MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

LA LETTRE CYBER en Région Grand Est

Gendarmerie nationale

GENDARMERIE

NOTRE ENGAGEMENT, VOTRE SÉCURITÉ

JUIN 2024

LA THEMATIQUE DU MOIS:

LES JEUX OLYMPIQUES DE PARIS (JOP)

Retour sur les menaces les plus courantes (2)

Ces derniers mois, nous avons vu que les JOP pouvaient constituer un moment particulièrement sensible pour notre sécurité informatique. Revenons sur les risques les plus courants.

ESCROQUERIES ET RANSOMWARES

Les escroqueries

Nous avons parlé du phishing qui constitue souvent la première étape pour manipuler les victimes afin de les inciter à cliquer au mauvais endroit ou à communiquer des informations personnelles.

L'objectif recherché sera dans la plupart des cas d'en tirer un profit financier. Mais si les escrocs pourraient se limiter à voler vos coordonnées en toute impunité pour les vendre sur le darkweb, en fait, cela ne leur suffit pas : ils vont aussi rechercher à multiplier leurs chances de gain...

Vous avez cliqué et vous avez communiqué vos informations personnelles pour profiter de promotions sur des billets pour les JO? Vous voudriez vous équiper pour l'occasion et acheter des goodies? Attention, l'escroquerie n'est peut-être pas loin !!

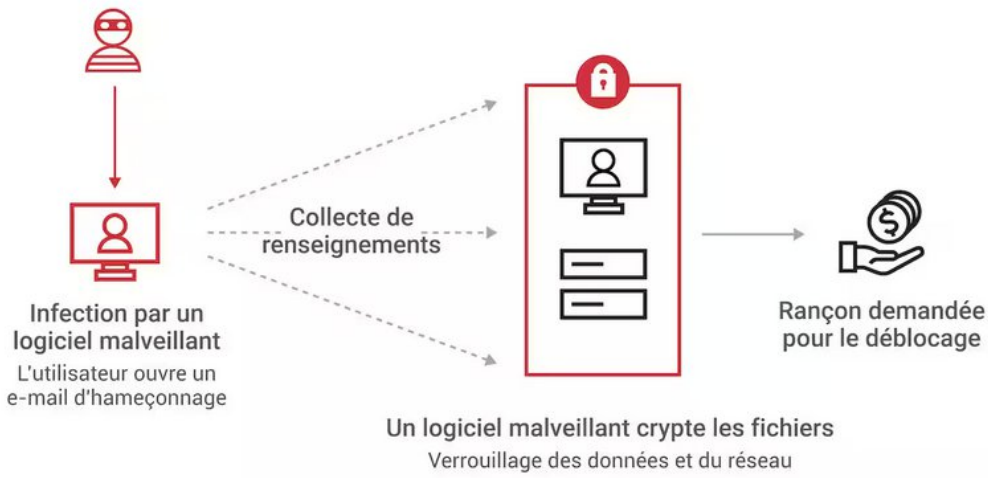
Quelques exemples

Durant toute cette période, nous pouvons être confrontés à de nombreuses formes d'escroqueries dont certaines ont (malheureusement !) déjà été identifiées:

- des faux sites de billetterie en ligne ;
- des fausses offres d'emplacements pour des Food-Trucks ;
- des fausses offres de transports ou de logements ;
- de faux sites de vente de produits dérivés ;
- de fausses annonces de gains: billets pour les JO, cadeaux, sommes d'argent etc…

De manière générale, peu importe ce qu'on vous propose : **si vous n'êtes pas à l'origine de la démarche, ne communiquez rien, ne répondez pas et signalez le mail/SMS.**

Rappel – Les ransomwares ou rançongiciels



Le point de départ d'un rançongiciel est souvent un mail d'hameçonnage dans lequel une victime clique là où il ne faudrait pas et introduit ainsi sans le savoir un logiciel malveillant dans son ordinateur. Le but de l'arnaque consiste ensuite à chiffrer les données de l'ordinateur avant de demander à la victime une rançon pour les rendre de nouveau lisibles. **Chacun doit se sentir ciblé en permanence** : particuliers, TPE/PME, collectivités, artisans, avec un petit ou un gros système informatique, avec ou sans sous-traitance. Chaque utilisateur d'internet doit en être conscient car ce type d'arnaque peut avoir de lourdes conséquences.

Nos conseils:

Ne jamais cliquer sur un lien ou une pièce-jointe sans s'assurer de la légitimité de l'expéditeur

Ne jamais communiquer d'informations personnelles y compris bancaires

Réaliser toutes les mises à jour: systèmes, PC, téléphones mobiles, applications…

Prévenir et sensibiliser vos collaborateurs

Verrouiller les postes et les connexions internet **lorsqu'ils ne sont pas utilisés**

Limiter les droits d'accès au strict nécessaire

Réaliser des sauvegardes (peut-être plus régulièrement que d'habitude en cette période sensible)

Changer et faire changer les mots de passe avant et après les JOP

Identifier le RSSI, le prestataire, **la personne à prévenir le plus rapidement possible en cas d'attaque.**

+ D'INFOS

CYBER MALVEILLANCE .GOUV.FR

PHAROS
PLATEFORME D'HARMONISATION, D'ANALYSE, DE RECOUPEMENT ET D'ORIENTATION DES SIGNALEMENTS

e-enfance 3018

CNIL. PROTÉGER les données personnelles ACCOMPAGNER l'innovation PRÉSERVER les libertés individuelles

ANSSI Agence nationale de la sécurité des systèmes d'information

Région de gendarmerie du Grand Est
LA LETTRE CYBER en région Grand Est

Directeur de la publication: GCA O.KIM
Responsable éditorial: COL L. GRAU
Rédacteur: ADJ M. KNOBLOCH

Si vous souhaitez recevoir cette lettre, envoyez un mail à :
Laurent.grau@gendarmerie.interieur.gouv.fr
Mathieu.knobloch@gendarmerie.interieur.gouv.fr

Suivez l'actualité de la gendarmerie: