académie Bordeaux

RÉGION ACADÉMIQUE
NOUVELLE-AQUITAINE

MINISTÈRE
DE L'ÉDUCATION NATIONALE
MINISTÈRE
DE L'ENSEIGNEMENT SUPÉRIEUR,
DE LA RECHERCHE
ET DE L'INNOVATION

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Sécurité des Systèmes d'Information

Réf : BUL05-SSI-07062017		Date : 7 juin 2017
	BULLETIN D'INFORMATION	
		Diffusion : tous les personnels de l'académie

OBJET : Ransomware (rançongiciel ou logiciel de rançon) et Cryptoware (cryptogiciel)

Les ***ransomware***, **rançongiciel** ou **logiciel de rançon** et les cryptoware ou cryptogiciel sont des logiciels malveillants qui prennent en otage les données qui se trouvent sur votre ordinateur et sur les espaces de partage de documents.

Pour ce faire, ces logiciels cryptent tout ou partie des fichiers d'un ordinateur puis demandent à leur propriétaire d'envoyer de l'argent en échange de la clé qui permettra de les décrypter. Ils peuvent également bloquer l'accès de tout utilisateur à un ordinateur, une tablette ou un smartphone jusqu'à ce qu'une clé ou un outil de débridage soit envoyé à la victime en échange d'une somme d'argent.
Ces logiciels de rançon sont créés et diffusés par des escrocs et peuvent être introduits par une pièce jointe. Ils peuvent également provenir de réseaux sociaux (Facebook, Linkedin…) au travers d'une image infectée ou de tout autre site internet.

Soyez très prudent lorsque vous surfez sur internet ou que vous lisez vos courriels, en particulier les pièces jointes qui y sont associées et les documents que vous téléchargez. Méfiez-vous des extensions : .svg, .js, .hta … Le logiciel malveillant est téléchargé automatiquement si vous cliquez sur l'image ou lorsque vous ouvrez le document.

Pour se prémunir des menaces liées aux logiciels malveillants qui tentent d'extorquer de l'argent et qui cryptent vos données, voici la conduite à tenir :

- **Sauvegardez vos fichiers** : il convient d'avoir ses données importantes dupliquées (stockées à deux endroits différents en tout temps). La sauvegarde doit être faite de façon régulière sur un support qui est lié à l'appareil à sauvegarder uniquement lors de la copie des fichiers (clé USB, disque dur externe, sauvegarde en ligne…). En effet les logiciels malveillants peuvent également se propager aux supports de stockage connectés à l'appareil infecté.

- **Mettez à jour vos systèmes et logiciels** : assurez-vous que vos systèmes Windows, Mac, Android, iOS ou autres sont à jour et vérifiez régulièrement que vous utilisez la dernière version de vos logiciels favoris, notamment les navigateurs. Les logiciels malveillants utilisent les failles de sécurité des systèmes et des logiciels pour s'installer.

- **Redoublez de prudence avec les pièces jointes :** les pièces jointes des courriels sont généralement les moyens utilisés par les pirates pour diffuser leurs logiciels malveillants. Il convient donc d'éviter d'ouvrir ou d'exécuter des pièces jointes reçues si vous avez un doute sur le but ou l'origine du message. Demandez confirmation à l'expéditeur si vous n'êtes pas certain que l'envoi est légitime. N'ouvrez pas les pièces jointes d'un courriel provenant d'un inconnu.

- **Surfez responsable et n'installez pas des applications provenant de sources inconnues** : évitez les sites douteux, ne cliquez pas sur des liens suspects, évitez de télécharger des fichiers et d'installer des applications trouvées sur internet ou depuis des sites non officiels.

- **Utilisez un antivirus à jour :** les logiciels malveillants, virus et autres malwares, évoluent en permanence. Pour cette raison on pourra trouver différentes variantes d'un même logiciel malveillant. Il est donc nécessaire d'utiliser un antivirus à jour qui permet de s'assurer que les dernières signatures de logiciels malveillants sont bien enregistrées et que votre antivirus pourra les reconnaitre. Attention toutefois : un fichier téléchargé mais non signalé comme dangereux par l'antivirus ne signifie pas pour autant qu'il est sain. L'anti-virus peut ne pas encore connaitre le logiciel malveillant qu'il contient ou sa variante.

  Utilisez un antispam : dans la mesure où les logiciels malveillants se propagent majoritairement par l'intermédiaire de la messagerie électronique, l'utilisation de filtres antispam permet de réduire le nombre de courriels malveillants et indésirables. La messagerie académique est équipée d'un logiciel antispam qui bloque une partie de ces messages et met en quarantaine les messages douteux.

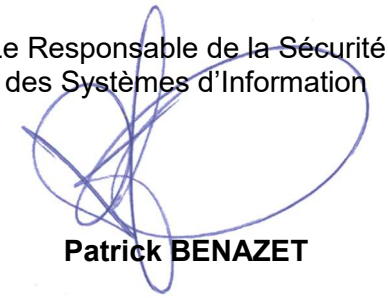
En cas d'infection par un ransomware :

- **Ne payez jamais en cas de demande de rançon :** rien ne vous garantit que les pirates vous fourniront la clé qui permettra de décrypter vos fichiers ou débloquer votre ordinateur. De plus, cela encourage ce type d'attaque et la mésaventure pourrait bien se répéter.

- **Arrêtez la propagation :** dès que vous vous apercevez de l'infection, éteignez l'ordinateur, la tablette ou le smartphone. Avant de rallumer débranchez les disques externes encore sains pour éviter le chiffrement de vos fichiers encore intacts et déconnectez-vous du réseau (filaire, wifi ou 3g).

- **Signalez l'attaque au service d'assistance :** contactez le service d'assistance informatique qui s'occupe de votre équipement afin qu'il vienne le désinfecter et vous aider à restaurer les données que vous aurez sauvegardées.

Le Responsable de la Sécurité
des Systèmes d'Information



Patrick BENAZET