre les acteurs à haut risque de la cybercriminalité doivent se poursuivre. Contre toutes attentes, les cybercriminels peuvent prendre plus de risques en ligne car ils ont l'impression que la probabilité de détection a été réduite. Les enquêtes des services répressifs spécialisés doivent donc se poursuivre au même rythme.

d. *La diplomatie publique et la sensibilisation sont essentielles à la prévention et doivent renforcer l'autonomie des groupes vulnérables, en particulier les enfants et les personnes âgées. Les mesures contre la désinformation et les informations erronées doivent fournir des informations évaluées, crédibles et utiles : cela doit être fait de manière transparente et responsable.*

e. *Toutes les mesures adoptées pour lutter contre la cybercriminalité doivent continuer à être proportionnées, légales, responsables et nécessaires. La technologie est utilisée par de nombreux gouvernements pour évaluer, identifier et localiser les patients potentiels de COVID19. Ce travail essentiel doit rester à l'étude, avec une supervision claire, pour veiller à ce que les mesures de surveillance soient retirées une fois l'objectif de contrôle de l'épidémie atteint. Il est maintenant temps de renforcer la cyber-confiance du public et de travailler ensemble pour faire face aux menaces les plus pressantes de notre époque de renforcer la confiance au niveau international.*

f. *Ce n'est pas le moment de désinvestir dans des services spécialisés dans la lutte contre la cybercriminalité. La capacité et les moyens de lutte contre la cybercriminalité sont des éléments essentiels pour protéger les infrastructures critiques nationales, assurer la sécurité des enfants en ligne, donner des moyens d'action à l'industrie, sécuriser les hôpitaux et soutenir la relance économique après le COVID19.*

g. *Le personnel de l'ONUDC spécialisé dans la lutte contre la cybercriminalité est disponible, 24 heures sur 24, 7 jours sur 7, partout dans le monde, pour assister les États membres dans la lutte contre la cybercriminalité. Les ressources de diplomatie publique de l'ONUDC sont disponibles sur le site* https://www.unodc.org/unodc/en/covid-19.html *et comprennent des liens à une session Instagram Live avec l'Envoyé spécial du Secrétaire général pour la jeunesse, des conseils en matière de protection cybernétique pour (le personnel des Nations Unies) et l'évènement iSEEK Live sur le cyber de tout le Secrétariat des Nations Unies.*

Diffusion : ce rapport (UNODC/CMLS/COVID19/Cyber1) peut être partagé sans aucune référence préalable à l'auteur.

FIN

[5] https://www.zdnet.com/article/dutch-police-take-down-15-ddos-services-in-a-week/