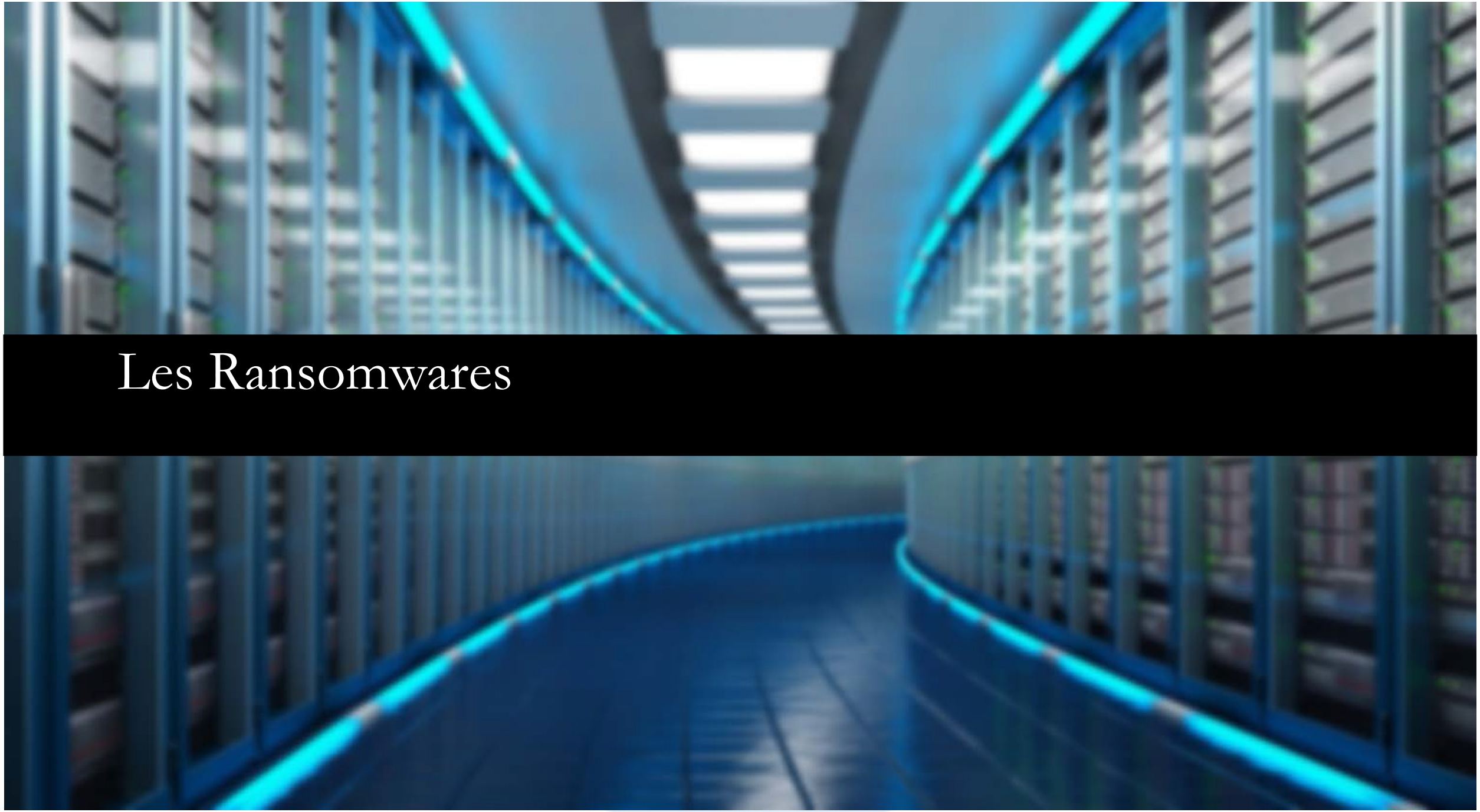
CYBERCRIMINALITE, UN RISQUE AU QUOTIDIEN !

Groupement de Gendarmerie Départementale de la SAVOIE

Adjudant-Chef ALGRAIN ERIC – NTECH S.O.L.C. 73
Enquêteur en technologie numérique



Les Ransomwares

Progression :

Progression :

Définition :

Définition de Ransomware : Un ransomware, ou rançongiciel en français, est un logiciel informatique malveillant, prenant en otage les données. Le ransomware chiffre et bloque les fichiers contenus sur votre ordinateur et demande une rançon en échange d'une clé permettant de les déchiffrer. Apparus dans un premier temps en Russie, les ransomwares se sont répandus dans le monde entier, et principalement aux États-Unis, en Australie ou en Allemagne. Bien souvent, le ransomware s'infiltre sous la forme d'un ver informatique, à travers un fichier téléchargé ou reçu par email et chiffre les données et fichiers de la victime. La finalité est d'extorquer une somme d'argent à payer le plus souvent par monnaie virtuelle pour éviter toute trace. *(Altospam.com)*

Dé

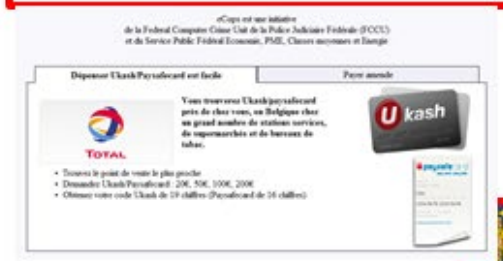
Don't worry,you can
If you want to resto
Use Tor Browser to
If you have not been

Ce blocage
illegaux. Le
derogation
On a releve
a "82.123.9
pornographi
de violence
avec les ele
meme on a
spam avec l

Gendarmerie/ecops

Gema

Gimemo



Goldenbaks

Silence locker

Reveton

AlertLock

ACCDFISA

Progression :

Les infractions :

ARTICLES	LIBELLÉ
Art. 312-1 du Code Pénal	**Extorsion** : De tels procédés relèvent de l'extorsion de fonds et non de l'escroquerie. En effet, ils se caractérisent par une contrainte physique – le blocage de l'ordinateur ou de ses fichiers – obligeant à une remise de fonds non volontaire.
Art. 323-1 du Code Pénal	**Atteinte STAD** : L'infraction d'atteinte à un système de traitement automatisé de données (STAD) pourra aussi être soit du fait d'une modification frauduleuse de données soit d'une entrave au bon fonctionnement d'un STAD.
Par ailleurs, depuis 2013, la détention ou la cession d'un rançongiciel, sans motif légitime, est passible des mêmes peines	
Dans le cadre des atteintes aux STAD, la circonstance aggravante de bande organisée est très souvent retenue. En effet, la commission de ces infractions requiert en principe la mise en œuvre de différentes compétences et donc l'intervention de plusieurs personnes pour la conception, injection du virus, expédition du mail infecté, collecte de la rançon.	

Progression :

Sites de déchiffrement de ransomwares:

- https://noransom.kaspersky.com/fr/
- https://id-ransomware.malwarehunterteam.com/
- https://www.nomoreransom.org/fr/index.html
- https://www.avast.com/fr-fr/ransomware-decryption-tools
- https://www.avg.com/fr-fr/ransomware-decryption-tools

Progression :

Conduite à tenir :

↳ **ISOLER LE SYSTEME INFECTE d'autant plus s'il est relié à un réseau (internet et intranet) ;**

↳ **DEBRANCHER les câbles Ethernet et déconnecter tout accès réseau (Wifi, Bluetooth…). Il en est de même si les serveurs (internes ou externes) sont touchés, il faut immédiatement les isoler du réseau**

↳ **IDENTIFIEZ LA SOURCE DE L'INFECTION la nature du ransomware ; le point de compromission et appliquer un protocole de déchiffrement s'il existe prendre les mesures nécessaires**

↳ **CONTACTER L'ADMINISTRATEUR RESEAU et mettre en place un protocole d'identification et de confinement des postes infectés**

↳ **AVERTIR LE PERSONNEL dans le but d'éviter que d'autres attaques soient générées et pour sensibiliser sur les risques liées à l'attaque**

↳ **UTILISEZ UNE MÉTHODE DE DÉCHIFFREMENT, uniquement si le malware est clairement identifié et que cette solution existe. Si le malware n'est pas identifié ne rien faire car il y a un de perte totale des données avec un effet irréversible**

Conduite à tenir (suite) :

- **FORMATER le poste et réinstaller un système sain si les fichiers ne présentent aucun caractère important**

- **ETRE ASSISTE de professionnels qualifiés suivant les cas**

- **PRENDRE soin de noter toutes les étapes et actions menées immédiatement et consécutivement à l'attaque**

- **COLLECTER tous les éléments de preuve qui seront utiles aux autorités dans le cadre de leurs investigations, mails, logs, liens, adresses internet et informations diverses**

- **DEPOSER une plainte auprès des autorités compétentes**

- **NE SURTOUT PAS PAYER afin de ne pas alimenter le système mafieux, en plus de n'avoir aucune garantie d'obtenir la clé de déchiffrement**

Progression :

Mesures préventives :

↳ **SENSIBILISER la formation et la sensibilisation restent la meilleure des défenses. Se tenir régulièrement informer des menaces de sécurité. Apprendre à détecter et gérer les anomalies rencontrées (ingénierie sociale, phishing, etc…)**

↳ **NE PAS OUVRIR les mails, leurs pièces jointes et ne pas cliquer sur les liens provenant de chaînes de messages, d'expéditeurs inconnus ou d'un expéditeur connu, mais dont la structure du message est inhabituelle ou vide. Qui ne vous semble pas adressé et qui comporte des anomalies, ou incohérences**

↳ **REALISER régulièrement des sauvegardes des données et du système afin de pouvoir le cas échéant les réinstaller à une date antérieure, si ces derniers n'ont pas été corrompus. Diversifier les sources et niveau de sauvegarde.**

↳ **TOUJOURS maintenir son système à jour les mises à jour logicielles apportent les correctifs nécessaires sur les failles de vulnérabilités connues. Il est donc nécessaire de les faire systématiquement dès qu'elles sont disponibles chez l'éditeur.**

↳ **TENIR A JOUR l'antivirus et configurer votre pare-feu, vérifier et mettre en place un protocole ne laissant passer que les applications, services, accès et machines autorisés. S'assurer que ces softwares soient à jour afin d'avoir toujours les dernières définitions de virus connues à ce jour.**

Mesures préventives :

- **UTILISER des mots de passe suffisamment complexes et les changer régulièrement, l'utilisation d'un gestionnaire de mots de passe est privilégié. A minima il faut un mot de passe de 12 caractère avec des caractères spéciaux.**

- **NE PAS INSTALLER d'applications ou de programmes dont l'origine ou la réputation sont douteuses**

- **CLOISONNER l'accès administrateur du système, il convient de définir très précisément l'accès au compte administrateur du système tout comme les personnes pouvant bénéficier de ces privilèges. En agissant de la sorte et en différenciant les comptes utilisateurs des comptes administrateurs, on limite l'accès aux points critiques du système.**

- **EVITER les sites non sûrs ou illicites tels que ceux permettant le téléchargement de contenus numériques (musique, films, logiciels…) ou certains sites pornographiques qui peuvent injecter du code en cours de navigation et infecter votre machine.**

- **DESACTIVER LES MACROS présentes dans de nombreux fichiers, notamment ceux des suites bureautiques, elles peuvent exécuter un malware. Les désactiver d'office réduit les conséquences que cela peut avoir si utilisateur sélectionne un fichier infecté.**

Mesures préventives :

- **ETRE VIGILANT avec les supports externes ils peuvent contenir des malwares qui s'exécuteront sur le système, ou à l'inverse le malware pourra s'installer dessus et s'installer sur d'autres systèmes.**

- **COMPARTIMENTER LE RESEAU les ransomwares chercheront à se propager, d'abord latéralement dans le système pour obtenir le maximum de données nécessaires puis « verticalement » en élevant consécutivement leurs privilèges jusqu'à atteindre l'administrateur. Ainsi un cloisonnement permet de limiter cette propagation du malware dans le système.**

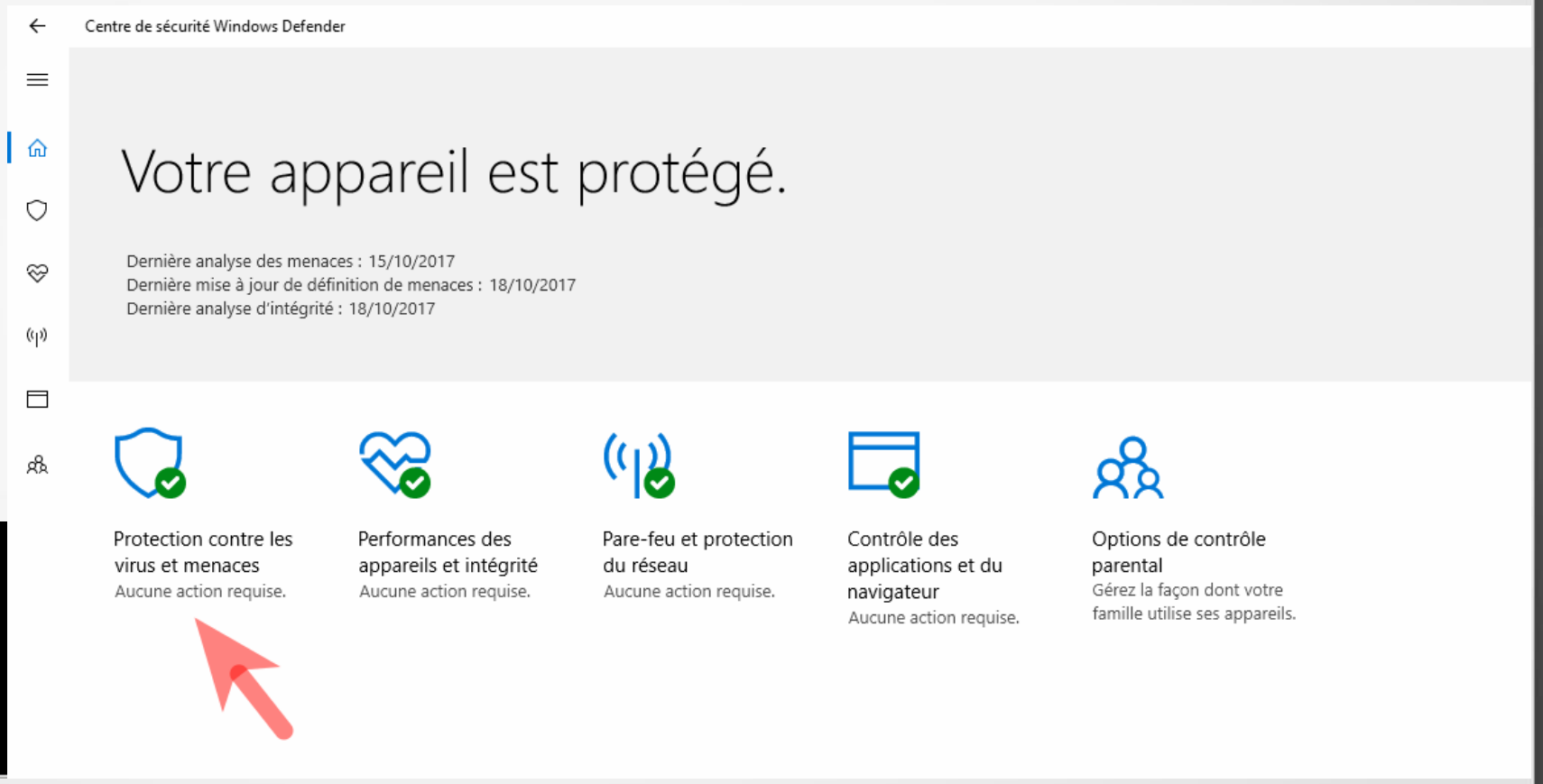
- **NE JAMAIS TRANSMETTRE ses données personnelles avant d'avoir vérifier les garanties d'un site. Dans tous les cas il est vivement conseillé de ne pas fournir ses coordonnées bancaires en ligne, pour une mise à jour de son dossier**

- **CHIFFRER dès que possibles données sensibles présentes sur votre PC**

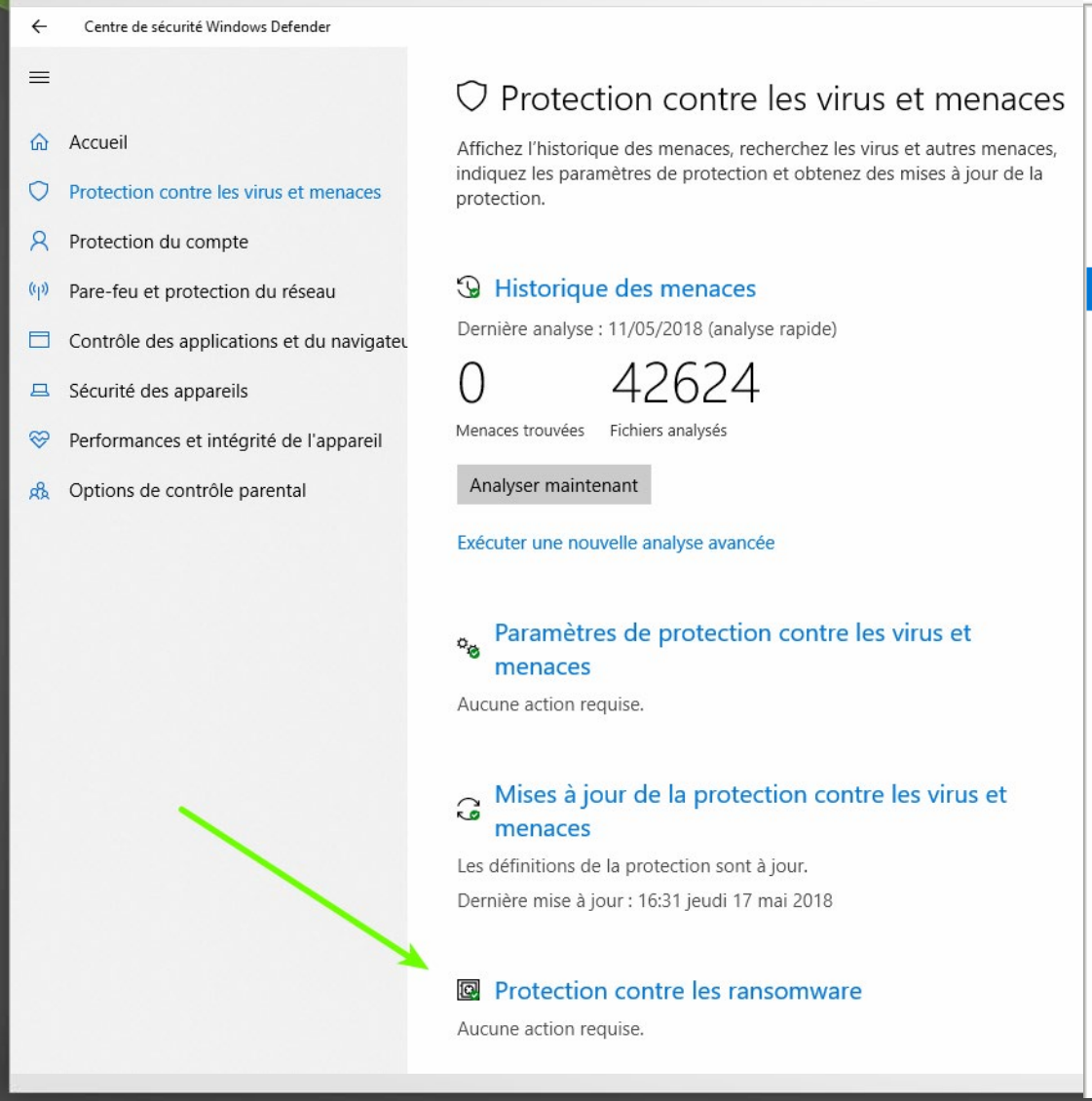
- **ÉTEINDRE votre machine dès lors que vous ne vous en servez pas**

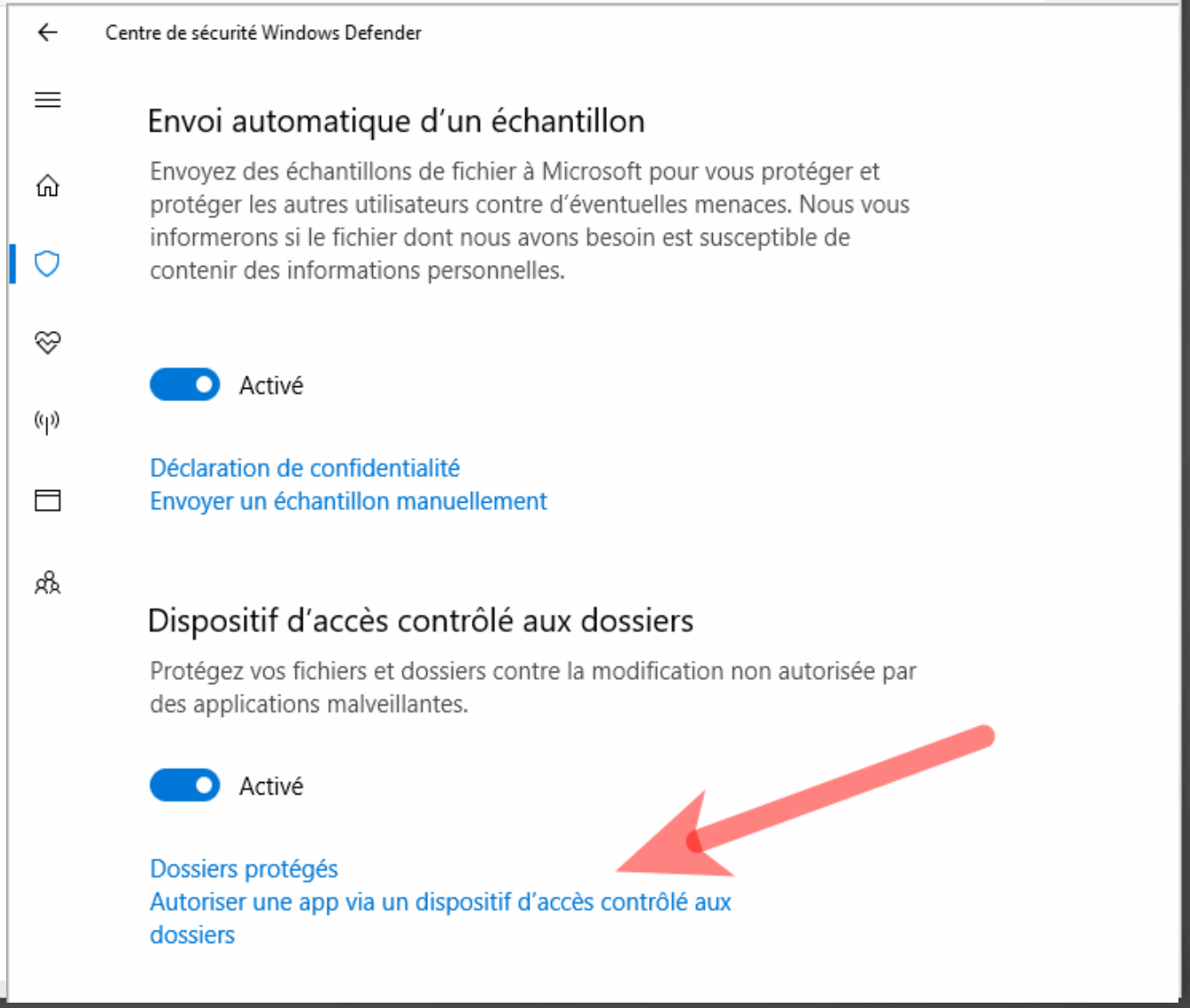
WINDOWS 10 : une solution ?

Comment activer la protection Anti-Ransomware de Windows 10

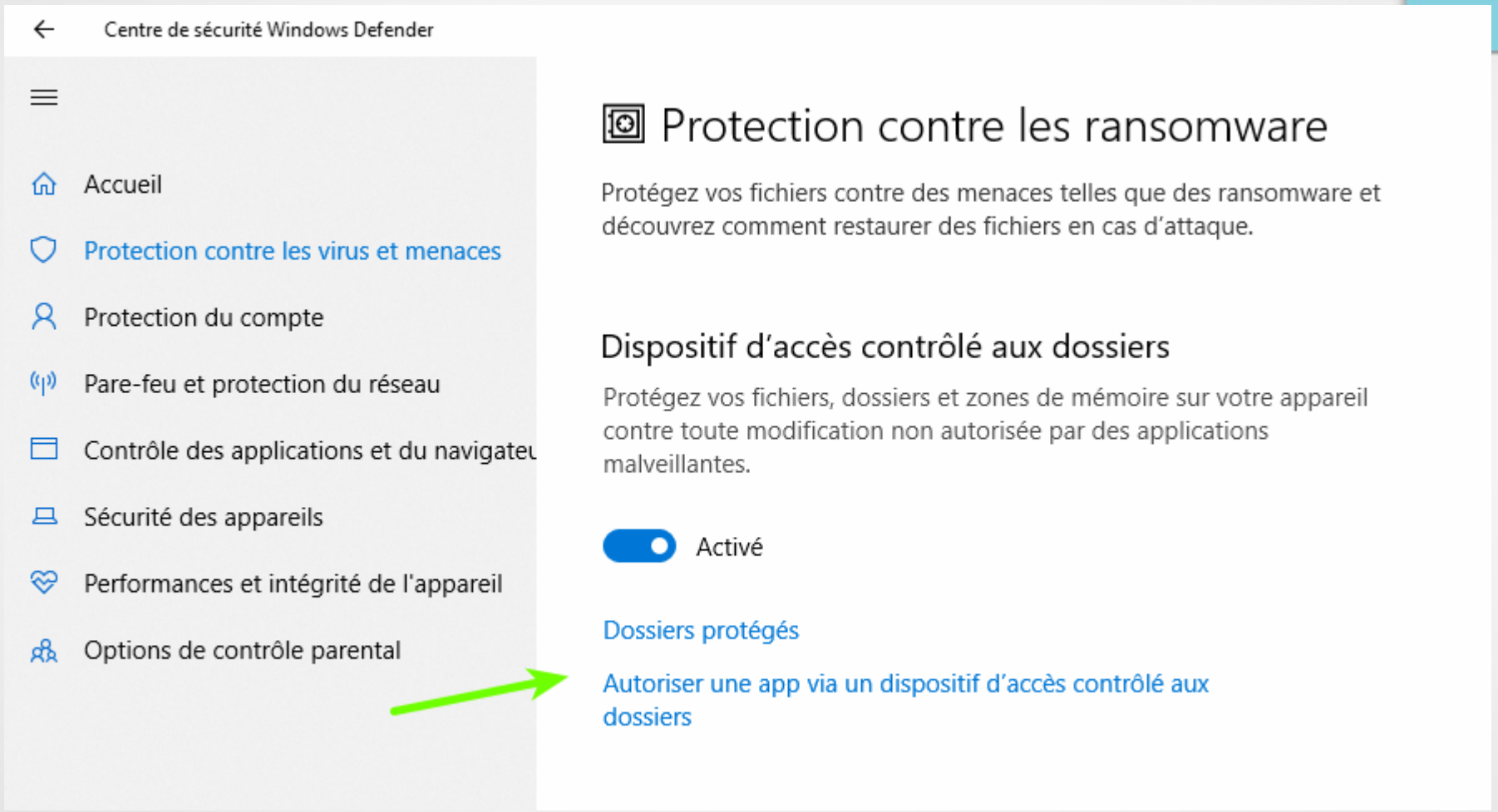


WINDOWS 10 : une solution ?





WINDOWS 10 : une solution ?



https://www.malekal.com/ransomwares/

Site gouvernemental:

Progression :

En Savoie aussi:

Mars 2021 :

1 entreprise sur le secteur de Montmélian :
Cryptage des données / Demande de rançon
40 serveurs cryptés / 10 PC windows
Nom du ransomware : RAGNAROK
Serveur de backup est lui-même chiffré.

Avril 2021 :

1 mairie et des entités associées :
Cryptage des données / Demande de rançon
70 serveurs cryptés / 16 PC windows
Nom du ransomware : AVADDON

L'origine des attaques : LA MESSAGERIE et MOTS DE PASSE TROP SIMPLE

La Section J3 CYBERCRIMINALITE du parquet de PARIS, face à l'augmentation de ce phénomène, fait systématiquement jouer sa concurrence nationale pour se saisir des faits.

Dans les deux cas, les parquets locaux ont été dessaisis, le C3N poursuit les investigations.

Et si c’est mon cas?:

Rappel et information :

La Section Opérationnelle de Lutte contre les Cybermenaces reste à votre écoute !

N’hésitez pas à les solliciter pour tout diagnostic de prévention Cyber !

Le groupement de Gendarmerie de Savoie est fort de 32 Correspondants NTECH (CNTECH) répartis dans les différentes brigades. Cette liste, évolutive, est consultable dans cette présentation plus complète !

Liste NTECH / CNTECH :

ANNUAIRES NTECH / CNTECH :

	Unité	Fonction	Nom	Prénom
GGD73	SOLC BDRIJ GGD73	NTECH	ALGRAIN	Eric
	SOLC BDRIJ GGD73	CNTECH	De Wilde	Thomas
CGD CHAMBERY	BR CHAMBERY	CNTECH	Beaulieu	David
	BR CHAMBERY	CNTECH	Calloud	Nicolas
	BP CHINDRIEUX	CNTECH	Pelabon	Gaétan
	BR CHAMBERY	CNTECH	Muffat	Nicolas
	BR CHAMBERY	CNTECH	Desporte	Guillaume
	BTA LE-CHATELARD	CNTECH	Barigand	Denis
	BTA CHAMBERY	CNTECH	Bouilly	Karl
	BTA LA-MOTTE-SERVOLEX	CNTECH	Le Meur	Rodolphe
	BTA VALGELON-LA-ROCHETTE	CNTECH	Olive	Charlotte
	BP LE PONT DE BEAUVOISIN	CNTECH	Turlure	David
	BTA CHALLES LES EAUX	CNTECH	Annerel	Anthony
	BP AIX LES BAINS	CNTECH	Combalot	Nicolas
	BP MONTMELIAN	CNTECH	Darosey	Yves
CGD ST-JEAN-DE-MAURIENNE	BTA MODANE	CNTECH	Cacciatore	Pierre
	BTA ST-JEAN-DE-MAURIENNE	CNTECH	Durupt	Julien
	BTA ST-JEAN-DE-MAURIENNE	CNTECH	Ghilardi	Philippe
	BTA VAL-CENIS	CNTECH	Mirgain	Maxence
	BR ST-JEAN-DE-MAURIENNE	CNTECH	Suzanne	Ludovic
	BTA ST-JEAN-DE-MAURIENNE	CNTECH	Didier	Nicolas
	BP VAL-D-ARC	CNTECH	Rouyer	Antoine
CGD ALBERTVILLE	BTA VAL-D-ISERE	CNTECH	Guillot	Alexandre
	BTA MOUTIERS	CNTECH	Gury	David
	BTA LES-BELLEVILLE	CNTECH	Larlet	Thomas
	BP GRESY-SUR-ISERE	CNTECH	Mongellaz	Cédric
	BTA MOUTIERS	CNTECH	Dufrene	Franck
	BTA BOURG-ST-MAURICE	CNTECH	Guggia	Pierre
	BR ALBERTVILLE	CNTECH	Ruffinatto	Nicolas
	BTA BEAUFORT	CNTECH	Arbault	Jérémy
	BTA AIME LA PLAGNE	CNTECH	Bollinger	Gilles
	BP ALBERTVILLE	CNTECH	Schifferling	Clément
EDSR73	PA STE-MARIE-DE-CUINES-FREJUS	CNTECH	Barbecot	Fabrice

Contact :

Groupement Gendarmerie Départementale de la SAVOIE

Cellule Prévention Technique de la Malveillance

28 rue de Sonnaz

73000 CHAMBERY

tél : 04-79-71-82-71

cptm.ggd73@gendarmerie.interieur.gouv.fr

Merci de votre attention !

Adjudant-chef ALGRAIN
NTECH - SOLC 73