INTERPOL

PANORAMA MONDIAL DE LA CYBERMENACE LIÉE AU COVID-19

#WashYourCyberHands

Des malfaiteurs prolifiques et opportunistes exploitent la pandémie de coronavirus COVID-19 pour lancer toutes sortes de cyberattaques. Des logiciels malveillants connus qui étaient relativement peu actifs ont notamment été de nouveau détectés depuis le début de la flambée épidémique ; ils ont pris de nouvelles formes ou se servent du COVID-19 pour renforcer leur tactique fondée sur l'ingénierie sociale. Dans ce domaine, l'évolution est constante, mais les cybermenaces ci-dessous figurent parmi les plus récentes constatées :

PANORAMA MONDIAL DE LA CYBERMENACE LIÉE AU COVID-19

Domaines malveillants

Le nombre de domaines enregistrés avec les mots clés « COVID » ou « corona » pour tirer parti de l'augmentation des recherches d'informations de la population concernant le COVID-19 est en hausse. Beaucoup sont considérés comme étant à visée malveillante – selon Palo Alto Networks, 2 022 nouveaux domaines enregistrés malveillants et 40 261 présentant un risque élevé avaient été découverts à la fin mars.

Escroqueries en ligne et hameçonnage

Les cybermalfaiteurs créent de faux sites Web liés au COVID-19 afin d'inciter les victimes à ouvrir des pièces jointes malveillantes ou à cliquer sur des liens d'hameçonnage aux fins d'usurpation d'identité ou d'accès illégal à des comptes privés. Trend Micro a également signalé que près d'un million de messages non sollicités envoyés depuis janvier 2020 avaient un rapport avec le COVID-19.

Les escroqueries aux faux ordres de virement (FOVI) sont devenues un outil de prédilection. Elles consistent à usurper les adresses e-mail de fournisseurs et de clients, ou à utiliser des adresses quasi identiques aux leurs, pour mener des attaques. Le besoin pressant de produits de première nécessité constitue pour les malfaiteurs une occasion idéale de récupérer des informations ou de détourner vers des comptes illicites des millions de dollars destinés aux approvisionnements.

Logiciels malveillants visant à obtenir des données

Les logiciels malveillants visant à obtenir des données, tels que les chevaux de Troie contenant un outil de prise de contrôle à distance, les voleurs d'informations, les logiciels espions et les chevaux de Troie bancaires, infiltrent les systèmes en utilisant comme appât des informations liées au COVID-19 afin de compromettre des réseaux, dérober des données, détourner des fonds et constituer des botnets.

Logiciels malveillants visant à désorganiser (rançongiciels et attaques par déni de service distribué)

Les cybermalfaiteurs déploient des logiciels malveillants qui visent à semer la perturbation, à l'instar des rançongiciels ciblant des infrastructures et établissements d'intervention essentiels comme les hôpitaux et centres médicaux, totalement débordés durant la crise sanitaire. En général, ces attaques par rançongiciel et par déni de service distribué n'ont pas pour objet de leur dérober des informations mais de les empêcher d'accéder à des données critiques ou de perturber le système, aggravant ainsi une situation déjà catastrophique dans le monde réel.

Vulnérabilité du télétravail

Les acteurs de la menace exploitent les vulnérabilités des systèmes, réseaux et applications actuellement utilisés par les entreprises, gouvernements et établissements scolaires pour permettre à leurs employés de télétravailler. L'augmentation du nombre de personnes ayant recours aux outils en ligne met à rude épreuve les mesures de sécurité mises en place avant la flambée du virus, et les malfaiteurs sont à la recherche de nouvelles failles leur permettant de voler des données, de s'enrichir ou de provoquer une désorganisation

Évolution attendue

Avec un environnement social et économique en rapide mutation, les cybermenaces pesant sur les particuliers, les entreprises et les infrastructures essentielles continueront à évoluer et à causer des préjudices dans le monde entier. Le nombre de cyberinfractions va augmenter, car les malfaiteurs cherchent à générer de nouvelles sources de revenus en tirant parti des aspects liés à Internet d'autres types de criminalité. Nous devrions donc assister aux phénomènes suivants :

- **Les escroqueries en ligne, l'hameçonnage et les escroqueries aux FOVI vont connaître une croissance importante en raison du ralentissement de l'activité économique et de l'évolution du monde de l'entreprise, et seront à l'origine de nouvelles activités criminelles.**
- Les malfaiteurs tireront parti du marché clandestin pour se tourner vers la « cybercriminalité en tant que service » en raison de la facilité d'accès et de la faiblesse du coût de ces plateformes, ainsi que de leur rendement potentiellement élevé.
- Les acteurs de la menace cibleront les informations personnelles des particuliers en usurpant l'identité des fournisseurs de contenus numériques et en exploitant ces derniers.
- Les gouvernements, entreprises et établissements scolaires dont les employés resteront en télétravail dépendront des connexions en ligne et des outils de communication virtuelle, ce qui les rendra plus vulnérables et ouvrira davantage de possibilités aux cybermalfaiteurs.

La réponse d'INTERPOL

Le Programme mondial de lutte contre la cybercriminalité d'INTERPOL élabore et pilote la réponse internationale des services chargés de l'application de la loi aux cybermenaces qui tirent parti de la flambée de coronavirus. Nous publions des notices mauves pour mettre en garde les pays membres contre les cybermenaces nouvelles et celles présentant un risque élevé, donnons des conseils techniques aux organisations victimes de ces attaques afin de les aider à en surmonter les conséquences et avons réalisé une enquête internationale sur la cybercriminalité afin de mieux appréhender l'évolution rapide de la situation mondiale. Nous collaborons également avec des communauté d'experts en matière de cybersécurité en ligne et organisons des réunions de crise virtuelles avec diverses parties prenantes, parmi lesquelles les chefs des unités nationales et régionales de lutte contre la cybercriminalité, le Groupe d'experts mondial d'INTERPOL sur la cybercriminalité et nos partenaires du secteur privé, afin de proposer aux pays membres des services adaptés en vue de prévenir et de détecter les cyberinfractions et d'enquêter à leur sujet.

INTERPOL

INTERPOL General Secretariat
Tel: +33 4 72 44 70 00
www.interpol.int