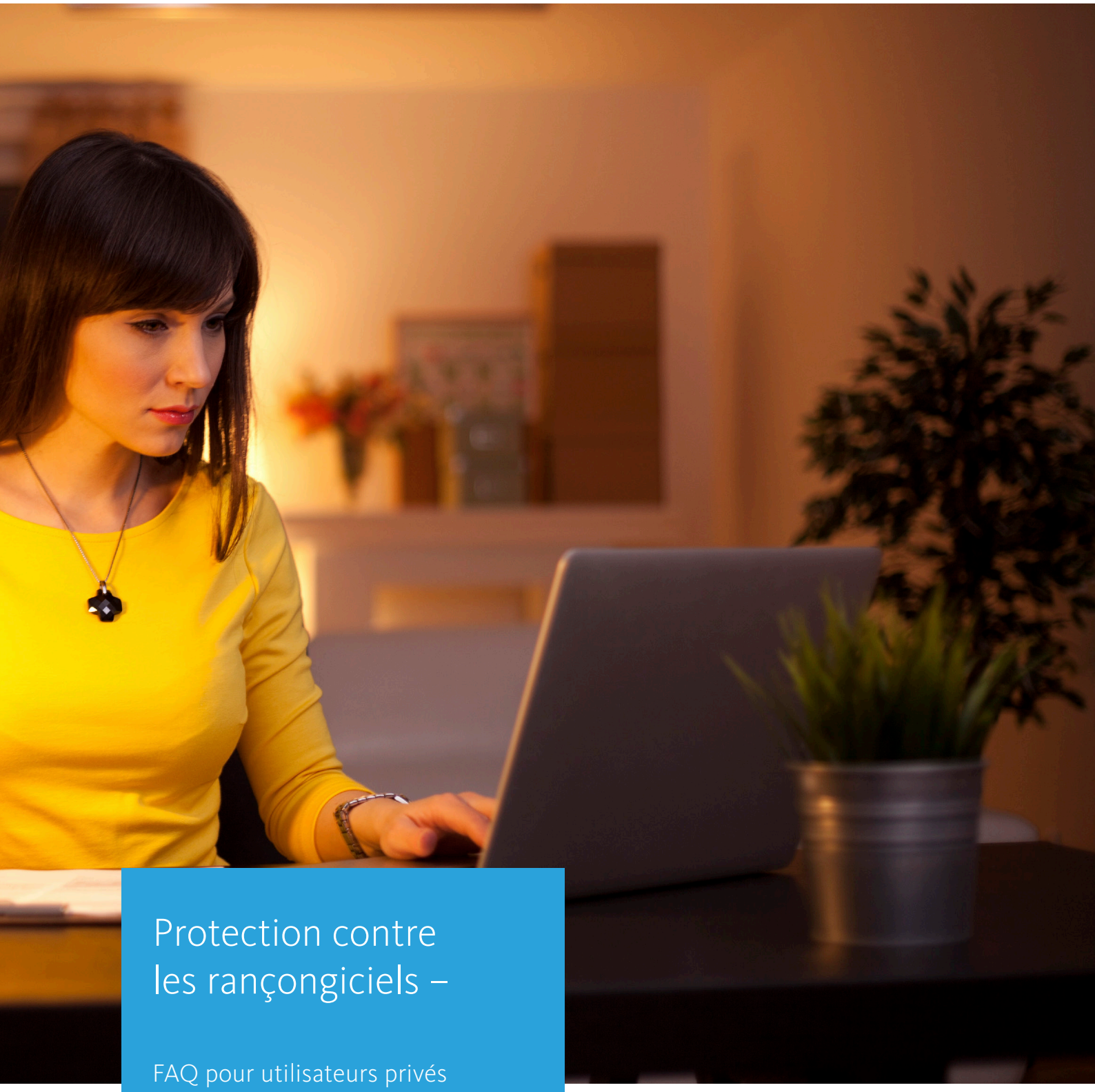
Avira



Protection contre les rançongiciels –

FAQ pour utilisateurs privés

www.avira.fr

1. Que sont les rançongiciels ?

Un rançongiciel est un logiciel de chantage qui chiffre les photos, vidéos, fichiers de musique et autres sur l'ordinateur ou bloque l'accès au système tout entier. La victime doit généralement s'acquitter d'une « rançon » pour recouvrer l'accès à ses fichiers et appareils.

2. Quels sont les différents types de rançongiciels ?

Il existe trois types de rançongiciels : le logiciel de rançon à chiffrement, qui chiffre les fichiers (en les rendant inutilisables), le rançongiciel de type Lockscreen qui bloque l'écran, et enfin le rançongiciel de type Master Boot Record, qui chiffre le secteur de démarrage de la table de partition pour les plateformes BIOS.

3. Que font les rançongiciels ?

Les rançongiciels sont distribués la plupart du temps par le biais d'e-mails ou d'exploits. Dans le premier cas, le cybercriminel envoie un e-mail d'hameçonnage doté d'une pièce jointe, par exemple à une organisation précise. L'utilisateur peu méfiant ouvre cette pièce jointe (document Word ou fichier JavaScript) car le texte contenu dans l'e-mail paraît fort vraisemblable aux yeux de la victime. À l'ouverture du document Word, un message invite l'utilisateur à activer des macros afin d'afficher correctement le contenu. Seule l'activation de macros permet de télécharger complètement et discrètement le rançongiciel à travers l'exécution d'un script caché et via un téléchargement automatique intempestif.

4. Que se passe-t-il lorsqu'un ordinateur est infecté par un rançongiciel ?

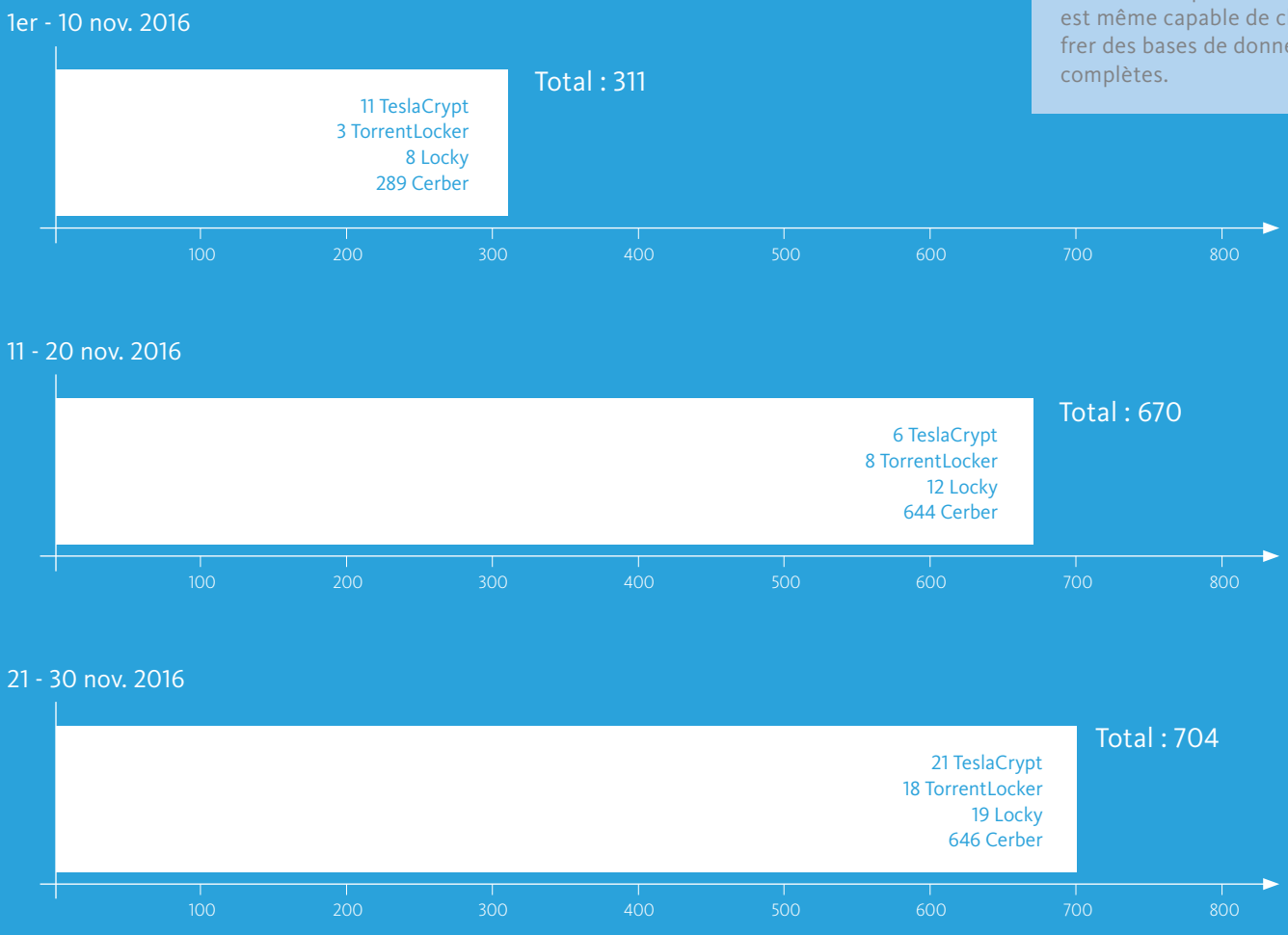
Le crypto-rançongiciel chiffre tous les fichiers existants comme les images, vidéos, fichiers Office, etc. Il chiffre également les données sur les disques amovibles ou services Cloud connectés à ce moment précis. Une fois tous les fichiers chiffrés et pourvus d'une extension de fichier spécifique, le rançongiciel exige une certaine somme d'argent en échange du déchiffrement de tous les fichiers. La « rançon », qui doit être réglée le plus souvent en bitcoins sur un site Internet spécial dans le darknet, peut s'élever à plusieurs milliers d'euros. Le rançongiciel qui bloque l'écran d'accueil pour empêcher l'accès de l'utilisateur à son appareil, lui réclame également une rançon pour débloquer l'écran, par exemple via l'achat d'une carte UKash ou d'un autre moyen de paiement numérique.

5. Quel est le niveau de menace actuel ?

Les attaques de rançongiciel vont continuer car ce modèle d'affaires s'avère très lucratif pour les cybercriminels et nombre de victimes se résignent à payer – le plus souvent dans la plus grande discrétion. Ce modèle d'affaires persistant bénéficie d'améliorations constantes par les cybercriminels. Dans les entrefaites, il fait de plus en plus appel aux langages de script (VBS, JavaScript, Powershell) en plus des programmes Windows (Portable Executable), et ce afin de contrecarrer leur classification en tant que logiciels malveillants. Les rançongiciels sévissent également désormais sur les appareils Android : l'utilisateur ne peut pas utiliser son smartphone tant qu'il n'a pas réglé la rançon par le biais d'un SMS. Les utilisateurs Mac sont notamment concernés par le rançongiciel KeRanger. D'autres espèces sont connues sous les noms de « Petya », « FBI Ransomware » ou « Locky », qui ont infecté d'ores et déjà des millions d'ordinateurs Windows.

Les rançongiciels – une menace permanente

Occurrences d'une sélection de chevaux de Troie de chiffrement en novembre 2016 | Source : ransomwaretracker.abuse.ch



Cerber

Une espèce particulièrement dangereuse de rançongiciel correspond à la famille Cerber, qui est distribuée en général sous la forme de pièces jointes à des e-mails. Sa version la plus récente est même capable de chiffrer des bases de données complètes.

6. Quelles sont les technologies de sécurité mises en œuvre par Avira pour lutter contre les rançongiciels ?

Pour réduire et freiner les facteurs de risque favorisant les rançongiciels, une approche de sécurité multicouche est requise. Avira a développé des technologies efficaces pour la détection et la lutte en temps réel contre les logiciels malveillants. Nous misons sur des technologies de pointe comme l'apprentissage automatique ou l'intelligence artificielle, la réputation, la détection basée sur le comportement et les analyses en temps réel pour classifier les fichiers inconnus. Nos clients ont systématiquement accès aux données les plus récentes sur notre Cloud. À l'avenir, les systèmes assistés par l'intelligence artificielle seront appelés à jouer un rôle essentiel pour l'analyse et la classification des logiciels malveillants encore inconnus.

Cinq conseils pour vous protéger efficacement contre les rançongiciels :

1

Installez un logiciel antivirus sur tous vos appareils	Utilisez une solution de protection antivirus sur l'ensemble de vos appareils (PC, Mac, smartphones et tablettes).	Avira détecte et bloque toutes les menaces connues de rançongiciels.

2

Attention aux e-mails et liens malveillants	Ouvrez seulement les pièces jointes des e-mails dont vous connaissez les expéditeurs.	Cliquez exclusivement sur les liens et publications de médias sociaux de confiance.

3

Maintenez tous vos programmes à jour

Installez toujours les mises à jour et les correctifs logiciels sans délai. Cela complique la tâche au rançongiciel, qui peut alors difficilement infecter l'ordinateur. Veillez à ce que les logiciels soient à jour sur tous vos appareils afin de limiter les points faibles. Si vous ne savez pas comment maintenir vos logiciels constamment à jour et éviter ainsi les failles de sécurité, faites appel à un outil tel qu'**Avira Software Updater**. Il vous avertit de la présence de logiciels obsolètes et prend en charge la recherche des mises à jour.

4

Créez régulièrement des sauvegardes de données

Nous vous recommandons de sauvegarder vos données régulièrement dans le Cloud ou sur un disque dur externe. En cas de chiffrement de vos fichiers par un rançongiciel, vous pourrez alors formater votre disque dur sans aucune hésitation car vous aurez sauvegardé vos données sur un emplacement externe.

5

Utilisez une protection de navigateur ou mieux : un navigateur sécurisé comme Avira Scout

L'extension de navigateur offerte gratuitement par Avira bloque les sites Internet nuisibles et protège votre vie privée.

Avira Scout bloque automatiquement les sites Internet malveillants et les pages d'hameçonnage et contient une fonction contre le suivi. Ceci place le navigateur d'Avira parmi les rares du marché à ne pas collecter des données sur vos pages visitées sur Internet, vos téléchargements et vos achats en ligne.

À propos d'Avira

Avira, entreprise affichant une croissance supérieure aux mains d'une même famille depuis 1986, a été fondée à Tettnang, sur les hauteurs du lac de Constance, par le pionnier de la sécurité informatique Tjark Auerbach pour devenir l'un des employeurs majeurs de la région.

Depuis déjà trois décennies, Avira propose à ses clients des solutions de sécurité développées en propre pour se prémunir contre les menaces circulant sur Internet, les attaques de logiciels malveillants, les programmes nuisibles et le vol de données. Plus de 100 millions d'utilisateurs – dont un grand nombre de micro-entreprises, de petites entreprises et d'utilisateurs à domicile – font confiance au logiciel d'Avira et apprécient sa fiabilité, ses performances et sa convivialité.

Avira occupe la seconde place parmi les éditeurs de logiciels antivirus leaders dans le monde. L'entreprise dirigée par Travis Witteveen abrite ses propres laboratoires antivirus et répond toujours présente quand il s'agit d'affirmer sa culture de l'innovation et sa productivité en développant des technologies de sécurité tournées vers l'avenir. La Protection temps réel par détection des logiciels malveillants basée sur le Cloud ou la console web Online Essentials en sont les solutions phares.

Avira collabore étroitement avec l'Office fédéral allemand de la sécurité des technologies de l'information et compte parmi les membres fondateurs de l'initiative « IT-Security made in Germany ».

L'expérience engrangée par Avira et ses produits et services maintes fois primés sont mis au service des personnes pour qu'elles puissent évoluer librement et en toute sécurité dans le monde numérique.

Mais Avira ne s'arrête pas là et se soucie également de la sécurité dans le monde réel : la fondation Auerbach, du nom du fondateur de l'entreprise, soutient les projets d'utilité publique et à vocation sociale, et encourage déjà plus de 300 projets dans les domaines de la formation et de l'éducation, de l'enfance, de la jeunesse et de la famille, de l'aide aux personnes âgées et handicapées ainsi que de l'art et de la culture.

Avira

© 2016 Avira GmbH & Co. KG. Tous droits réservés.
Nos conditions générales de ventes (CGV) sont
disponibles sur Internet : www.avira.com

Avira Operations GmbH & Co. KG
Kaplaneiweg 1 | 88069 Tettnang
Allemagne
Téléphone : +49 7542-500 0

Sous réserve d'erreurs et de modifications techniques. Version : décembre 2016

PROTECTING PEOPLE
IN THE CONNECTED WORLD

www.avira.fr