**CONCOURS ou EXAMEN**

donnant accès à l'emploi de :

**TECHNICIEN TERRITORIAL**

à titre interne ☑ (1)
à titre externe ☐ (1)
au titre du troisième concours ☐ (1)

Spécialité : **Ingenierie informatique et systèmes d'information**

Épreuve de **RAPPORT TECHNIQUE**

Date de l'épreuve : **12/04/2018**

---

**Ville de Techniville**  
**le 12/04/2018**

**RAPPORT TECHNIQUE**

à l'attention du directeur des systèmes d'information

**LES ATTAQUES VIRALES DE TYPE “RANSOMWARE”**

---

L'accès illimité à Internet apparaît comme étant la grande révolution du 21ème siècle. Des milliers de français en sont équipés, facilitant ainsi leurs moyens de communication, avec notamment le développement des réseaux sociaux, mais aussi en simplifiant leurs démarches administratives. Personnellement et professionnellement, Internet est devenu indispensable dans notre quotidien.

De rives de la Méditerranée à ce succès retentissant ;
la cyber-criminalité.

En pleine expansion, les attaques virales sont de plus en plus nombreuses et fréquentes sur la toile. Parmi elles, le ransomware appelé aussi xarjogiciel ou logiciel de rançon.

Ce rapport technique permettra de faire, dans un premier temps, un état des lieux des attaques virales du type ransomware.

Dans un second temps, il mettra en exergue la prévention des risques face aux attaques de xarjogiciel.

I. État des lieux des ransomwares

Dans cette première partie, une définition du terme anglais "Ransomware" sera apportée. De plus, il sera présenté différentes formes de ransomware.
A. Qu'est-ce qu'un ransomware ?

Contreirement à ce que l'on peut croire, les ransomwares ou rançongiciels ne sont pas vraiment nouveau puisque les premiers ont fait leur apparition dès 1989. Cependant, ils ont connu une croissance exponentielle ces dernières années.

Un ransomware est un logiciel malveillant qui infecte un ordinateur ou certaines données en les cryptant. Dès lors que l'ordinateur est infecté par ce logiciel, un message d'alerte s'affiche sur l'écran demandant une rançon à payer pour obtenir une clé qui permettra au propriétaire de l'ordinateur infecté de déchiffrer les données. La rançon demandée est généralement de l'ordre de centaines de dollars. De fonctionnement d'un ransomware est à peu près similaire à un cheval de Troie.

Le but du rançongiciel est d'extraire de l'agent à l'utilisation de l'ordinateur par différents moyens de paiement : virement bancaire, SMS, autarx, plateformes de paiement ou encore par le biais d'une carte prépayée.

Personne n'est à l'abri d'une attaque d'un logiciel de rançon. Des cyber-criminels s'attaquent généralement aux utilisateurs les plus vulnérables et non aux grands groupes et aux grandes entreprises qui sont le plus du temps bien équipées et bien préparées à ce genre d'attaques virales.

B. Les différentes formes de rançongiciels

Les ransomwares se renouvellent constamment et peuvent révéler différentes formes.

En premier lieu, il existe les ransomwares pécuniers. En bloquant l'ordinateur de l'utilisateur ou simplement le navigateur internet, le logiciel demande de payer une *d'euces par ordinateur*.
amandé par un message de l’État, de la police ou de la gendarmerie au démançage de l’ordinateur.


De plus, si l’ordinateur est connecté en réseau, le logiciel de rançon peut se propager et s’étendre aux autres ordinateurs cryptant ainsi des millions de données.


La multiplication des ransomwares et leur dangerosité plus ou moins apparente engendrent impliquent aux responsables de la sécurité des systèmes d’information (SSI) d’appliquer certains principes de prudence en amont et en aval d’une cyber-attaque.
II. La prévention des risques face aux attaques de ransomware

Afin de se protéger des attaques virales causées par des ransomware, quatre règles simples sont à appliquer. De plus, en cas d'infection, il faudra agir le plus vite possible afin d'en limiter les dégâts.

A. Prévenir et sensibiliser aux risques d'attaque

Afin de perdre le minimum de données, il est essentiel de réaliser des sauvegardes de l'ensemble du contenu régulièrement. Ainsi en cas d'attaque, la majorité des données pourra être restaurées sur l'ordinateur.

La deuxième règle à appliquer pour limiter le risque d'attaque est la mise à jour constante des systèmes d'exploitation, des navigateurs, des périphériques, des antivirus, dès que celles-ci sont possibles.

La troisième règle à suivre est la protection de l'ordinateur en lui-même, par l'installation d'un antivirus. Il en va de même pour la protection des boîtes mails qui doivent être équipées d'un système d'analyses de type Altospan et de l'activation du chiffrement TLS.

Enfin, la dernière règle est non des moindres : la sensibilisation des usagers. Il faut

Afin de limiter au mieux le risque d'attaque et de propagation, il doit être mis en place une vraie stratégie de sensibilisation par la mise en œuvre d'une charte informatique expliquant les règles de base de manière claire et simple comme : la non ouverture d'un mail suspect et des pièces jointes, le signalement d'e-mails douteux, la mise en place de mots de passe complexes...

De plus, la définition de référents SSI par direction parait être
Une solution pour être aux plus proches des agents et aussi contribuer au rappel des règles de "bonne conduite" à adopter pour éviter une cyber-attaque.
Enfin, la formation personnelle et professionnelle des utilisateurs internautes paraît être une solution durable et efficace sur les risques liés aux cyber-attaques.

B. Que faire en cas d'infection?

En cas d'infection par un logiciel de rançon, l'utilisateur devra avoir des réflexes rapides afin de limiter la propagation de la première chose à faire en cas d'attaque sera de désactiver la connexion internet pour éviter toute propagation supplémentaire.

Ensuite, il faudra supprimer le plus tôt possible le logiciel de rançon.

Si une sauvegarde a été effectuée peu avant l'attaque, les données pourront être réinstallées après la restauration et le nettoyage de l'ordinateur infecté.

Si la sauvegarde des données n'avait pas été faite avant, il faut considérer que les données cryptées par le ransomware sont définitivement perdues, le paiement de la rançon n'assurant pas la récupération des données. De plus, le choix de payer la rançon peut s'avérer néfaste, permettant ainsi le financement des attaques de ransomware nouvelles.

Enfin, il est recommandé de porter plainte en cas d'attaque virale.
D'ailleurs, les articles 33 et 34 du RCGD qui renvoient très prochainement en vigueur, obligent à faire état des attaques ransomware auprès des autorités ainsi qu'aux
En conclusion, il peut être dit que le ransomware est un vrai fléau grandissant de par son agressivité et les différents formes qu’il peut revêtir. Pour limiter son impact négatif, il sera d’usage de prévenir les risques en protégeant au mieux le matériel et en sensibilisant les usagers aux risques engendrés par ces xénogiciels.