Revue de presse des Cybermenaces

Com CyberGend

#7 – Juillet/Août 2022

Département Fusion et analyse de la menace
revue-presse-comcybergend@gendarmerie.interieur.gouv.fr

A retenir

Dans cette revue de presse nous continuons de constater une **évolution des techniques des cybercriminels** qui n'hésitent pas à réagir et à s'adapter aux événements : la restructuration du groupe Conti ou les escroqueries visant le pouvoir d'achat en sont de bons exemples (voir la rubrique « Informations sur la menace »). En complément, le « fait marquant » souligne les impacts de l'**usurpation d'identité** numérique et propose quelques recommandations.

Le chiffre du mois

24 milliards

Il s'agit du nombre d'identifiants et de mots de passe qui seraient en vente sur les forums cybercriminels, soit une augmentation de 5 milliards depuis 2020. On retrouve parmi eux de nombreux mots de passe connus pour être très utilisés. A ce propos, la dernière édition du mois de la Cybersécurité a partagé des bonnes pratiques faciles à mettre en place pour définir des mots de passe robustes. Source : Digital Shadows

Informations générales

Le parlement européen et les États membres de l'UE sont parvenus à un accord sur la directive NIS2 (SRI en français). Pour rappel, la directive NIS première version visait à imposer des normes communes en matière de cybersécurité pour les organisations critiques européennes. Cette nouvelle version de la directive élargit son champ d'application à de nouvelles entités et de nouveaux secteurs tout en renforçant les exigences attendues en la matière. A noter que les États membres disposeront de 21 mois après l'entrée en vigueur de la directive pour la transposer dans leur droit national.

Informations sur la menace

Des chercheurs ont découvert une nouvelle famille de rançongiciel appelée **GoodWill** qui demande aux victimes de réaliser trois activités bienveillantes en échange de la clé de déchiffrement. Quelques exemples : fournir des vêtements aux sans-abri, acheter de la nourriture pour les enfants pauvres ou encore payer des soins médicaux à des personnes n'en ayant pas les moyens. Dans chaque cas, les victimes doivent prouver leurs actions en communiquant sur le sujet, photos à l'appui.

Le célèbre gang Cybercriminel **Conti** a officiellement mis fin à ses activités. L'infrastructure a été mise hors service. Les membres de Conti se sont divisés en petites unités et se sont répartis sur d'autres opérations. Pour rappel, le gouvernement américain considère Conti comme l'une des souches de rançongiciel les plus coûteuses jamais créée, ayant fait des milliers de victimes et permis de soustraire plus de 150 millions de dollars de rançon. Leurs exploits ont conduit le gouvernement américain à offrir une récompense pouvant aller jusqu'à 15 millions de dollars pour l'identification et la localisation des responsables.

DuckDuckGo fait partie des moteurs de recherche alternatifs qui ne tracent pas ses utilisateurs. Mais est-ce vraiment le cas ? Peut-être pas complètement. Un chercheur en cybersécurité a révélé l'existence d'un partenariat qui autorise certains sites appartenant à Microsoft, comme Bing ou LinkedIn, à récupérer des données personnelles sur les internautes.

Forte augmentation d'**escroqueries visant les particuliers** en lien avec le **pouvoir d'achat**. Ces attaques ont pour finalité la récupération des informations bancaires des victimes, usurpant pour cela les sites légitimes de commerçants. Plusieurs techniques sont utilisées, notamment des faux bons de réduction ou de promotion, des faux sites de réservation de voyages et d'hôtels, ou encore des arnaques à l'énergie solaire.

Des **entreprises européennes de l'aérospatiale et de la défense** ciblées par le groupe **Lazarus**. L'entreprise de cybersécurité ESET dévoile le mode opératoire des cybercriminels : ces derniers utilisent les réseaux sociaux, en particulier LinkedIn, pour établir une relation de confiance avec des employés peu méfiants avant de leur envoyer des fichiers malveillants qui usurpent des descriptions de poste. Les cybercriminels n'hésitent pas à s'inspirer d'offres de recrutement légitimes pour ajouter de la crédibilité à leurs campagnes.

Rançongiciel, une **nouvelle tendance à surveiller** : certains cybercriminels piratent le site internet officiel de la victime pour publier leur demande de rançon, exposant ainsi publiquement le méfait et accroissant la pression.

Nouvelle vulnérabilité critique

Une **nouvelle vulnérabilité dans le protocole Bluetooth** pourrait permettre aux attaquants de déverrouiller à distance des serrures intelligentes et des voitures.
La vulnérabilité est liée à des faiblesses dans l'implémentation actuelle de Bluetooth Low Energy (BLE), une technologie sans fil utilisée pour authentifier les appareils Bluetooth qui sont physiquement situés à proximité. Un chercheur de l'entreprise NCC Group a effectué une démonstration vidéo au moyen d'une voiture Tesla.
En attendant un correctif, les chercheurs conseillent aux utilisateurs des produits concernés de désactiver la fonctionnalité de déverrouillage passif et le Bluetooth sur les appareils mobiles.

Source : NCC Group.

Principales cyberattaques

- 14 mai, des cybercriminels ont tenté plusieurs attaques par dénis de service (DDoS) avant et pendant l'**Eurovision 2022**. Source : Zataz
- 27 mai, le **centre hospitalier de Mâcon** victime d'une cyberattaque. L'hôpital s'est mis en relation avec l'ANSSI ainsi que le CERT santé et a déposé plainte. Le fonctionnement interne du système d'information n'a pas été impacté, permettant la prise en charge de l'ensemble des patients. Source : le journal de Saône-et-Loire
- 17 juin, l'**Urssaf** met en garde contre des campagnes frauduleuses relatives au paiement des cotisations. Source : Urssaf
- 8 juillet, La Poste mobile a annoncé avoir été victime d'une attaque par rançongiciel commise par le groupe Lockbit, impactant ses services administratifs et de gestion. Source : Le Monde

Le fait marquant

L'**usurpation d'identité numérique** est le miroir des arnaques en ligne, l'un crédibilisant l'autre. La tendance haussière actuelle est rendue visible par la création de faux comptes. Ceux-ci sont utilisés, par exemple, pour diffuser des informations fallacieuses, partager des liens frauduleux, vendre des biens ou tenter de récupérer des coordonnées bancaires. Il est assez facile de dupliquer un compte existant en usurpant le nom, l'avatar, la marque et la description de ce dernier. Ce nouveau faux compte prétendra alors que le compte original a été piraté.

Nous pouvons citer plusieurs exemples issus de cas réels :
- Usurpation du compte d'une artiste visant à vendre des contenus pornographiques.
- Usurpation du compte d'une société organisant un concours en ligne où les participants ont ensuite été contactés en privé pour leur annoncer qu'ils avaient gagné et leur demander leurs coordonnées PayPal.
- Usurpation du compte d'un consultant réputé pour ensuite recommander d'investir dans certains NFT ou crypto-actifs.

L'impact de ces attaques va au-delà des **pertes immédiates** dues aux activités malveillantes. La personne dont le profil est détourné peut être associée aux actions de l'usurpateur, portant également **atteinte à sa réputation**. La multiplication de ces incidents entraîne une **baisse de confiance** dans l'aptitude des réseaux sociaux à protéger ses utilisateurs. De plus, le délai de réaction de ces plateformes dans le traitement de la demande de fermeture peut paraître assez important (compte-tenu de la perception des faits par les victimes).

Que faire ?

- **Vérifier régulièrement l'existence d'éventuels profils dupliqués**. Si vous en trouvez, utilisez les mécanismes de signalement pour qu'ils soient supprimés. Vous pouvez également obtenir des conseils auprès de Cybermalveillance, demander de l'aide auprès d'associations telles que e-enfance, et bien sûr procéder à un dépôt de plainte !
- **Disposer d'un statut vérifié** permet d'accélérer les demandes de suppression des faux comptes. Ce type de compte est cependant souvent restreint aux personnes ayant une forte visibilité.

Source : ComputerWeekly