



CYBERGEND  
NTECH

**CYBERCRIMINALITE,  
UN RISQUE AU QUOTIDIEN!**

INVESTIGATION & CRIMINALISTIQUE

**Groupement de Gendarmerie Départementale de la SAVOIE**

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

A futuristic, curved hallway with blue lighting and a grid ceiling. The hallway is illuminated with a vibrant blue light that creates a strong sense of depth and perspective. The ceiling is composed of a grid of rectangular panels, and the walls are also illuminated with the same blue light. The overall atmosphere is clean, modern, and high-tech.

# 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'infiltré 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 restore  
Use Tor Browser to  
If you have not been



Ce blocage  
illégal. Le  
dérogation  
On a relevé  
a "82.123.98"  
pornographi  
de violence  
avec les ele  
meme on a  
spam avec l



# Gendarmerie/ecops

**ATTENTION!**  
Votre ordinateur a été bloqué pour violation de la loi Française

**Gendarmerie nationale**

Les infractions suivantes ont été détectées:

- Le fait, en vue de sa diffusion, de faire, d'engager ou de transmettre des matériels pornographique impliquant des mineurs
- Spam
- Utilisation des logiciels en infraction avec les droits d'auteur
- Partager des fichiers multimédia en infraction avec les droits d'auteur

Pour débloquer votre ordinateur, vous devez payer 200 € dans les 3 jours prochains. Si vous ne payez pas dans le délai précisé, votre ordinateur sera confisqué et votre cas sera soumis au tribunal.

**ecops**

**ATTENTION!**  
Votre ordinateur a été bloqué pour violation de la loi Belgique

Les infractions suivantes ont été détectées:

- Le fait, en vue de sa diffusion, de faire, d'engager ou de transmettre des matériels pornographique impliquant des mineurs
- SPAM
- Utilisation des logiciels en infraction avec les droits d'auteur
- Partager des fichiers multimédia en infraction avec les droits d'auteur

Pour débloquer votre ordinateur, vous devez payer 200 € dans les 3 jours prochains. Si vous ne payez pas dans le délai précisé, votre ordinateur sera confisqué et votre cas sera soumis au tribunal.

Après le déblocage, nous recommandons que vous:

- Supprimez tous les fichiers multimédia en infraction avec les droits d'auteur
- Supprimez des logiciels en infraction avec les droits d'auteur
- Installez un logiciel anti-virus, si vous n'avez pas de virus
- Faire un scan anti-virus

Vous NE: Windows Seven Vous ETE: Windows Vista  
Vous adresse IP: Vous ville:

# Gema

**GEMA**

Access to your computer was denied.

Recently downloaded music tracks or other works, "various artists" have been detected on your PC. Any files being downloaded by the browser mentioned tracks were copied - that's why you a criminal offence in accordance with §104 of the Copyright Act (Urheberrechtsgesetz - URG).

Both copyrighted music tracks (downloaded from the Internet and copied) and illegal copies (downloaded from the Internet) are illegal under §104 of the Copyright Act (Urheberrechtsgesetz - URG) and prohibited by other regulations of copyright law in up to three years of imprisonment. Moreover, according to §104 of the Criminal Code the property is subject to forfeiture - if you carry forward the computer you have been forbidden from the above mentioned files downloading.

The system identification both of your person and that who uses your IP address and host name points to your address.

The infected and copied music were captured and copied to prevent copyright violation.

For information and confirmation of any other offences resulting from infringement of copyright law you should go to a nearby police station. The payment should be delivered through our financial partner - Paysafe.com. After the payment procedure is complete successfully your PC will be unlocked automatically.

For the completion of the above mentioned payment send your PaysafeCard's payment ID number to our service center.

GEMA holds legal rights and permanently contacts with state legislation.

**paysafecard**  
pay cash, pay safe.

# Gimemo

**Police Nationale**

bloqué!

Vous avez été bloqué pour avoir téléchargé des fichiers illégaux. Pour débloquer votre ordinateur, vous devez payer 200 € dans les 3 jours prochains. Si vous ne payez pas dans le délai précisé, votre ordinateur sera confisqué et votre cas sera soumis au tribunal.

«Cops est une initiative de la Federal Computer Crime Unit of the Public Judiciary Federal (CCU) et du Service Public Fédéral Economie, P.M.E., Classes moyennes et Jeunesse»

Disposez l'ash Paysafecard en facile

Vous trouvez l'ash Paysafecard prêt de chez vous, en Belgique chez un grand nombre de stations services, de supermarchés et de bureaux de tabac.

**U kash**

- Trouvez le point de vente le plus proche
- Demandez l'ash Paysafecard 20€, 50€, 100€, 200€
- Obtenez votre code l'ash de 19 chiffres (Paysafecard de 18 chiffres)

# Goldenbaks

**Goldenbaks**

Activité illécite détectée!

Un message d'information de la police a été envoyé à votre ordinateur. Ce message a été envoyé à votre ordinateur parce que vous avez téléchargé des fichiers illégaux. Pour débloquer votre ordinateur, vous devez payer 200 € dans les 3 jours prochains. Si vous ne payez pas dans le délai précisé, votre ordinateur sera confisqué et votre cas sera soumis au tribunal.

Vous pouvez acheter un voucher l'ash?

Vous pouvez acheter un voucher l'ash chez un grand nombre de stations services, de supermarchés et de bureaux de tabac.

**U kash**

# Silence locker

**Silence locker**

**ATTENTION!**  
Pour des raisons de sécurité, votre système Windows a été bloqué.

Votre système informatique a été infecté par un virus. Ce virus a détecté des fichiers illégaux sur votre ordinateur. Pour protéger votre système informatique et éviter la perte de données, nous avons bloqué votre système Windows.

Sélectionnez la méthode préférable de paiement:

- U kash** POSSIBLE ✓
- paysafecard** POSSIBLE ✓

Votre système informatique a été infecté par un virus. Ce virus a détecté des fichiers illégaux sur votre ordinateur. Pour protéger votre système informatique et éviter la perte de données, nous avons bloqué votre système Windows.

Cette mise à jour payée est destinée également pour les systèmes infectés. Cette mise à jour va protéger complètement votre système contre les virus et les logiciels malveillants, va stabiliser votre système informatique et va éviter la perte de données.

**Office Central de Lutte contre la Criminalité Liée aux Technologies de l'Information et de la Communication**

Activité illécite détectée!

Un message d'information de la police a été envoyé à votre ordinateur. Ce message a été envoyé à votre ordinateur parce que vous avez téléchargé des fichiers illégaux. Pour débloquer votre ordinateur, vous devez payer 200 € dans les 3 jours prochains. Si vous ne payez pas dans le délai précisé, votre ordinateur sera confisqué et votre cas sera soumis au tribunal.

Vous pouvez acheter un voucher l'ash?

Vous pouvez acheter un voucher l'ash chez un grand nombre de stations services, de supermarchés et de bureaux de tabac.

**U kash**

# Reveton

**BUNDESPOLIZEI**

**ACHTUNG!!!**

Achtung!!!

Ein Warnungsschreiben wurde an Ihren Computer geschickt. Diese Warnung wurde geschickt, weil Sie illegale Dateien heruntergeladen haben. Um Ihren Computer zu entlockern, müssen Sie 200 Euro bezahlen. Wenn Sie nicht bezahlen, wird Ihr Computer beschlagnahmt und Ihr Fall dem Gericht übergeben.

Sie können ein U kash kaufen?

Sie können ein U kash kaufen in den meisten Supermärkten, Tankstellen und Tabakläden.

**U kash**

# AlertLock

**sacem**

**Police Nationale**

Votre ordinateur a été verrouillé.

Un message d'information de la police a été envoyé à votre ordinateur. Ce message a été envoyé à votre ordinateur parce que vous avez téléchargé des fichiers illégaux. Pour débloquer votre ordinateur, vous devez payer 200 € dans les 3 jours prochains. Si vous ne payez pas dans le délai précisé, votre ordinateur sera confisqué et votre cas sera soumis au tribunal.

Vous pouvez acheter un voucher l'ash?

Vous pouvez acheter un voucher l'ash chez un grand nombre de stations services, de supermarchés et de bureaux de tabac.

**U kash**

**ACCFDISA**

**Warning: Access to your computer is limited.**

**WHY?**  
Your computer was detected making (open) adverts illegal sites with child pornography, which (violates) law and harm other network users.

Probably your computer has been infected and as a result our service blocked access to your computer, including a fully networked access (except for our staff).

As the virus sends the illegal spam mail is very dangerous and modifies itself every 48 hours, including removing our program protection, you have 48 hours, otherwise we will remove all protection program data including the operating system and all your files without the possibility of recovery.

To solve this problem you need to buy and send sms with MoneyPal or Paysafecard or U kash code (100€ or 200€) and your Reference Number: #18722101648 to the special Service phone number: +18722101648 or email: antispam@cyber-services.com

You can buy MoneyPal card at the nearest stores - Walgreens, Walmart, CVS pharmacy, Kmart, SevenEleven, Rite Aid or go to www.moneypal.com to find location stores near you.

To find Paysafecard and location stores near you visit www.paysafecard.com or U kash at www.ukash.com

After that our experts within 1-3 hours will do scan and clean up your computer from viruses sending out spam and send you sms on the cell phone or email (from which you send card code and your reference number) control code (which unlocks your PC) that must be enter here.

Do not attempt in any way to remove the protection program, because if you try to do this, your operating system Windows will be unstable.

Anti-Cyber Crime Department of Federal Internet Security Agency (ACCFDISA)

# Progression :



# Les infractions :

ARTICLES	LIBELLÉ
<a href="#">Art. 312-1 du Code Pénal</a>	<b>Extorsion</b> : 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.
<a href="#">Art. 323-1 du Code Pénal</a>	<b>Atteinte STAD</b> : 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 liés 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 caractères 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 vérifié 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

Centre de sécurité Windows Defender

Votre appareil est protégé.

Dernière analyse des menaces : 15/10/2017  
Dernière mise à jour de définition de menaces : 18/10/2017  
Dernière analyse d'intégrité : 18/10/2017

- Protection contre les virus et menaces  
Aucune action requise.
- Performances des appareils et intégrité  
Aucune action requise.
- Pare-feu et protection du réseau  
Aucune action requise.
- Contrôle des applications et du navigateur  
Aucune action requise.
- Options de contrôle parental  
Gérez la façon dont votre famille utilise ses appareils.



# WINDOWS 10 : une solution ?

← Centre de sécurité Windows Defender

- Accueil
- Protection contre les virus et menaces**
- Protection du compte
- Pare-feu et protection du réseau
- Contrôle des applications et du navigateur
- Sécurité des appareils
- Performances et intégrité de l'appareil
- Options de contrôle parental

## Protection contre les virus et menaces

Affichez l'historique des menaces, recherchez les virus et autres menaces, indiquez les paramètres de protection et obtenez des mises à jour de la protection.

### Historique des menaces

Dernière analyse : 11/05/2018 (analyse rapide)

0 42624

Menaces trouvées Fichiers analysés

Analyser maintenant

[Exécuter une nouvelle analyse avancée](#)

### Paramètres de protection contre les virus et menaces


Aucune action requise.

### Mises à jour de la protection contre les virus et menaces

Les définitions de la protection sont à jour.  
Dernière mise à jour : 16:31 jeudi 17 mai 2018

### Protection contre les ransomware

Aucune action requise.



← Centre de sécurité Windows Defender

## Envoi automatique d'un échantillon

Envoyez des échantillons de fichier à Microsoft pour vous protéger et protéger les autres utilisateurs contre d'éventuelles menaces. Nous vous informerons si le fichier dont nous avons besoin est susceptible de contenir des informations personnelles.

Activé


[Déclaration de confidentialité](#)  
[Envoyer un échantillon manuellement](#)

## Dispositif d'accès contrôlé aux dossiers

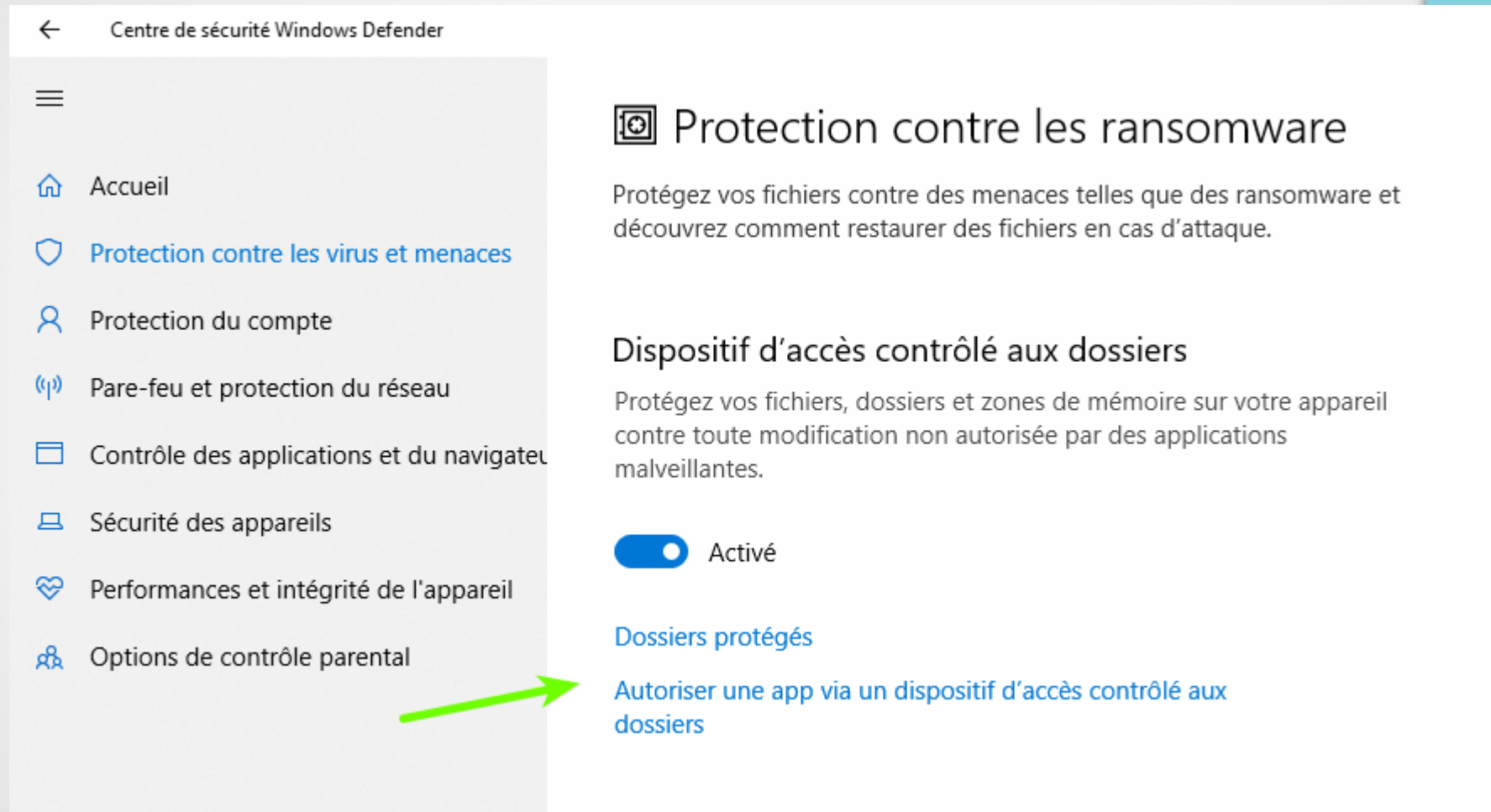
Protégez vos fichiers et dossiers contre la modification non autorisée par des applications malveillantes.

Activé

[Dossiers protégés](#)  
[Autoriser une app via un dispositif d'accès contrôlé aux dossiers](#)



# WINDOWS 10 : une solution ?



The screenshot shows the Windows Defender Security Center interface. On the left is a navigation pane with the following items: Accueil, Protection contre les virus et menaces (highlighted in blue), Protection du compte, Pare-feu et protection du réseau, Contrôle des applications et du navigateur, Sécurité des appareils, Performances et intégrité de l'appareil, and Options de contrôle parental. A green arrow points from the 'Options de contrôle parental' item to the 'Autoriser une app via un dispositif d'accès contrôlé aux dossiers' link in the main content area.

Centre de sécurité Windows Defender

## Protection contre les ransomware

Protégez vos fichiers contre des menaces telles que des ransomware et découvrez comment restaurer des fichiers en cas d'attaque.

### Dispositif d'accès contrôlé aux dossiers

Protégez vos fichiers, dossiers et zones de mémoire sur votre appareil contre toute modification non autorisée par des applications malveillantes.

Activé

Dossiers protégés

[Autoriser une app via un dispositif d'accès contrôlé aux dossiers](#)

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

# Site gouvernemental:

**CYBERMALVEILLANCE.GOUV.FR**  
Assistance et prévention du risque numérique

ESPACE PRESTATAIRE    MON ESPACE    🔍

## ASSISTANCE ET PRÉVENTION DU RISQUE NUMÉRIQUE AU SERVICE DES PUBLICS

COMPRENDRE LES MENACES ET AGIR    ADOPTER LES BONNES PRATIQUES    L'ACTUALITÉ DE LA CYBERMALVEILLANCE    **ASSISTANCE** 🛠️

<https://www.cybermalveillance.gouv.fr/>

### VICTIME D'UN ACTE DE CYBERMALVEILLANCE ?

Cybermalveillance.gouv.fr a pour missions d'aider les entreprises, les particuliers et les collectivités victimes de cybermalveillance, de les informer sur les menaces numériques et de leur donner les moyens de se défendre.

# 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
<b>GGD73</b>	SOLC BDRJ GGD73	NTECH	ALGRAIN	Eric
	SOLC BDRJ GGD73	CNTECH	De Wilde	Thomas
<b>CGD CHAMBERY</b>	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
<b>CGD ST-JEAN- DE-MAURIENNE</b>	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
<b>CGD ALBERTVILLE</b>	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-AURICE	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
<b>EDSR73</b>	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](mailto:cptm.ggd73@gendarmerie.interieur.gouv.fr)



**Merci de votre attention !**

**Adjudant-chef ALGRAIN  
NTECH - SOLC 73**