CENTRE DE GESTION
DE LA FONCTION PUBLIQUE TERRITORIALE DU RHÔNE

CONCOURS ou EXAMEN

donnant accès à l'emploi de :

TECHNICIEN TERRITORIAL

à titre interne [X] (1)

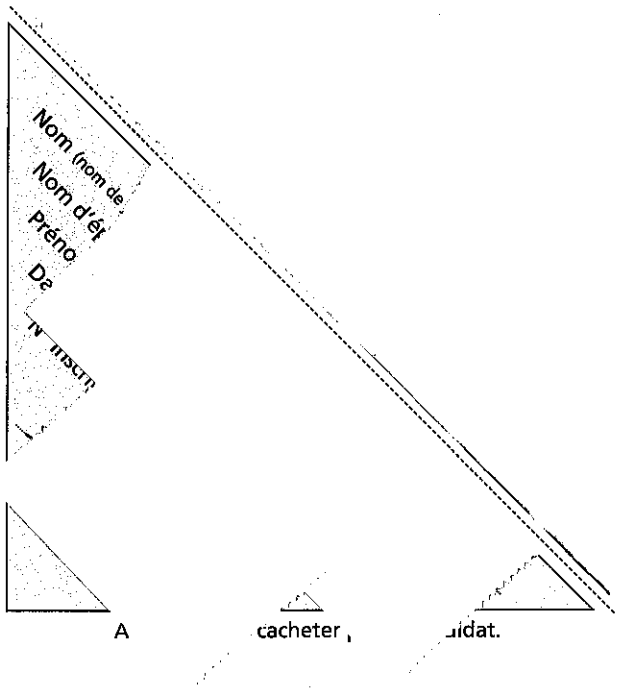
à titre externe [ ] (1)

au titre du troisième concours [ ] (1)

Spécialité Ingénierie informatique et système d'information

Épreuve de RAPPORT TECHNIQUE

Date de l'épreuve 12/04/2018



Colonne réservée à l'Administration

Numéro de correction

Numéro d'anonymat

Note attribuée (réservé au jury)

15,50

Visa du jury ou de la Commission de Surveillance

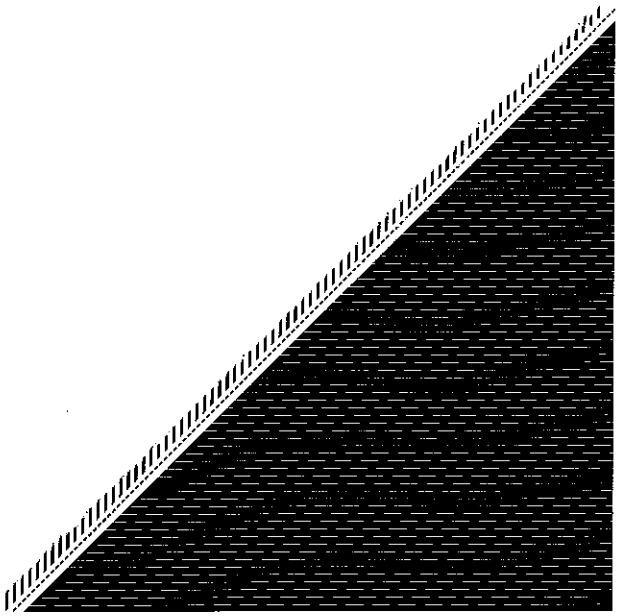
(1) Cocher la case correspondante

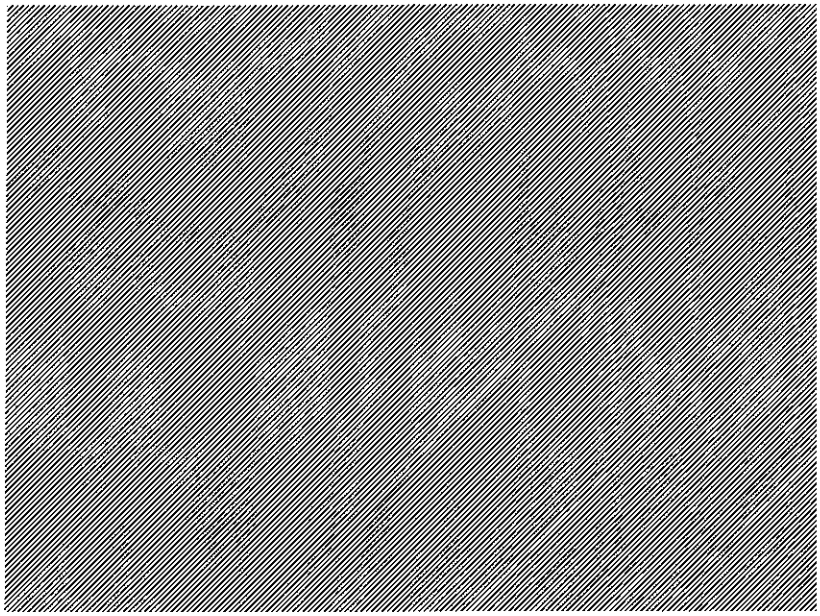
Ville de Techniville. le 12/04/2018

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 millions 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 revers de la médaille 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 rançongiciel ou logiciel de rançon.

Ce rapport technique permettra de faire, dans un premier temps, un état des lieux des attaques virales de type Ransomware.
Dans un second temps, il mettra en exergue la prévention des risques face aux attaques de rançongiciel.

I- Etat 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 ?

Contrairement 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 l'ors 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 infesté de déchiffrer les données. La rançon demandée est généralement de l'ordre de centaines* de fonctionnement d'un ransomware est à peu près similaire à un cheval de troie.
Le but du rançongiciel est d'extorquer de l'argent à l'utilisateur de l'ordinateur par différents moyens de paiement : virement bancaire, SMS surtaxés, plateformes de paiement ou encore par le bitcoins, une monnaie virtuelle anonyme.
Personne n'est à l'abri d'une attaque d'un logiciel de rançon. Les cyber-criminels s'attaquent généralement aux utilisateurs les plus vulnérables et non aux grands groupes et aux grandes entreprises qui sont la plupart du temps bien équipées et bien préparées à ce genre d'attaques virales.

B. Les différentes formes de rançongiciels

Les ransomware se renouvellent constamment et peuvent revêtir différentes formes.

En premier lieu il existe les ransomwares policiers. En bloquant l'ordinateur de l'utilisateur ou simplement le navigateur internet, le logiciel demande de payer une

*d'euros par ordinateurs.

amende par un message de l'Etat, de la police ou de la gendarmerie au démarrage de l'ordinateur.

Ensuite, il existe les crypto-ransomwares. Ces rançongiciels vont infecté l'ordinateur de l'utilisateur par le chiffrement de certains données. Les crypto-ransomwares envoient un message d'alerte en réclamant un rançon contre l'obtention d'une clé de décryptage. Ces logiciels passent par la voie du mail et ont besoin de droits d'administration pour s'installer sur l'ordinateur. En règle générale se sont des fichiers de types .zip, .pdf ou des documents word, qui ouverts, patent l'infection dans l'ordinateur par une faille du système d'exploitation (exemple: logiciel Wannacry qui passe par la faille du protocole SMB de Windows).
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 milliers de données.

La dernière forme de ransomware est moins nuisible puisqu'elle n'infecte pas les données. ~~mais~~ Certains rançongiciels vont juste bloquer l'accès à l'ordinateur en demandant de cliquer sur des publicités pour le déverrouiller. Chaque clic appate à l'auteur du virus de l'argent.

La multiplication des ransomwares et leur dangerosité plus ou moins ~~aggressive~~ agressive implique aux responsables de la sécurité des systèmes d'information (SSI) d'appliquer certains principes de précaution 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 rançongiciels, 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 Altospam 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 paraît être

une solution pour être au plus proche des agents et ainsi 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 liées 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.

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 réinstallée 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 cryptés 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 RGPD, qui rentrera très prochainement en vigueur, obligent à faire état des attaques ransomware auprès des autorités ainsi qu'auprès

des personnes affectées par ces attaques.

En conclusion, il peut être dit que le ransomware est un vrai fléau grandissant de par son agressivité et les différentes 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 ransogiciels.