ONUDC
Office des Nations Unies
contre la drogue et le crime

COVID-19
RIPOSTE

COVID-19: Analyse des cybermenaces

Office des Nations Unies contre la drogue et le crime du Moyen-Orient et de l'Afrique du Nord
Évaluation et actions

Un aperçu des tendances criminelles en ligne de la région MENA liées à la pandémie et comment prévenir et se protéger contre ces tentatives de tromper et de frauder les victimes.

Produit par le programme de Cybercriminalité du Bureau régional pour le Moyen-Orient et l'Afrique du Nord (ROMENA)

10 mai 2020

COVID-19: Analyse des cybermenaces

Introduction

Le 17 novembre 2019, cette date a marqué le début d'une longue route pour ce qui est maintenant connu comme la pandémie de COVID-19.[1] Nous ne pouvions guère soupçonner que nous nous lancerions dans une crise mondiale qui mettrait au défi tous les niveaux de la société et tous les secteurs industriels, commerciaux et résidentiels connus du monde. Cette pandémie des temps modernes a engendré de nouveaux défis auxquels nous nous attendons en temps de crise. Le tsunami de 2004 en Asie et le tremblement de terre de 2010 en Haïti sont des exemples clairs de la façon dont le comportement humain réagit à la crise qui a secoué le monde.[2]

Chaque fois qu'une nouvelle crise émerge, différents acteurs criminels sont les premiers à saisir l'occasion d'exploiter les victimes sans méfiance en période de peur, d'incertitude et de doute. Ces attaques prennent de multiples formes, du monde physique au monde numérique. L'histoire nous a appris que la méthode la plus efficace pour contrer initialement ces menaces est la prévention et la sensibilisation à tous les niveaux de la vie professionnelle et personnelle.

La pandémie présente à cet égard un défi de taille qui a rarement été observé par le passé; il est mondial et affecte tout le monde, indépendamment de leur lieu, race, origine ethnique, religion, origine sociale, sexe, handicap ou revenu, ou tout autre statut. Même si certains groupes sont plus à risque, ces cercles de risque pourraient s'étendre jusqu'à nos familles, nos amis et nos collègues. Compte tenu de ce contexte, les criminels sont prêts à tirer parti de ces craintes. Ce document se concentrera sur la prise en compte de l'aspect numérique de ces menaces et sur la manière d'éviter de tomber davantage dans la victimisation causée par cette pandémie.

Perspective de la menace numérique[3]

En une seule période de 24 heures, du 14 avril au 15 avril 2020:

170 387 courriels de spam contenaient « corona » ou « COVID » dans la ligne d'objet.

19 694 adresses IP uniques ont été utilisées pour envoyer ces e-mails.

8 391 domaines de messagerie uniques ont été utilisés pour envoyer ces e-mails.

583 de ces e-mails ont envoyé une pièce jointe infectée. Si on clique dessus, l'attaquant pourrait prendre le contrôle total de l'ordinateur de la victime.

Il s'agit d'une seule journée et d'une concentration sur un seul type de menace.
Il est désormais facile d'imaginer l'impact mondial de ce phénomène.

Table des matières

Introduction 1
Quelles sont les principales menaces? 3
Campagnes malveillantes 3
Emails d'hameçonnage 3
Domaines malveillants 5
Désinformation 6
Utilisation accrue des médias sociaux 8
Perspective régionale 11
Risques liés au cyberespace MENA 11
Infrastructure bancaire et gouvernementale 11
Les médias sociaux 11
Attaques sur les visioconférences 12
Campagnes d'hameçonnage 12
Réponse régionale de l'ONUDC 13
Plans futurs 14
Contributeurs 15
Matériel référencé 16

Quelles sont les principales menaces?

Ce rapport se concentrera sur les menaces largement utilisées qui affligent le monde numérique dans le cadre de cette crise ainsi que les nouveaux défis qui en découlent pour le cyberespace. Il est encore tôt pour déterminer l'efficacité de ces attaques, mais elles peuvent être dévastatrices. Néanmoins, nous devons garder à l'esprit que la plupart de ces attaques ciblent toute personne utilisant la technologie en ligne et exploiteront leurs émotions pour les victimiser. Voici un aperçu des différentes attaques qui sont observées quotidiennement et une brève explication de leurs mécanismes internes et de leurs objectifs.

Campagnes malveillantes

Emails d'hameçonnage

Le courrier électronique est, et continuera d'être, le principal vecteur de menace pour les particuliers et les organisations. Les cybercriminels utilisent depuis longtemps des événements majeurs et largement médiatisés dans des campagnes d'hameçonnage pour améliorer l'efficacité de leurs attaques, et la pandémie actuelle ne fait pas exception.

Plusieurs sites Web malveillants sur le Dark Web font la publicité de ensembles de messagerie d'hameçonnage COVID-19 en utilisant une pièce jointe infectée, déguisée en une carte de l'épidémie du virus à divers prix pouvant aller de 150 $ à 1000 $. Les cybercriminels qui achètent ces « ensembles » peuvent ensuite les utiliser pour lancer leurs campagnes de courrier électronique ciblant tout le monde, des particuliers aux grandes organisations. Ces infections sont rendues possibles par des systèmes d'exploitation non corrigés et la pièce jointe infectée exploitera les faiblesses de l'ordinateur sur lequel elle est visualisée.

Différents thèmes sont utilisés dans ces courriels pour améliorer le taux de clics de la campagne. Cela peut aller des rapports sur la pandémie aux conseils de santé provenant de sources gouvernementales officielles. Une fois cliqué sur, ces virus peuvent inclure divers dommages à un système qui peuvent aller de rançongiciel, enregistreurs de frappe et autres types de collecte d'informations personnelles.

Ils annonceront également la vente de masques faciaux ou d'autres produits liés à l'épidémie du virus Corona dans le but d'extraire un maximum d'informations du système informatique, qu'il a désormais infecté, ainsi que la possibilité de recueillir des informations de carte de crédit dans le cas où une victime sans méfiance achète de faux produits médicaux.

Les criminels envoient des vagues et des vagues de ces campagnes qui peuvent inclure plus de 150 000 à 175 000 courriels envoyés à la fois. Plusieurs campagnes sont observées quotidiennement. Le volume actuel de leurres de courrier électronique liés aux coronavirus représente de loin le plus grand nombre d'attaques que le cyberespace ait connues.

Le saviez-vous?

Les cybercriminels utilisent actuellement la vague Covid-19 pour créer et exploiter des problèmes d'infection. Mais ce phénomène n'est pas nouveau dans le cyberespace. Les cybercriminels utilisent depuis longtemps les faux résultats de tests de dépistage du VIH pour cibler les sociétés de soins de santé, d'assurance et pharmaceutiques à l'échelle mondiale.

PANDÉMIE DE VIH / SIDA (À SON POINT CRITIQUE, 2004-2012)
Nombre de morts: 32 millions
Cause: VIH / SIDA

Le VIH / sida s'est véritablement révélé être une pandémie mondiale, tuant plus de 32 millions de personnes depuis 1981. Entre 2004 et 2012, le nombre annuel de décès dus au VIH / sida dans le monde est passé de 1,7 million à 770 000.[4]

Les attaques en ligne liées au VIH / SIDA ont déjà été éclipsées par rapport au nombre de campagnes qui veulent exploiter la panique du Coronavirus.

Ces campagnes rappellent que les appâts liés à la santé n'ont pas commencé et ne s'arrêteront pas avec les dernières attaques sur le thème du coronavirus que nous assistons. Ils opèrent dans le cadre d'une stratégie cohérente, car les agresseurs percevraient l'utilité du facteur d'alarme lié à la santé. Souvent, les cybercriminels tentent de personnaliser les courriels envoyés dans le cadre de leur campagne afin de déclencher la curiosité du destinataire. Les informations personnelles indiquées dans le courriel peuvent avoir été obtenues d'une source publique ou d'actions illicites antérieures.

Si vous recevez l'un de ces courriels, ne l'ouvrez pas, surtout si vous ne vous attendez pas à ce que des résultats vous soient envoyés par mail. Au lieu de cela, contactez votre médecin ou professionnel de la santé directement pour discuter des résultats ou utilisez un rendez-vous de suivi pour tout test que vous pourriez avoir subi. Cela garantira que vous ne serez victime d'aucune cyber-campagne potentielle.

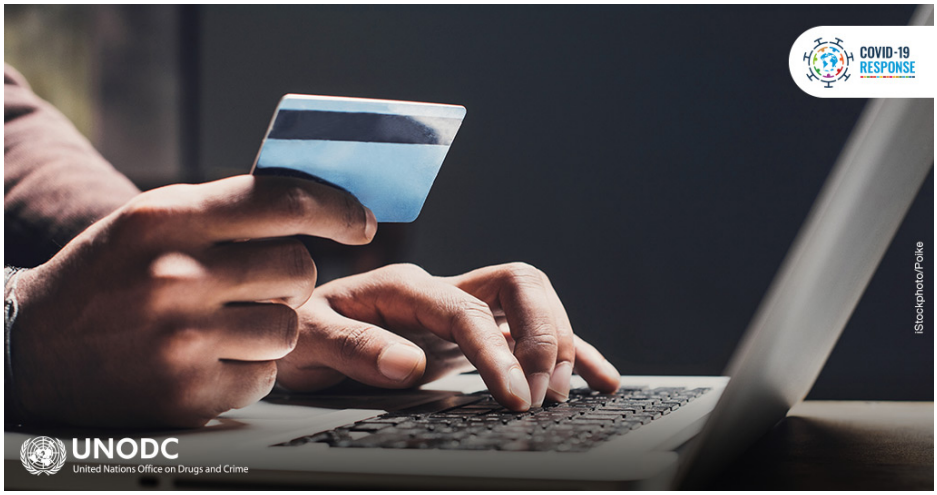
Domaines malveillants

De nouveaux sites Web sont en cours d'enregistrement pour diffuser des informations relatives à la pandémie. Cependant, beaucoup d'entre eux seront également des pièges pour les victimes sans méfiance. Au cours des six dernières semaines, des centaines de domaines liés à COVID-19 ont été enregistrés quotidiennement. Alors que certains d'entre eux sont authentiques et fournissent des informations précises sans mauvaises intentions, une grande partie d'entre eux sont de nature malveillante. Fin mars 2020, plus de 9 000 domaines étaient enregistrés avec le thème Corona Virus.

Ces sites Web malveillants disposent d'une grande variété d'attaques. Voici quelques-unes de ces attaques:

Usurper l'identité d'un site Web officiel

Le *National Cyber Security Center* (NCSC) au Royaume-Uni (UK) a rapporté que les cybercriminels se sont fait passer pour le *US Center for Disease Control* (CDC), créant des noms de domaine comme l'adresse Web du CDC pour demander des mots de passe et même des dons de bitcoins pour financer un faux vaccin.[5]

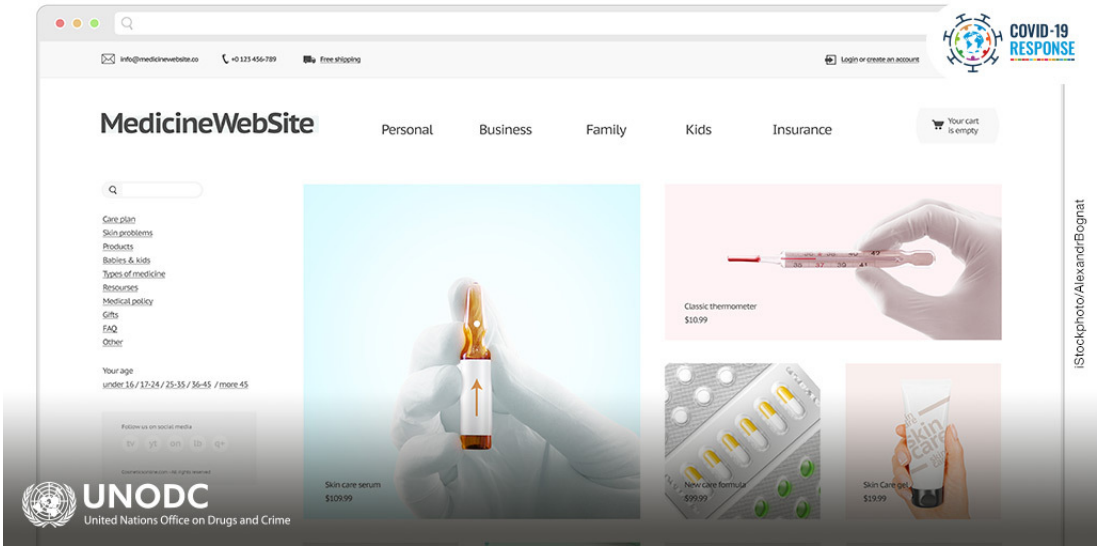


Diffusion de logiciels malveillants

Beaucoup de ces domaines créeront des pages Web chargées de divers malwares conçus pour exploiter les faiblesses de systèmes d'exploitation spécifiques. Ces malwares peuvent voler des informations d'identification de toute nature; numéros de carte de crédit, données bancaires, données sensibles du navigateur et exporter les informations acquises à des fins criminelles. Ce logiciel malveillant peut également collecter des portefeuilles de crypto-monnaie, prendre le contrôle non autorisé des webcams, collecter des informations sur l'appareil et installer un enregistreur de frappe qui enregistrera tout ce qui est tapé à l'aide du clavier du système infecté.

Fausses campagnes

Les sites Web feront également la publicité d'une multitude de services et de produits et demanderont souvent l'aide de la population en général pour ce faire. Par exemple, un site Web demandera aux utilisateurs de partager la puissance de calcul de leur ordinateur pour la consacrer à la recherche COVID-19, uniquement pour fournir en retour des logiciels malveillants volant des informations.[6] En termes simples, le don de puissance de calcul est le fait d'autoriser une autre personne / entité à utiliser la puissance de traitement de votre ordinateur ou appareil afin qu'elle puisse effectuer des calculs ou d'autres tâches à l'aide de votre matériel. Gardez à l'esprit que dans ce scénario spécifique, le don de puissance de calcul n'est qu'un prétexte pour garantir qu'ils voleront vos données.



Désinformation

Les concepts de fausses nouvelles ne sont pas nouveaux. De toute évidence, la situation actuelle a facilité la diffusion de ces informations sur toutes les plateformes sociales. Une très grande partie des utilisateurs d'Internet sont confinés à la maison et utilisent Internet à une capacité accrue, ce qui permet de publier, de republier et d'ajouter des informations erronées sur tous les médias.

Les techniques utilisées sont très complexes et peuvent prendre plusieurs formes. En fait, toutes les techniques discutées dans le présent document peuvent être combinées car elles sont toutes liées entre elles.

Par exemple, un employé d'une grande et importante organisation internationale reçoit un e-mail d'hameçonnage et la personne tombe dans le piège en cliquant sur le lien ou ouvre

le contenu joint. Cette action a déclenché le reste de la chaîne qui permettra à la cyber campagne de devenir beaucoup plus efficace. L'attaquant a désormais accès à une multitude de comptes appartenant à la victime sans méfiance. Le criminel peut utiliser ces comptes pour lancer de nouvelles attaques d'hameçonnage via courriel ou peut commencer à publier des informations sur les médias sociaux d'une personne respectée au sein de la communauté internationale. Cela ajoutera de la crédibilité aux fausses informations diffusées sur différentes plateformes. Ce n'est qu'un exemple simple qui pourrait devenir assez complexe et s'étendre bien au-delà des limites normales si l'attaquant est déterminé à atteindre ses objectifs.

Quels sont les objectifs de la désinformation?

Il existe de nombreuses définitions de ce concept. Généralement, l'intention est d'induire en erreur afin de nuire à une agence, une entité ou une personne et / ou d'obtenir un avantage financier ou politique. Il peut également être utilisé pour le sensationnalisme, la malhonnêteté ou les gros titres fabriqués pour augmenter le lectorat. À une époque où le nombre d'abonnés ou de lecteurs peut devenir une source de gain financier, nous pouvons facilement comprendre les raisons des efforts déployés pour la désinformation ces dernières années. En ce qui concerne cette pandémie spécifique, comme c'est le cas dans tous les titres à travers le monde, les créateurs de désinformation mènent des campagnes malveillantes et secrètes en créant des histoires et des erreurs dans tous les secteurs et toutes les plateformes sociales pour atteindre leur objectif.

Il existe des sites Web qui tentent d'enquêter sur la désinformation liée à COVID-19.[7] En un peu plus d'un mois, plus de 50 articles ont été démystifiés et se sont révélés faux. Il est devenu extrêmement difficile de suivre la quantité de désinformation liée à la situation actuelle.

Compte tenu de cela, il est devenu plus important que jamais de veiller à ce que la source des informations soit vérifiée, crédible et corroborée avant toute action concernant les informations.

Utilisation accrue des médias sociaux

Alors que de plus en plus de personnes dépendent des médias sociaux pour obtenir des informations, communiquer avec leurs amis et leur famille, travailler, faire des achats en ligne et plus encore, l'utilisation de tous les médias sociaux a connu une croissance exponentielle à la suite de la crise du COVID-19. Comme souligné ci-dessous, les statistiques montrent maintenant cette augmentation et cela nous aide à comprendre l'impact que les campagnes malveillantes citées ci-dessus pourraient avoir dans le contexte actuel. Cela permet aux cybercriminels d'avoir une base plus large de victimes potentielles dans le cadre de leurs tentatives incessantes de frauder des individus ou des entités.

Les statistiques ci-dessous ont été recueillies à partir d'une enquête auprès de plus de 25 000 consommateurs dans 30 marchés et ont été menées du 14 mars au 24 mars 2020.[8]

L'application WhatsApp a vu une augmentation globale de 40% de son utilisation. Initialement, il a bondi de 27% au tout début de la crise. Pendant la phase intermédiaire de la pandémie, ce nombre a atteint 41% et enfin pour les pays déjà dans la phase avancée de la pandémie, l'utilisation de WhatsApp a bondi de 51%.

Dans certains pays, l'utilisation peut même représenter une valeur beaucoup plus élevée. Par exemple, l'utilisation de WhatsApp en Espagne a atteint 76%.

Cependant, cette application n'est pas seule dans son utilisation améliorée; l'étude a révélé que Facebook, Instagram, WeChat et Weibo ont également connu une augmentation de 40% de leur temps d'interaction.

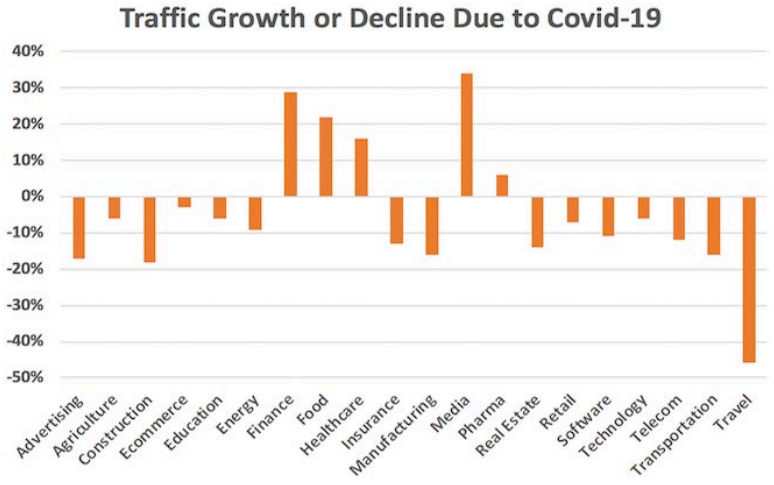


Tableau 1 ([9])

Plus important encore, les consommateurs ont indiqué qu'ils ne faisaient pas confiance à leurs plateformes de médias sociaux pour les nouvelles critiques liées à COVID-19, malgré les taux d'utilisation croissants de ces applications dans le monde entier. Ces informations sont hautement louables et montrent directement que la base d'utilisateurs générale est consciente que les fausses nouvelles et les informations erronées sont monnaie courante sur ces supports.

Les chaînes d'information nationales et les sites Web des agences gouvernementales ont été considérés comme de meilleures options, la plupart des répondants au sondage les identifiant comme une source « fiable » de nouvelles et d'informations. Les plateformes de médias sociaux, quant à elles, n'étaient considérées comme « dignes de confiance » que par 11% des consommateurs.[10]

L'un des résultats statistiques les plus importants résultant de l'utilisation des médias est l'augmentation du temps d'appel en groupe, qui a bondi à plus de 1000% au cours du dernier mois, comme l'a rapporté Facebook Messenger. Cela indique qu'une grande partie du monde maintient correctement la distanciation sociale.

Percent Change in Average Monthly In-Home Data Usage by Device

2019 VS. 2020 - GIGABYTES RECEIVED

	CONNECTED TV	GAMING CONSOLE	PC/MAC	PHONE	SMART SPEAKER	STREAMING BOX/STICK	TABLET	GRAND TOTAL
JAN	26%	6%	-3%	21%	7%	24%	18%	16%
FEB	22%	12%	-5%	27%	-4%	21%	15%	16%
MAR*	27%	12%	-4%	34%	30%	24%	12%	18%

comscore

Source: Comscore Total Home Panel Custom Reporting.
*March compares same 17-day period for both 2019 and 2020

Tableau 2

Average Daily In-Home Data Usage by Device

GIGABYTES RECEIVED

SUN/MON/TUES PERIOD	CONNECTED TV	GAMING CONSOLE	PC/MAC	PHONE	SMART SPEAKER	STREAMING BOX/STICK	TABLET	GRAND TOTAL
MARCH 17-19, 2019	2.6	3.0	1.4	0.7	0.1	3.9	0.4	12.0
MARCH 15-17, 2020	3.6	4.4	1.6	1.0	0.1	5.4	0.6	16.6
PERCENT CHANGE	37%	48%	15%	53%	44%	38%	33%	38%

comscore

Source: Comscore Total Home Panel Custom Reporting

Tableau 3

COVID-19 Impact régional [11]

(au 21 avril 2020)

Nombre total de cas

143,317

Total des décès

6 651

Total des tests effectués

1 992 420

COVID-19 Impact mondial

(au 21 avril 2020)

Nombre total de cas

2 529 707

Total des décès

174 683

Total des tests effectués

22,130,676

Perspective régionale

Dans le contexte des cyberattaques, la région de l'Afrique du Nord et du Moyen-Orient n'est pas épargnée. Les cybercriminels exploitent le fait que les autorités sont actuellement occupées à éviter que la pandémie ne dégénère en une situation incontrôlable. Les attaquants profitent du fait que les gouvernements ont réaffecté du personnel clé pour s'assurer que la crise sanitaire reste sous contrôle. Cette partie du document mettra en évidence différents événements survenus dans la région depuis le début de cette pandémie mondiale.

Risques liés au cyberespace MENA

Infrastructure bancaire et gouvernementale

Plusieurs événements se sont produits au cours des dernières semaines visant des infrastructures bancaires et gouvernementales dans la région. Le service étant limité en raison de nombreux couvre-feux dans plusieurs pays de la région, les cybercriminels sont intervenus pour lancer diverses attaques contre cette infrastructure essentielle.

Bien que toutes les attaques ne réussissent pas, certaines ont permis aux cybercriminels de frauder les victimes à un moment où les économies de chacun deviennent importantes. Dans certains cas, les autorités ont réussi à identifier les suspects et des enquêtes officielles sont en cours.

Les médias sociaux

Pendant cette crise, alors que les gens sont confinés à la maison, beaucoup utilisent les médias sociaux pour se divertir et s'amuser. Les cybercriminels ont tourné leur attention vers plusieurs applications largement utilisées dans la région pour lancer diverses attaques. Par exemple, le 15 avril 2020, l'application populaire Tiktok, dont l'utilisation dans la région a connu une croissance exponentielle au cours des dernières semaines, a été témoin de plusieurs faiblesses exploitées par des cybercriminels où des vidéos non approuvées et non autorisées seraient ajoutées au compte des victimes à leur insu. Il est important de noter que plusieurs organisations régionales utilisent cette application et cela pourrait conduire à des informations erronées sur COVID-19.

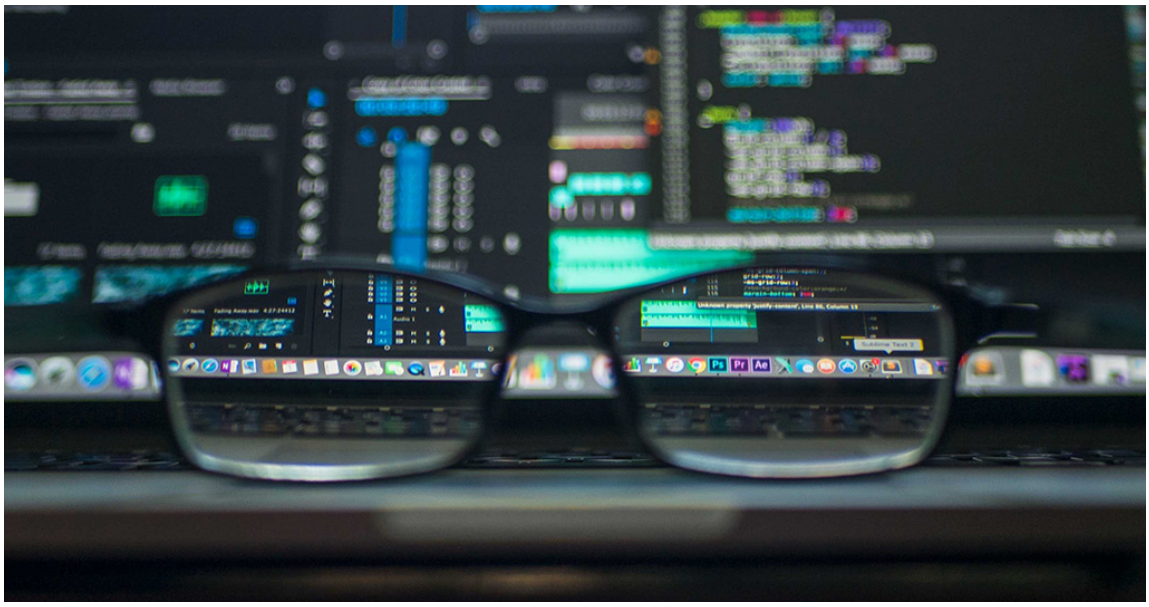
Attaques sur les visioconférences

Alors que la plupart des pays de la région sont soumis au couvre-feu, plusieurs organisations ont permis à leurs employés de travailler à domicile pour aider les autorités à réduire la charge du secteur de la santé en ce qui concerne les infections liées au COVID-19. Ces entreprises, cependant, doivent continuer de mener leurs activités et sont passées à des applications en ligne pour organiser des réunions et d'autres activités requises par leur propre mandat.

Par conséquent, les cybercriminels sont toujours à la recherche d'opportunités d'exploiter différents aspects de la communauté en ligne. Par exemple, une application utilisée pour organiser des réunions, diverses conférences téléphoniques et des formations est devenue populaire depuis que la plupart des pays ont commencé à pratiquer la distanciation sociale. Une faiblesse de l'application a permis aux attaquants de prendre le contrôle total d'une session. Le cybercriminel pouvait intercepter l'audio et la vidéo de tout le monde au cours de la réunion et pouvait également injecter du contenu non sollicité pendant la conférence ou la formation. Il va sans dire que ces réunions contenaient potentiellement des informations confidentielles qui ont ensuite été divulguées ou utilisées de différentes manières criminelles.

Campagnes d'hameçonnage

Comme indiqué précédemment dans ce document, les e-mails de d'hameçonnage font partie de la vie quotidienne depuis la fin des années 1990 et la crise actuelle n'a vu qu'un afflux de ces attaques. Dans la région MENA, plusieurs attaques de ce type ont eu lieu dans toutes les industries, locales, régionales ou internationales. La diligence raisonnable est devenue plus importante que jamais, car nous nous appuyons tous sur des informations publiées en ligne, et nous devons nous assurer que les données sur lesquelles nous travaillons ou que nous visualisons sont correctes.



Réponse régionale de l'ONUDC

Le programme régional sur la cybercriminalité mène actuellement une multitude d'activités d'assistance technique dans la région. Les experts de l'ONUDC en matière de cybercriminalité répondent à la forte demande de leurs homologues concernant cette thématique en leur fournissant l'équipement, la formation et les conseils appropriés.

La situation actuelle étant un défi pour tous les niveaux de gouvernement, les activités et l'équipement à fournir ont été ajustés pour correspondre à la réalité actuelle et pour répondre aux besoins immédiats des différents ministères régionaux impliqués dans la crise qui secoue le monde.

De nombreux risques attendent les gouvernements avec les attaques spécifiques indiquées dans le document actuel. Le vol de données, l'information trompeuse du grand public, la confiance réduite, les problèmes de réputation ne sont que quelques-uns de ces risques qui pourraient devenir une réalité pour toute entité. Par conséquent, une réponse à ces attaques est obligatoire. Cela permettra de minimiser les impacts générés par les cybercriminels dans leur quête pour perturber la confiance du public et réaliser des gains financiers.

Plans futurs

Le programme Cybercriminalité MENA prévoit différentes activités et achats prévus pour les mois suivants, qui renforceront les capacités des pays à répondre plus efficacement à la crise du COVID-19 du point de vue du monde numérique.

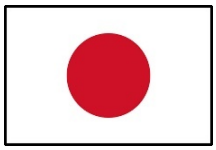
Cette réponse peut prendre les formes suivantes:

- Renforcement de la Cybersécurité pour les infrastructures critiques au niveau national.
- Élaboration de procédures opérationnelles normalisées pour assurer une réponse numérique appropriée.
- Assurer des cycles de formations reconnue internationalement pour les premiers intervenants et les fonctionnaires.
- Acquisition d'équipements d'extraction de données numérique pour garantir une enquête appropriée sur diverses cyber-attaques dans le contexte actuel.
- Évaluation des besoins et assurer une assistance coordonnée au niveau régionale.
- La spécialisation des enquêtes et des interventions sur la cybercriminalité pour empêcher de nouvelles attaques.
- Réponse de criminalistique digitale à diverses scènes de crime ou suivi de données.
- Examen législatif et conseil.
- Assistance à la coopération internationale.
- Campagne de sensibilisation aux réseaux sociaux sur des problèmes spécifiques de la pandémie.

À l'heure actuelle, ces activités ont un besoin immédiat afin d'aider les pays à garantir que la riposte soit uniforme dans le monde entier.

Comme l'indique manifestement l'initiative du Programme mondial de lutte contre la cybercriminalité de l'ONUDC, « le moment n'est pas venu de retirer l'investissement dans la lutte contre la cybercriminalité. La capacité de lutter contre la cybercriminalité sont des éléments essentiels pour protéger les infrastructures nationales critiques, assurer la sécurité des enfants en ligne, autonomiser l'industrie, sécuriser les hôpitaux et soutenir la reprise économique de COVID-19. »[11]

L'équipe de l'ONUDC du programme de cybercriminalité à ROMENA exprime sa gratitude à l'Union européenne, au gouvernement du Japon, au Royaume de la Norvège et aux États-Unis d'Amérique qui, grâce à leur soutien, ont rendu possible les efforts susmentionnés.



Le contenu de cette publication relève de la seule responsabilité de l'ONUDC MENA et ne reflète pas nécessairement les vues des pays mentionnés.

Contributeurs

Les principaux contributeurs au présent rapport font partie du programme de Cybercriminalité de l'ONUDC du Bureau régional pour le Moyen-Orient et l'Afrique du Nord.

M. Patrick BOISMENU,patrick.boismenu@un.org
Conseiller contre la cybercriminalité dans la région MENA et coordinateur du programme

M. Moustafa ELBANNA,mostafa.elbanna@un.org
Responsable régional du programme Cybercriminalité MENA

M. Sadok BEN REJEB,sadok.benrejeb@un.org
Responsable du programme national de cybercriminalité en Tunisie

Mme Nada FARRAG,nada.farrag@un.org
Responsable administrative du programme régional Cybercriminalité MENA

Matériel référencé

1. Dweepobotee Brahma, Sikim Chakraborty and Aradhika Menokee, *The early days of a global pandemic: A timeline of COVID-19 spread and government interventions*, (2 April 2020)
2. UNODC MENA Regional Programme, *COVID-19: How to stay safe from cybercriminals exploiting the pandemic* (March 2020)
3. RiskIQ, *RiskIQ i3: COVID-19 Daily Update* (15 April 2020)
4. UNAIDS, Fact Sheet - World AIDS Day 2019 (1 December 2019)
5. National Cyber Security Centre United Kingdom, *Cyber experts step in as criminals seek to exploit Coronavirus fears (16 March 2020)*
6. Jeremy H, Axel F and Proofpoint threat insight team, *New RedLine Stealer Distributed Using Coronavirus-themed Email Campaign* (16 March 2020)
7. Jane Lytvynenko, *Here's A Running List Of The Latest Hoaxes Spreading About The Coronavirus* (24 March 2020), Jane Lytvynenko, *Here Are Some Of The Coronavirus Hoaxes That Spread In The First Few Weeks* (2 March 2020)
8. Sarah Perez, *Report: WhatsApp has seen a 40% increase in usage due to COVID-19 pandemic* (26 March 2020)
9. Neil Patel, *What The Coronavirus (COVID-19) Means For Marketers* (15 April 2020)
10. Worldometer, *COVID-19 CORONAVIRUS PANDEMIC* (21 April 2020)
11. UNODC Global Programme on Cybercrime, *CYBERCRIME AND COVID19: Risks and Responses* (14 April 2020)