Groupement de gendarmerie du Var

Menaces émergentes liées au COVID-19

Depuis la mise en place du confinement, du télétravail et du chômage partiel, certaines entreprises sont à l'arrêt complet ou en forte baisse d'activité pendant que d'autres sont à plein régime.
Cette situation inédite favorise l'apparition d'infractions « cyber » pouvant toucher potentiellement toutes les couches de la population mais également le monde de l'entreprise, l'administration et les collectivités territoriales.

1. Le télétravail

Le télétravail créé naturellement une faille sécuritaire. Les postes de travail sont généralement connectés à la box du particulier et les données sont ensuite transmises à l'entreprise ou la collectivité via internet.

2 hypothèses se présentent au niveau matériel :

- L'employé ou l'agent utilise un ordinateur du travail mis à sa disposition
  - Le responsable de la sécurité des systèmes de l'information doit assurer la maintenance régulière des postes mis à disposition principalement en s'assurant de la mise à jour du système et de sa base virale.
- L'employé ou l'agent utilise son ordinateur personnel
  - L'employeur doit sensibiliser ses subordonnés sur l'importance de la mise à jour des systèmes et de sa base virale
  - L'employé doit dissocier au maximum le professionnel du personnel en stockant par exemple les données de travail sur un support amovible et non sur le PC lui-même

2. L'activité économique

Dans le monde de l'entreprise, le manque d'activité d'un côté et la suractivité d'un autre attirent les cyberdélinquants.

Très en vogue depuis plusieurs années, le Ransomware reste particulièrement actif actuellement :

- **Mespinoza** a touché la mairie de MARSEILLE il y a quelques semaines. Ce logiciel vise particulièrement les collectivités locales, chiffre les fichiers et ajoute l'extension «.pysa ».
- **Maze 2019** circule toujours. Il crypte les fichiers du système informatique et exige une rançon à payer. La communauté Maze a posté un communiqué de presse officiel déclarant ne plus s'attaquer aux organisations médicales durant toute la période d'activité du COVID-19
- **Mamba** et sa famille. Attaque et chiffre un disque complet. Il arrive par une pièce jointe d'un mail frauduleux et se propage sur le système et le réseau. Il est capable de chiffrer un disque complet au lieu de simplement des fichiers individuels.
- **Matrix** est un Ransomware apparu en 2016. Il est en constante évolution. Contrairement à ses pairs, il ne provient pas d'une pièce jointe mais d'un malware, de ce fait il est invisible de l'utilisateur du système. Une fois installé dans le PC, Matrix agit comme un Ransomware traditionnel.

Groupement de gendarmerie du Var
Section Opérationnelle de Lutte contre les Cybermenaces
solc.bdrij.ggd83@gendarmerie.interieur.gouv.fr

La neutralisation simple sans finalité financière fait aussi rage en cette période avec l'apparition de deux malwares :

- Le malware **Covid19.exe** a fait son apparition. Il a juste pour but de réécrire la MBR (Master Boot Record) du système ce qui empêche simplement de démarrer le système et entraîne une immobilisation de l'ordinateur le temps d'une maintenance.
- Un deuxième malware est en circulation, celui-ci laisse sa victime croire qu'il s'agit d'un Ransomware alors que le programme en arrière-plan s'occupe de récupérer tous les identifiants et mots de passe de la victime.

Une attention particulière peut être également apportée sur les escroqueries du type « faux ordres de virement (FOVI) ». Ces escroqueries sont principalement axées sur la pénurie de masques et de gel hydroalcooliques, une pharmacie de Seine Maritime a très récemment été victime après avoir passé une commande pour 6 millions d'Euros de gel. Ce risque de « FOVI » est très élevé en raison de la baisse de vigilance sur les protocoles de vérification des virements au sein d'une entreprise dont les personnels sont soumis au régime du télétravail.

Les visioconférences :

L'utilisation de la visioconférence est démultipliée en cette période de confinement. Comme tous logiciels informatiques des failles existent et sont exploitées par les hackers. Le logiciel ZOOM a fait récemment l'objet d'un « ZOOM-bombing » dont le principe est de pénétrer des conférences professionnelles pour y perpétrer du désordre. La faille est corrigée pour cette application mais les logiciels SKYPE, SLACK et WEBEX ont récemment été usurpés.
La société KASPERSKY a pu identifier 1 300 fichiers reprenant les noms des applications citées supra. Parmi ceux-ci contenaient des publiciels (adwares) et maliciels (malwares). Une fois installés à l'insu de l'utilisateur, ils mettent en péril les données et leur confidentialité.

Pour éviter au maximum le risque lié aux visioconférences :

Télécharger le logiciel **exclusivement** sur le site officiel de l'éditeur.

Rappel général sur les « gestes barrière » informatiques :

La majorité des Ransomware, Malware ou encore FOVI peuvent être écartés en respectant les mesures suivantes :

- Maintenir le système d'exploitation à jour
- Vérifier l'actualisation régulière de la base virale de son antivirus
- Ne jamais ouvrir la pièce jointe d'un mail de provenance inconnue (vérifier avec attention l'orthographe du mail de l'expéditeur)
- Sauvegarder régulièrement les données sensibles sur un support externe
- Télécharger les données et attestations ou consulter via des sites du gouvernement

Rappel : le « *hashtag* » *#Cyberchezmoi* a été créé par l'ANSSI afin de rappeler les bonnes pratiques à adopter par les télétravailleurs et leurs employeurs. Sur TWITTER, il est régulièrement utilisé à cet effet par les entreprises, institutions ou utilisateurs privés.[1]

Consultez aussi : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/recommandations-securite-informatique-teletravail

1 ANSSI : https://twitter.com/ANSSI_FR/status/1248163021375094784?s=19
CESIN FRANCE : https://twitter.com/CESIN_France/status/1248645438976266241?s=19
ISSA FRANCE : https://twitter.com/ISSA_France/status/1249985972051288065?s=19