



LES ATTAQUES DE CRYPTOMALWARE

Kaspersky Lab France

SOMMAIRE

- 3 VOS DONNÉES PRISES EN OTAGE
EVOLUTION DES CRYPTOMALWARE
- 17 COMMENT SE PRÉMUNIR DE CES ATTAQUES
RECOMMANDATIONS
- 25 LES TECHNOLOGIES KASPERSKY LAB
PROTECTION CONTRE LES CRYPTOMALWARE

VOS DONNÉES PRISES EN OTAGE

EVOLUTION DES CRYPTOMALWARE

Des bloqueurs d'écrans avec demande de rançon et des outils de chiffrement évolués

DÉFINITION

« Un **ransomware**, ou rançongiciel, est un logiciel malveillant qui prend en otage des données personnelles. Pour ce faire, un rançongiciel chiffre des données personnelles puis demande à leur propriétaire d'envoyer de l'argent en échange de la clé qui permettra de les déchiffrer. »

source : wikipedia.org



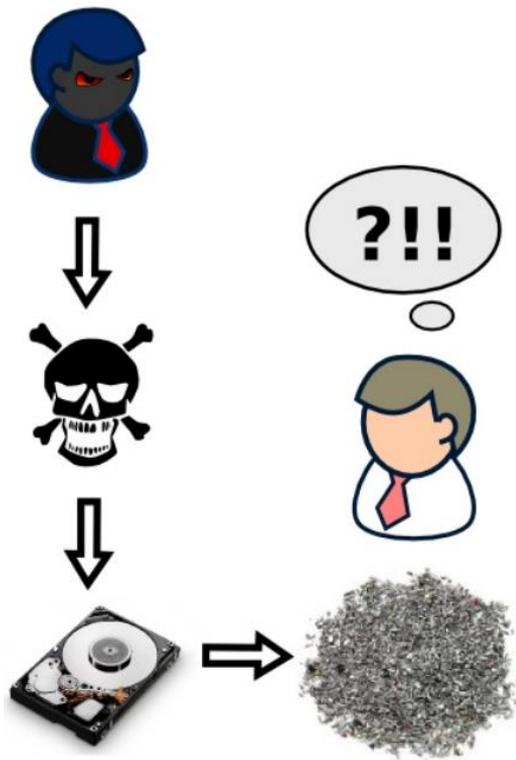
1. System Lockers



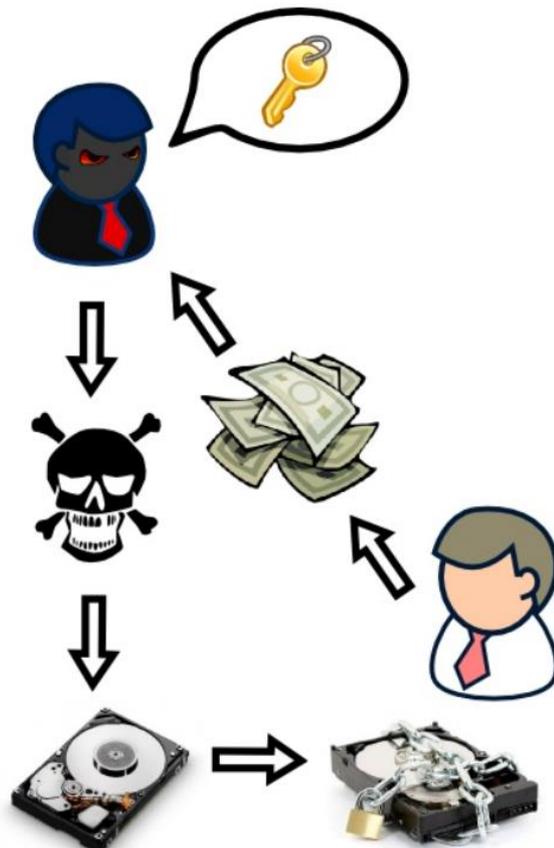
2. Data Encoders

POURQUOI LES RANSOMWARE

Malware destructeur « classique »



Ransomware



GPCODE : LE 1ER RANSOMWARE

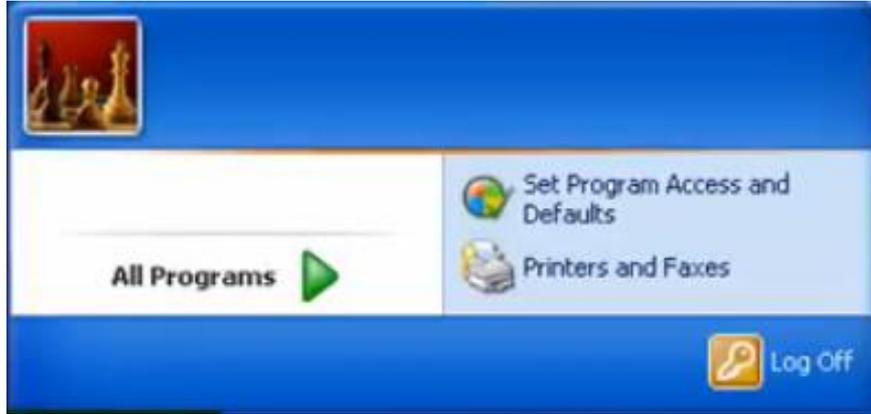
```
Dane do zestawienia.txt - Notatnik
Plik Edycja Format Widok Pomoc
PGPcoder 00000000003200ã-KYÜG00²0SN4ÆÜ~'vj@,&0PuÖH0k†A>R6*nBæšž2
Zâo;%0]`iÆe00²0ÆN4ÆÜ}'ui-0%ÜYqÖI0a...'=Q5)mAâ™01• I!Eyy00é-0¥Y]ñUE
I!Eyy00é-0¥Y]ñUE0á09%ñu0iÆe00±0%M;Àù}'ui-0%ÜYqÖI0a...'=Q5)mAâ™01•
...'=Q5)mAâ™01• I!Eyy00é-0¥Y]ñUE0á09%ñu0iÆe00±0%M;Àù}'ui-0%ÜYqÖI
I!Eyy00é-0¥Y]ñUE0á09%ñu0iÆe00±0%M;Àù}'ui-0%ÜYqÖI0a...'=Q5)mAâ™01•
...'=Q5)mAâ™01• I!Eyy
I"Fz00é.0 Z^òvÑ'00hÜ
I1Fz00é.0 Y]0VÉZâ0:%
I"Fz0æ÷ê.0 Z^æwÉZâ0:%
I"Fz0Bpê.0 Z^"AÉZ00:%
I"Fz0pê.0 Z^,^ÉZâ0:%
I"Fz00é.0 Z^âwÉZâ0:%
I"Fz00é.0 Z^æwÉZâ0:%
I"Fz0pê.0 Z^0xÉZâ0:%
I"r-l..0ã 0 Z^0dÉZâ0:0
```

```
readme.txt - Notatnik
Plik Edycja Format Widok Pomoc
Some files are coded by RSA method.
To buy decoder mail: dervish34@rambler.ru
with subject: RSA 5 68243170728578411
```

Emergence des premiers codes malicieux maître-chanteurs en Russie.

- Décembre 2004 : 1^{ère} variante de Gpcode
- Juin 2005 : nouvelle vague d'attaques sur l'Internet Russe après + de 25 modifications du malware
- Janvier 2006 : 1^{ère} utilisation de l'algorithme de chiffrement public RSA 56 bit
- Avril 2006 : Nouvelles variantes basée sur RSA 67 bit
- 6 Juin 2006 : la longueur de la clé atteint 330 bit
- 7 Juin 2006 : nouvelle variante avec une clé de 660 bit.

KROTTEN : BLOQUEUR D'ÉCRAN



Développement de la technique de chantage viral.

- Trojan modifiant la base de registre système de Windows afin de limiter les actions de l'utilisateur
 - Blocage de l'accès à l'éditeur de registre et au gestionnaire des tâches
 - Empêche la fermeture des navigateurs
 - Bloque l'accès aux configurations des fichiers et dossiers
 - Modifie le contenu du menu « Démarrer »
 - Bloque le lancement de l'invite de commande DOS, etc.



CRYZIP / MAYARCHIVE : L'ARCHIVAGE FORCÉE

How to pay to get your information back.

1. click on this link to open your free e-gold account - the first screen is the e-gold "terms and conditions" page. You need to agree to these by clicking on the "I AGREE" button on the bottom on the page.
2. On the next page is the sign up form:
 1. "Account name" - here is where you name your account - tip: make it easy to remember (as you will be asked for it) and reasonably short, example, "John's e-gold", "My Money e-gold" or perhaps "Felix" (whatever you like, just make it easy for you to remember it).
 2. "User Name" - here just repeat the account name (from 1 above).
 3. "Point of Contact" - this is where you put our name, address, phone number and email address (any email address can be used here but it is recommended you use your ISP address - not a free hotmail, etc address).
It is also recommended your also include a fax number (don't have a fax number? This company offers free fax to email services). Try and make it as easy as possible for e-gold to contact you.
 4. "Passphrase" - this is the most important piece of information connected to any e-gold account. We can not stress enough how important it is that your passphrase is kept safe and secure.
 5. "Turing Number Entry" - type the 6 numbers you see there into the box below.
 6. The last step click "Open"

Une autre technique de chantage.

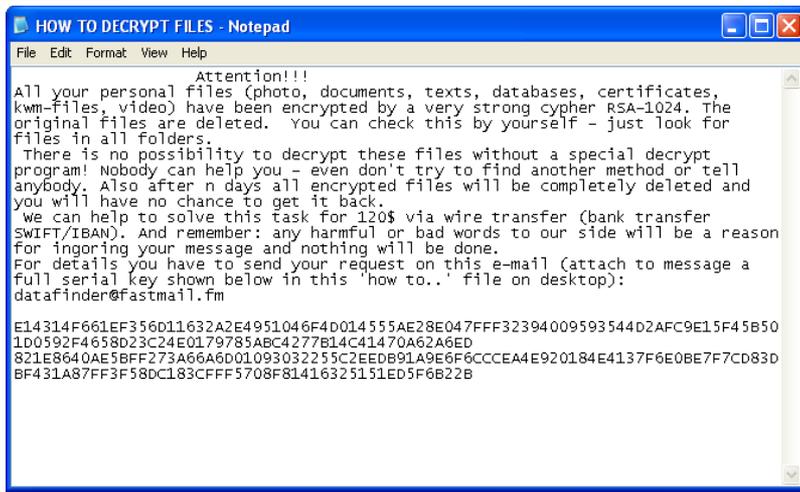
- Trojan place les fichiers personnels dans des archives ZIP protégées par mot de passe
- Mot de passe supérieur à 10 caractères
- Demande de rançon de 300\$

GPCODE : LE RETOUR



Nouvelle vague d'infection .

- Juin 2008 : Utilisation de RSA 1024 bit
- Déchiffrement impossible des données
- Utilisation possible de l'outil PhotoRec pour restaurer les données supprimées
- Novembre 2010 : nouvelle variante basée sur RSA-1024 et AES-256



LES FAUX MESSAGES DE VERROUILLAGE



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



Les infractions suivantes ont été détectées:

- Le fait, en vue de sa diffusion, de fixer, d'enregistrer 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 prochaines. Si vous ne payez pas dans dans le délai précisé, votre ordinateur sera confisqués et votre cas sera soumis au tribunal.

Vous pouvez payer l'amende avec l'aide des vouchers Ukash ou Paysafecard. Acheter les vouchers par Ukash ou Paysafecard de 200 €. Ensuite, ouvrez le tab «Payer amende», remplir le forme avec les codes et valeurs des vouchers, et clique sur le bouton «Payer amende». Votre ordinateur sera débloqué dans les 24 heures suivantes.

Victimisation de l'Internaute.

- Blocage de l'écran complet (ou du navigateur) avec affichage d'une demande de rançon
- Usurpation d'une autorité (Gendarmerie, Police, HADOPI, OCLCTIC)
- Détection de contenus illicites
- Affichage d'informations personnelles (adresse IP, Pays, Ville, FAI, etc.) et détournement de la webcam pour inclure une photo dans la demande de rançon
- Verrouillage du système : gestionnaire des tâches, explorateur windows, mode sans échec

LE BLOCAGE DU MBR

```
Your PC is blocked.
All the hard drives were encrypted.
Browse www.sakru to get an access to your system and files.
Any attempt to restore the drives using other way will
lead to inevitable data loss !!!
Please remember Your ID: 77██████,
with its help your sign-on password will be generated.Enter password:_
```

```
00 00 00 00-00 00 00 00-00 00 00 00-00 00 55 AA Uκ
EB 04 68 6A-6D 63 FB E8-4E 01 BE 7A-7E E8 21 01 w♦hjmс√wN@jz~w!@
BE BA 7F E8-1B 01 BB 7A-7E 31 FF B4-10 CD 16 80 j||Δw+@jz~1 |>=A
FC 01 74 2B-80 FC 0E 74-34 80 FC 1C-74 3D 80 FC N@t+ANfAt4ANt=AN
E0 74 38 3C-21 72 E4 3C-7E 77 E0 83-FF 10 73 DB pt8<?rφ<~wpΓ >S█
88 01 47 53-B8 2A 0E BB-07 00 CD 10-5B EB CC 85 M@GSq*βη• => [w|E
FF 74 C8 4F-B0 20 88 01-E8 E8 00 EB-F2 85 FF 74 tLQ M@ww wCE t
BA 4F B0 20-88 01 E8 DA-00 EB B0 53-B8 0D 0E BB ||O M@w Γ wSqJβη
07 00 CD 10-B8 0A 0E BB-07 00 CD 10-5B B0 20 83 • => q|βη• => I | Γ
FF 10 73 05-88 01 47 EB-F6 B1 10 31-D2 BE 7A 7E >S M@Gw9 >1πjz~
FC AC E8 D3-00 FE C9 75-F8 3B 16 FA-7F 74 13 BE Hvw H Γu°; - Δt!!j
DA 7F E8 8C-00 E8 B0 0E BB-07 0E 79 7E-0F 85 60 FF ΓΔwM w ||βy~wE
EB 6B BB 00-7E B9 05 00-BA 80 00 B8-01 02 CD 13 wκj ~|s ||A q@=!!
73 08 BE 81-7D E8 69 00-EB FE BF FE-7F 81 3D BE s□β>wi w|j Δβ=j
AF 74 08 BE-8D 7D E8 58-00 EB FE BA-55 AA 89 15 nt□H>wX w||UκβS
B9 01 00 BA-80 00 B8 01-03 CD 13 73-08 BE 81 7D |@ ||A q@v=!!s□β>
E8 3E 00 EB-FE B9 00 02-BF 00 7E 30-C0 F3 AA BB w> w|: |@ ~° ekj
00 7E B9 02-00 BA 80 00-08 01 03 CD-13 B9 03 00 ~|@ ||A q@v=!!|v
B8 01 03 CD-13 B9 05 00-08 01 03 CD-13 B8 40 00 q@v=!!|s q@v=!!q@
8E C0 BB 72-00 31 C0 26-89 07 68 FF-FF 68 00 00 0 L Γr 1 L&N°h h
CB 60 FC AC-20 C0 74 09-BB 07 00 B4-0E CD 10 EB π Hm t@j• |β>w
F2 61 C3 60-BB 07 00 B8-08 0E CD 10-B8 20 0E CD Gαt' π• q@β> j β=
10 B8 08 0E-CD 10 61 C3-60 BB 07 00-B8 0D 0E CD > j β>a' π• q Jβ=
10 B8 0A 0E-CD 10 61 C3-50 51 88 C4-30 C0 31 C2 > j β>a' PQM-0 L T
B1 08 D1 E2-73 04 81 F2-21 10 FE C9-75 F4 59 58 █ T s ♦ β G ! > | Γ u Y X
C3 49 2F 4F-20 65 72 72-6F 72 0D 0A-00 44 61 74 |I/O error J@ Dat
61 20 63 6F-72 72 75 70-74 65 64 0D-0A 00 00 00 a corrupted J@
```

Blocage au démarrage de la machine.

- Après 3 mots de passe incorrects la machine redémarre et le même message apparaît
- Les données ne sont pas chiffrées contrairement à ce qu'indique le message
- Demande de rançon de 100\$

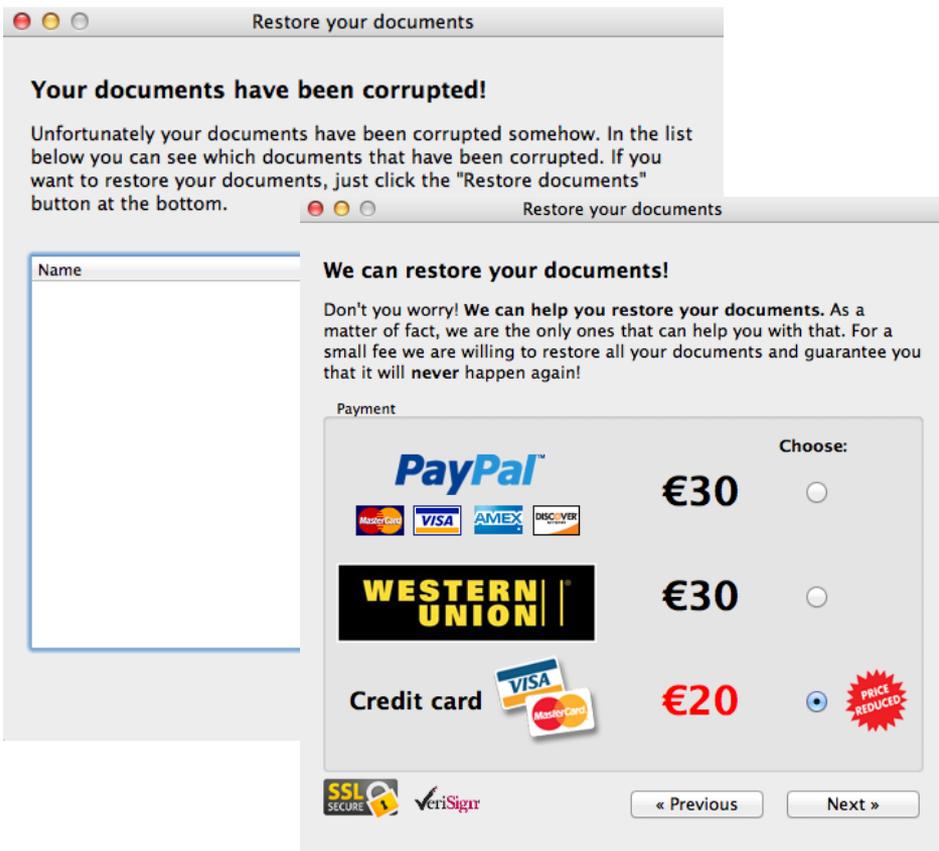
CRYPTOLOCKER : LE RANSOMWARE DESTRUCTEUR



Nouvelle méthode de chiffrement.

- Utilisation du chiffrement assymétrique (clé publique / clé privée) RSA-2048.
- Algorithme de génération de nom de domaine pour les serveurs de commande et de contrôle (C2)
- Chiffrement des données présentes sur les clés USB, disques durs externes, dossiers partagés et services de stockage cloud
- Propagation via le réseau
- Améliorations continues du malware : CryptoDefense (exploit) et Cryptowall (TOR)

RANSOMWARE OSX



Une preuve de concept

- Aucun fichier chiffré
- Ce ransomware crypte ses propres fichiers mais n'affecte pas ceux de l'utilisateur
- Affichage d'une demande de rançon mais fonction inopérante

PLETOR, SVPENG : RANSOMWARE POUR MOBILE

За просмотр
запрещенного(Педофилия,Зоофилия
я и т.д.) порно ваш телефон
блокирован!



Все Фото и видео материалы с вашей камеры
переданны на рассмотрение.

Для разблокировки вашего телефона и
удаление материалов
вам необходимо оплатить штраф 1000 руб. в
течении 24 часов

Для этого вам нужно пополнить Номер
+79147011354

В ближайшем терминале оплаты.

ВНИМАНИЕ: При попытке избежать штрафа
Все данные будут направлены в публичные
источники



Your device is blocked due to at least of the reasons specified below.

Your device was trying to access a **child pornography** directory and has been **locked**.

Everyday we are working on blocking such sites and distribution of awful materials, and it costs a lot to maintain our operations. You are required to pay **administrative fees**.

Watching, downloading and possessing such horrific materials is highly punishable and will **leave a long lasting effect** on your friends and relatives.

If we don't receive a payment within

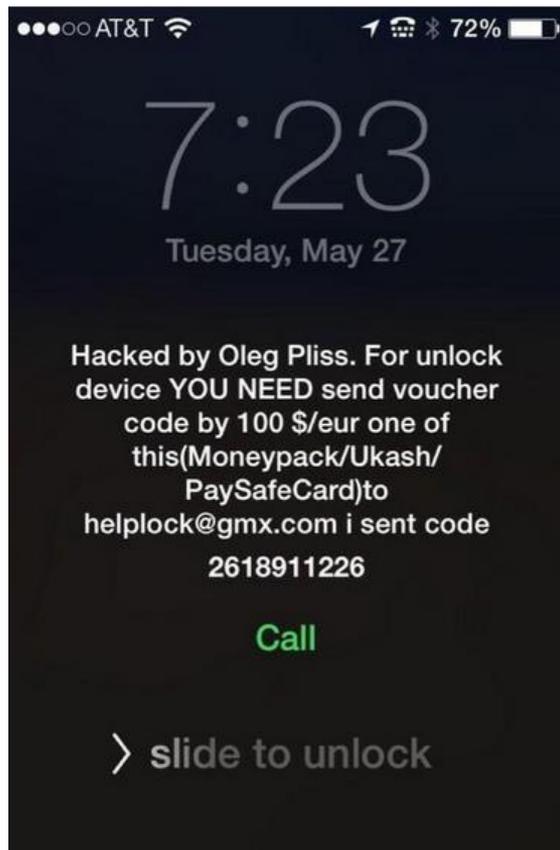
Pletor.

- Chiffrement via AES
- Chiffrement des fichiers multimédias et documents personnels
- Mugshot de l'utilisateur

SVPENG.

- Imitate une analyse du téléphone puis le bloque
- Demande de rançon de 500\$
- Empêche le redémarrage / arrêt du terminal

RANSOMWARE IOS



Hammeçonnage sur l'Apple ID

- Verrouillage à distance du terminal à l'aide d'un code PIN et activation du « Lost Mode »
- Affichage d'une demande de rançon grâce à la fonction « Find my iPhone »
- Les victimes utilisaient les mêmes mots de passe pour d'autres services

CTB-LOCKER : CURVE + TOR + BITCOIN

Vos dossiers personnels sont encryptés par le CTB-Locker.

Vos documents, vos photos, vos données et d'autres dossiers importants ont été encryptés avec un encodage plus fort et une clé unique, générés par cet ordinateur.

La clé privée pour décrypter est gardé dans un serveur d'Internet secret et personne ne peut décrypter vos dossiers jusqu'à ce que vous payez et obteniez la clé privée.

Si vous voyez la fenêtre-casier principale, suivez les instructions sur le casier. Autrement, il semble que vous ou votre antivirus élimine le programme casier. Maintenant, vous avez la dernière opportunité de décrypter vos dossiers.

Ouvrez [http://\[redacted\]](http://[redacted]) ou [http://\[redacted\]](http://[redacted]) dans votre navigateur. Ils sont des portails publics vers le serveur secret.

Si vous avez des problèmes avec les portails, utilisez une connexion directe:

1. Téléchargez le Navigateur Tor <http://torproject.org/>

2. Sur le navigateur Tor, ouvrez [http://\[redacted\]](http://[redacted])
Notez que ce serveur n'est que disponible à travers du navigateur Tor. Réessayez dans une heure si le site n'est pas accessible.

Écrivez sur la prochaine clé publique sous la forme d'entrée, sur le serveur. Évitez les erreurs typographiques.

Suivez les instructions sur le serveur.

Ces instructions sont aussi gardées dans un dossier appelé Decrypt-All-Files.txt dans le dossier Documents. Vous pouvez l'ouvrir et utiliser le copié-collé pour les adresses et la clé.

Une nouvelle génération de cryptomalware

- Serveurs de C&C cachés dans le réseau anonyme TOR
- Paiement de la rançon en Bitcoin
- Compression des fichiers avant chiffrement
- Utilisation d'un schéma de cryptographie complexe et du protocole de chiffrement assymétrique ECDH
- Support multilingues : Français, Anglais, Allemand, Italien, Hollandais, Espagnol, Letton.

COMMENT SE PRÉMUNIR DE CES ATTAQUES RECOMMANDATIONS

Des conseils pour les administrateurs et les utilisateurs

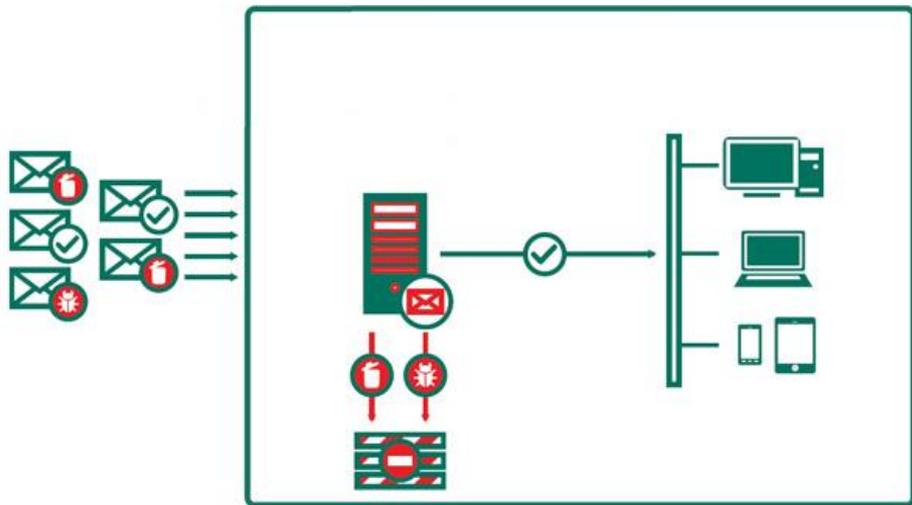
SAUVEGARDE DES DONNÉES SENSIBLES



La protection ultime contre les cryptomalware.

- Il est désormais impossible de restaurer les fichiers chiffrés : réalisez des copies de sauvegarde des fichiers importants
- Attention ! Risque de chiffrement des disques réseaux : les opérations de sauvegarde régulières doivent être réalisées sur un périphérique de stockage uniquement accessible lors de la sauvegarde
- Ne pas payer la rançon : pas de garantie de récupération des données et cela encourage les créateurs de cryptomalware

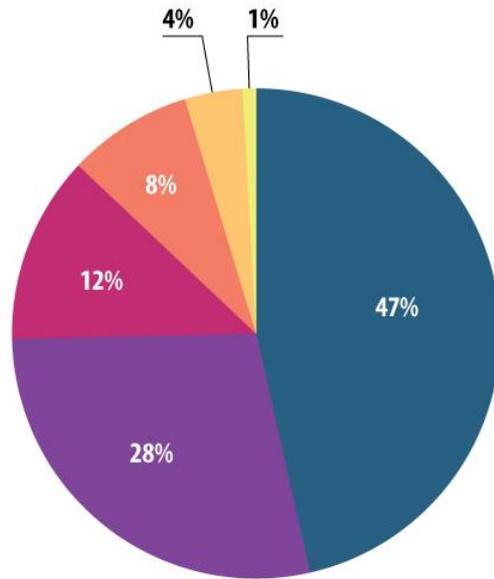
PROTECTION DES FLUX DE MESSAGERIE



Analyse des emails en amont.

- Analyse antivirus du corps des messages, des pièces jointes et des liens (phishing)
- Analyse à de multiples niveaux de l'infrastructure de messagerie : postes de travail, boîtes aux lettres, périmètre réseaux (DMZ, appliance), Fournisseur de Service Internet
- Filtrage sur les extensions des pièces jointes : SCR dans ZIP pour CTB-Locker

MISES À JOUR SYSTÈMES ET APPLICATIONS TIERCES



■ Browsers

■ Adobe Flash Player

■ Oracle Java

■ Microsoft Office

■ Adobe Reader

■ AndroidOS

Correction des vulnérabilités pour prévenir leurs exploitations.

- Mise à jour des vulnérabilités des systèmes
- Mise à jour des applications tierces : navigateurs, Java, Adobe Reader, Flash Player, Microsoft Office, etc.
- Automatisation du processus d'installation des mises à jour et des correctifs
- <http://securelist.com/analysis/quarterly-malware-reports/67637/it-threat-evolution-q3-2014/>

PROTECTION DES POSTES DE TRAVAIL



La dernière ligne de défense.

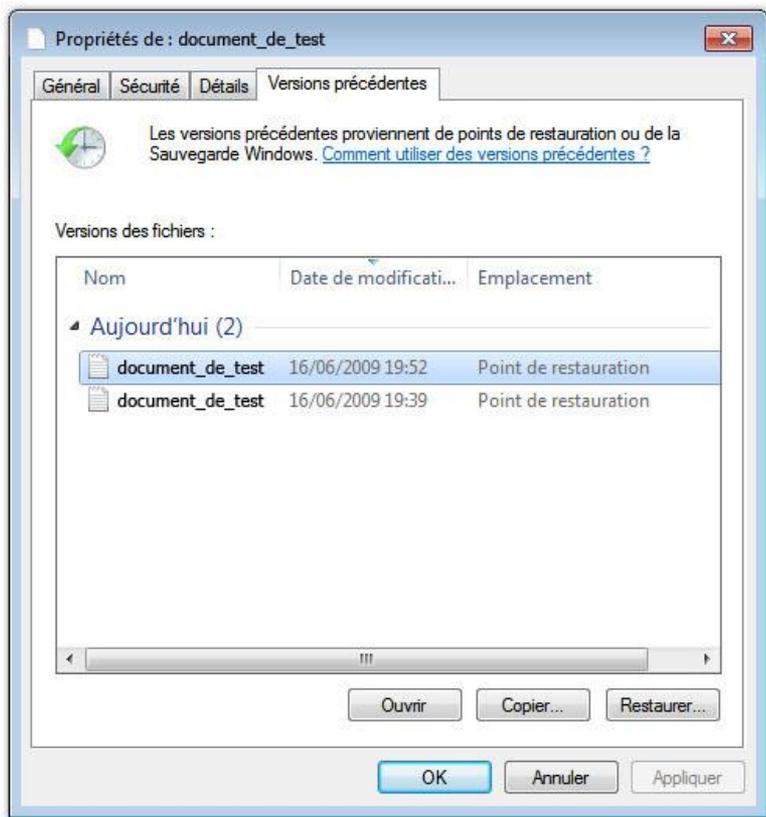
- Analyse du flux de messagerie et du système de fichiers
- Technologies d'analyse par signature, analyse comportementale et calcul de réputation
- Mise à jour régulière (toutes les heures) des signatures des menaces
- L'utilisateur ne doit pas être en mesure de désactiver la protection ou d'affecter la configuration de l'antivirus

PROTECTION DES PÉRIPHÉRIQUES MOBILES



- Installer un antivirus pour une analyse temps réel des applications installées
- Ne téléchargez pas d'applications depuis des forums, des sites Web externes, etc. Utilisez uniquement des sources fiables : dans les paramètres de sécurité, désactivez l'option d'installation des applications tierces
- Activez la double authentification sur iCloud (Apple)
- Avant de l'installer, vérifiez les permissions que requière l'application.
- Evitez le jailbreak/root du périphérique mobile.

AUTRES RECOMMANDATIONS



- Configurer l'accès aux dossiers partagés sur le réseau : accès restreint en écriture à l'essentiel
- Activez la protection système des disques (versions précédente des fichiers)
- Affichez les extensions des fichiers dont le type est connu
- Eduquez & avertissez vos utilisateurs

LES PIÈCES JOINTES DANS LES EMAILS



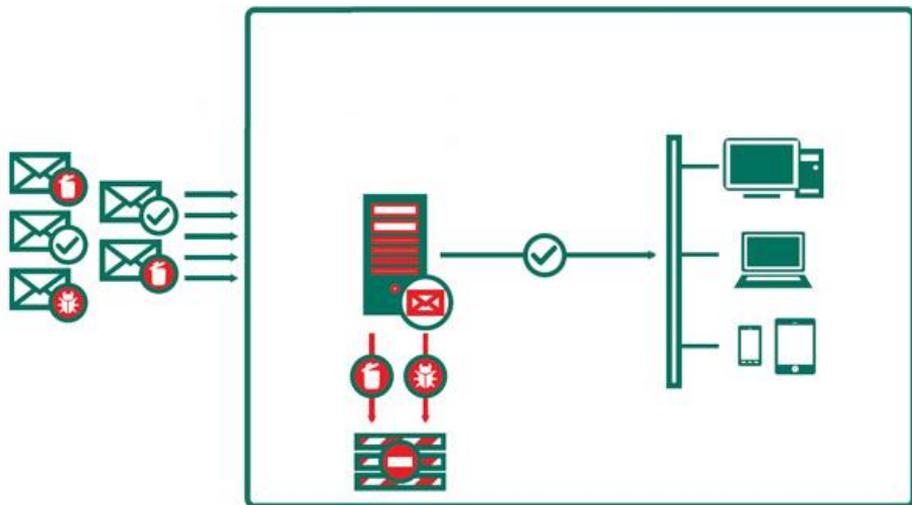
Eduquez les utilisateurs à la sécurité informatique.

- Ne pas ouvrir les pièces jointes dans les emails en provenant d'inconnus
- Ne pas cliquer sur les liens suspects
- Attendre la mise à jour de l'antivirus le matin avant de lire ses emails

LES TECHNOLOGIES KASPERSKY LAB PROTECTION CONTRE LES CRYPTOMALWARE

Des solutions de protection pour les différents niveaux de l'infrastructure de l'entreprise, mesures spécifiques de lutte contre les cryptomalware

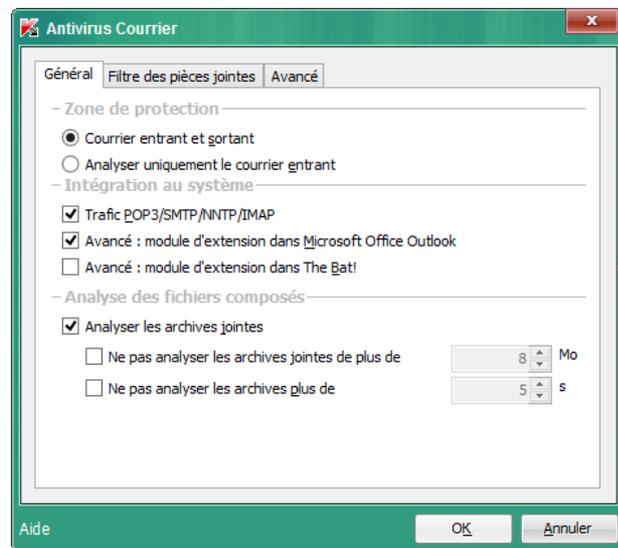
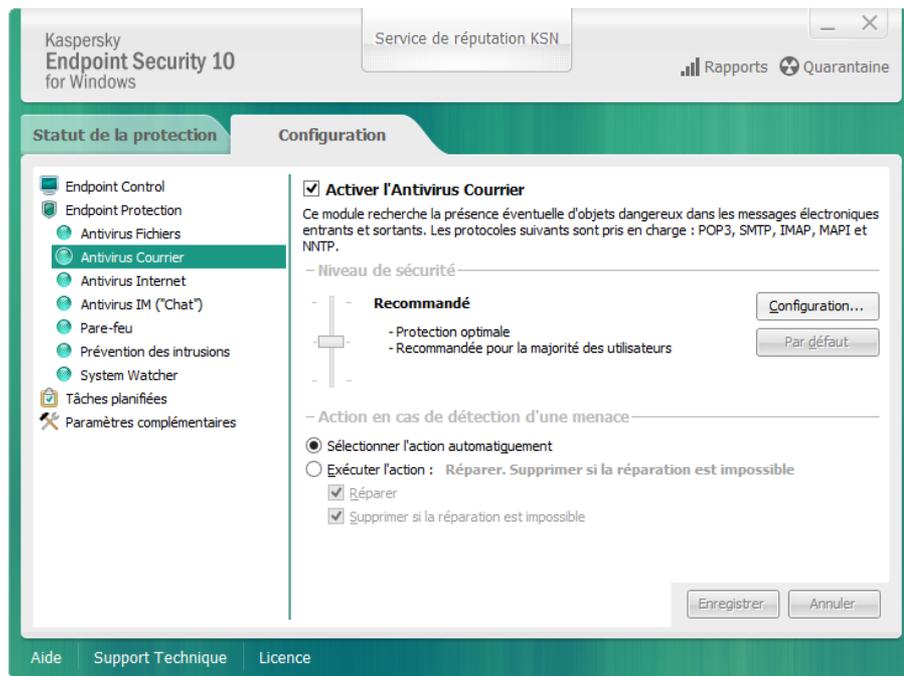
PROTECTION DES FLUX DE MESSAGERIE SUR LES SERVEURS



Une analyse approfondie des messages.

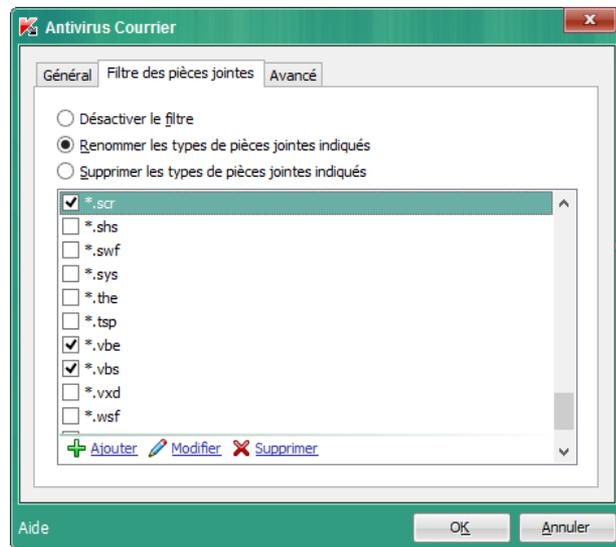
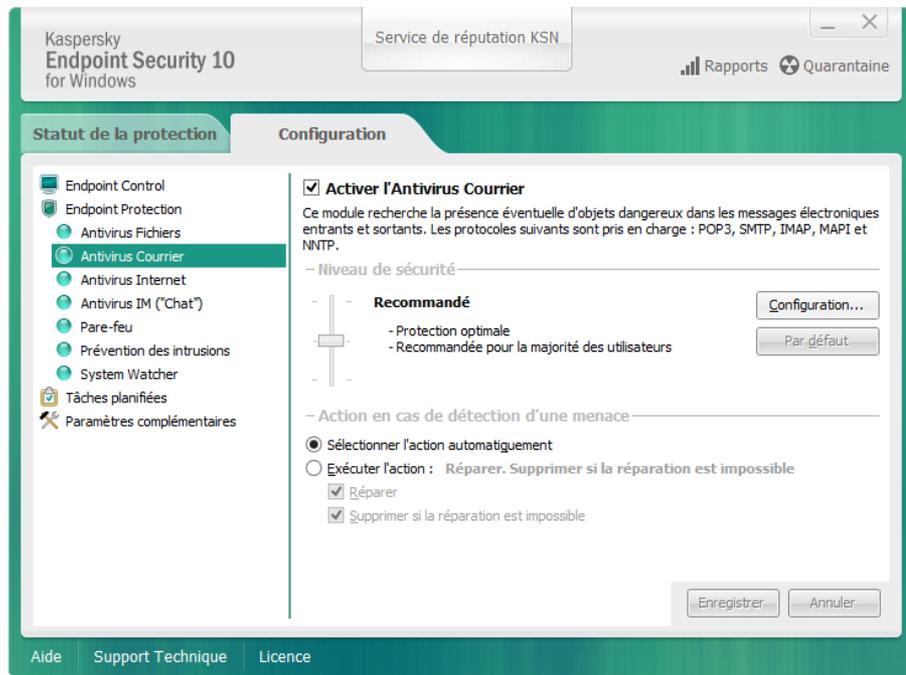
- Pour MS Exchange, Linux et Lotus Domino
- Analyse antivirus des pièces jointes (fichier et archives) et du corps des emails (URL malveillantes et phishing)
- Détection des programmes malveillants dans le cadre des attaques ciblées : exploitation des failles de sécurité
- Technologie de détection cloud KSN

PROTECTION DES FLUX DE MESSAGERIE SUR LES POSTES DE TRAVAIL : ANALYSE DES FLUX



- Analyse des flux POP3/IMAP/MAPI
- Analyse des archives jointes

PROTECTION DES FLUX DE MESSAGERIE SUR LES POSTES DE TRAVAIL : FILTRAGE DES PIÈCES JOINTES



- Filtrage / Renommage / Suppression des pièces jointes selon une liste d'extension configurable

PROTECTION ANTIVIRUS FICHIERS



Intercepte toutes les opérations sur les fichiers.

- 3 technologies d'analyse :
 - Analyse par signature
 - Analyse heuristique
 - Analyse KSN
- Couvre les disques durs, les périphériques amovibles et les disques réseaux
- Analyse en temps réel des fichiers vecteurs d'infection

CONTRÔLE DE L'ACTIVITÉ DES APPLICATIONS

Kaspersky Endpoint Security 10 for Windows

Contrôle de l'activité des applications
L'application a été placée dans un groupe à privilèges restreints

Type d'événement : L'application a été placée dans un groupe à privilèges restreints

Application (Nom) : ctb-locker.scr

Application (Chemin) : c:\users\enduser\downloads\ctb-locker\

Application (ID du processus) : 1896

Utilisateur : enduser-PC\enduser (Utilisateur actif)

Module : Contrôle de l'activité des applications

Résultat (Degré de menace) : Faible

Résultat (Exactitude) : Exactement

Action : L'application a été placée dans le groupe

Objet : Douteuses

Objet (Type) : Groupe d'applications

Objet (Nom) : Douteuses

Raison : Service KSN

[Plus d'informations...](#)



Applications

Règles de contrôle des applications | Ressources protégées | Surveillance de l'activité des programmes

Configuration des règles de contrôle de l'activité des applications

Les règles de contrôle de toutes les applications installées sont créées en mode automatique. Elles sont appliquées en fonction des signatures numériques des applications et des états attribués aux applications sur la base des informations reçues de la part des participants au réseau Kaspersky Security Network.

Modifier

Application	Editeur	Groupe	Popularité
De confiance			
Restrictions faibles			
Restrictions élevées			
Douteuses			
ctb-locker.scr		Moins de 10 utilisateurs	

ctb-locker.scr

Signature numérique : Inexistante

Groupe recommandé : Douteuses

Apparition dans KSN : Aujourd'hui

Groupe : [Douteuses](#)

Aide



Règles de contrôle de l'application

ctb-locker.scr

Fichier | Fichiers et base de registre | Privilèges | Règles réseau | Historique | Exclusions

Ressource	Autorisation
Privileges	
Accès aux autres processus	Interdit
Modification du système	Interdit
Accès aux objets du système	Interdit
Accès de faible niveau au disque	Interdit
Accès de faible niveau au système de fichiers	Interdit
Enregistrement des branches du registre dans le fichier	Interdit
Création de captures d'écran	Interdit
Modifications suspectes dans le système	Interdit
Création de clés de base de registre cachées	Interdit
Création de liens fixes vers un fichier	Interdit
Arrêt de Microsoft Windows	Interdit
Accès aux paramètres des comptes utilisateurs	Interdit
Lancement du programmeur	Interdit
Modification des privilèges	Interdit
Modification des privilèges des objets	Interdit
Accès caché au réseau	Interdit
Utilisation de la ligne de commande du navigateur	Interdit
Utilisation des interfaces de programmation du navigateur	Interdit
Lancement	Interdit

✓ - autorisé ⛔ - interdit

Aide

OK Fermer

Kaspersky Endpoint Security 10 for Windows

Contrôle de l'activité des applications
La règle de surveillance de l'activité des applications a fonctionné

Type d'événement : La règle de surveillance de l'activité des applications a fonctionné

Application (Nom) : ctb-locker.scr

Application (Chemin) : c:\users\enduser\downloads\ctb-locker\

Application (ID du processus) : 1252

Utilisateur : enduser-PC\enduser (Utilisateur actif)

Module : Contrôle de l'activité des applications

Résultat (Description) : Interdit

Résultat (Type) : Accès aux paramètres de sécurité

Résultat (Nom) : Lancement

Résultat (Degré de menace) : Elevée

Résultat (Exactitude) : Exactement

Action : Lancement

Objet : Application inconnue

Objet (Nom) : Application inconnue

Raison : Lancement

[Plus d'informations...](#)

1. Analyse puis assigne l'application à un groupe lors de sa 1^{ère} exécution
2. Limite l'interaction des applications avec le système et les autres applications

Les applications douteuses n'ont pas le droit d'être exécutées

SYSTEM WATCHER : ANALYSE COMPORTEMENTALE

Kaspersky Endpoint Security 10 for Windows

System Watcher

Un objet malveillant a été détecté

Type d'événement :	Un objet malveillant a été détecté
Application\Nom :	ctb-locker.scr
Application\Chemin :	c:\users\enduser\downloads\ctb-locker\
Application\ID du processus :	3952
Utilisateur :	enduser-PC\enduser (Utilisateur actif)
Module :	System Watcher
Résultat\Description :	Déteecté
Résultat\Nom :	PDM:Trojan.Win32.Bazon.a
Résultat\Degré de menace :	Elevée
Résultat\Exactitude :	Exactement
Objet :	c:\users\enduser\downloads\ctb-locker\ctb-locker.scr
Objet\Type :	Processus
Objet\Chemin :	c:\users\enduser\downloads\ctb-locker\ctb-locker.scr
Objet\Nom :	ctb-locker.scr

[Plus d'informations...](#)

- 
- Analyse comportementale via la technologie BSS (Behavior Stream Signatures)**
 - Arrêt du processus et mise en quarantaine automatique en cas de détection**

Kaspersky Endpoint Security 10 for Windows

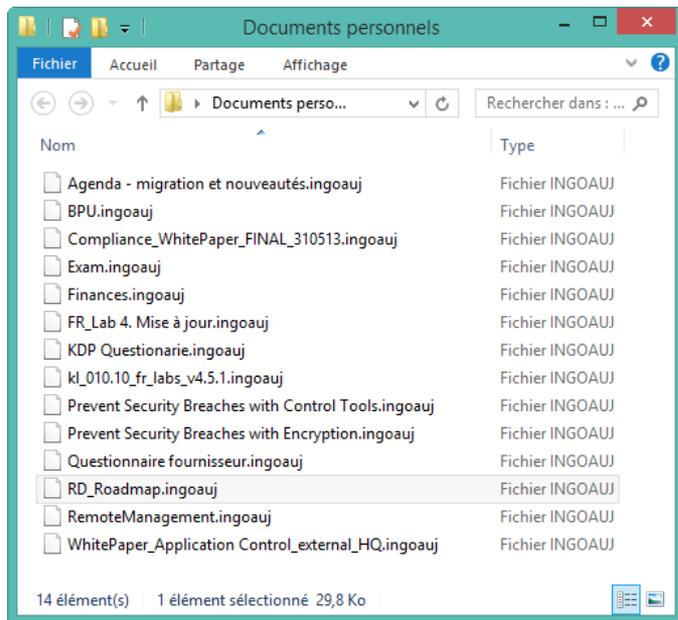
System Watcher

Objet placé en quarantaine

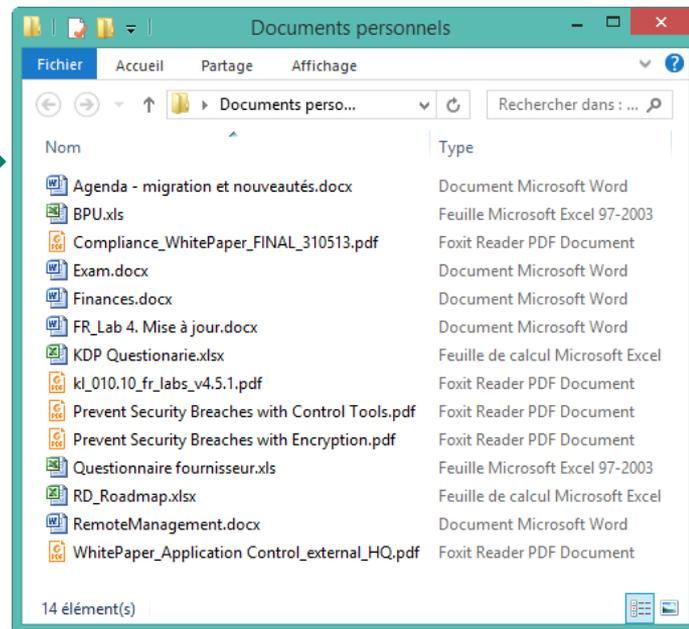
Type d'événement :	Objet placé en quarantaine
Application\Nom :	ctb-locker.scr
Application\Chemin :	c:\users\enduser\downloads\ctb-locker\
Application\ID du processus :	3952
Utilisateur :	enduser-PC\enduser (Utilisateur actif)
Module :	System Watcher
Résultat\Description :	Mis en quarantaine
Résultat\Nom :	PDM:Trojan.Win32.Bazon.a
Résultat\Degré de menace :	Elevée
Résultat\Exactitude :	Exactement
Objet :	c:\users\enduser\downloads\ctb-locker\ctb-locker.scr
Objet\Type :	Processus
Objet\Chemin :	c:\users\enduser\downloads\ctb-locker\ctb-locker.scr
Objet\Nom :	ctb-locker.scr

[Plus d'informations...](#)

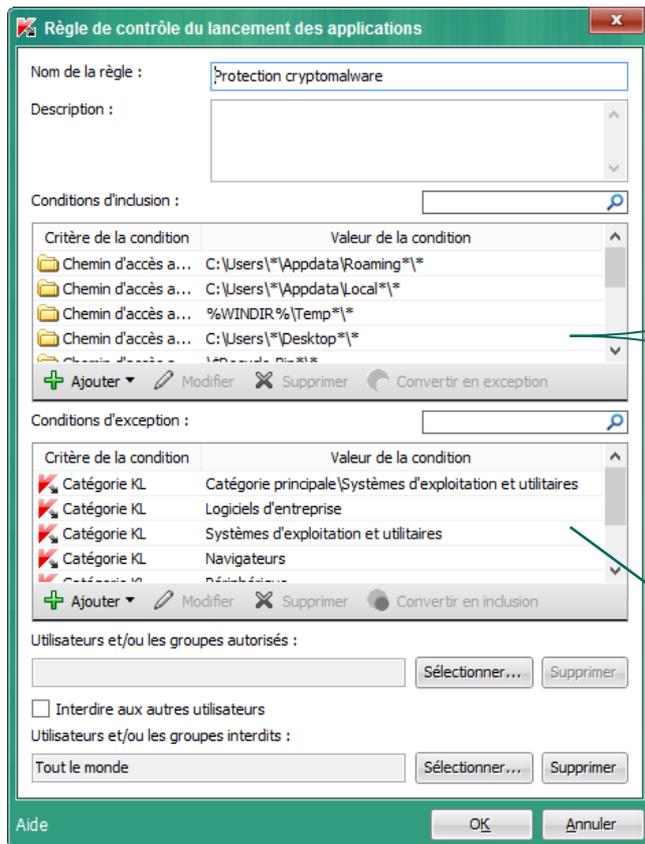
SYSTEM WATCHER : RESTAURATION DES FICHIERS CHIFFRÉS



En cas de détection d'une activité de chiffrement de la part d'un processus suspect, les fichiers sont restaurés dans leurs versions d'origine



RENFORCER LA SÉCURITÉ CONTRE LES CRYPTOMALWARE : BLOQUER LES APPLICATIONS



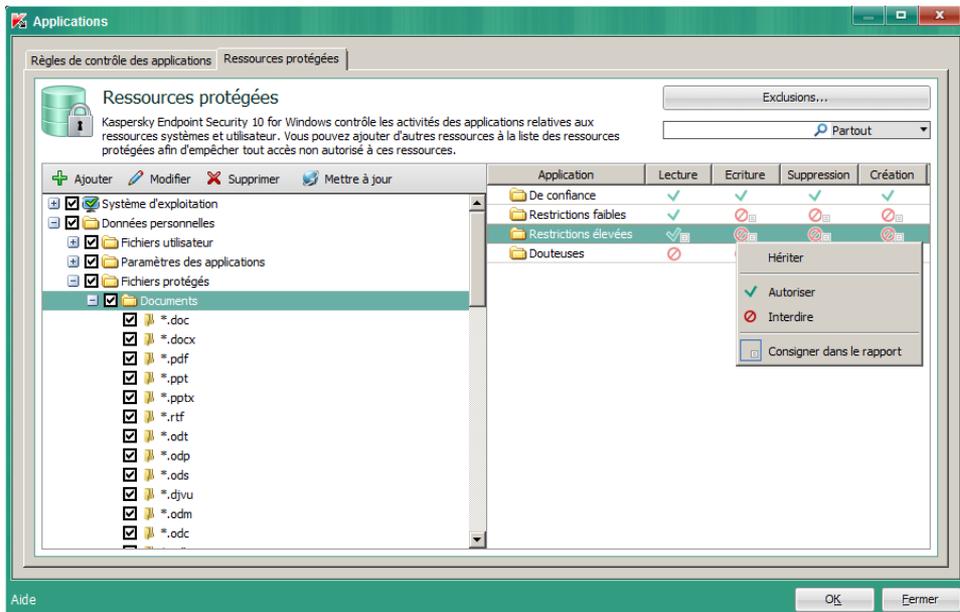
Bloquer le lancement d'applications dans certains répertoires :

- APPDATA
- TEMP
- Dossier des fichiers d'Internet Explorer
- Bureau
- Corbeille
- Répertoire système
- Dossier des documents utilisateurs
- Dossier de démarrage
- <http://support.kaspersky.com/viruses/common/10952#block4>

Exclure les applications de confiance référencées dans les catégories KL :

- <http://whitelist.kaspersky.com/catalogue>

RENFORCER LA SÉCURITÉ CONTRE LES CRYPTOMALWARE : PROTÉGER VOS DONNÉES



Référencer les extensions de fichiers sensibles :

- Documents (*.doc, *.docx, *.odt, *.pdf, *.pst, etc)
- Images (*.jpeg, *.jpg, *.png, etc)
- Archives (*.zip, *.rar, *.7z, etc)
- Multimédia (*.avi, *.mp3, *.mpg, etc)
- Bases de données (*.mdb, *.sql, etc)
- Sauvegarde (*.bak, *.back, etc)
- Fichiers sources (*.php, *.js, *.c, etc)
- Fichiers issus d'applications métiers

Configurer les permissions pour les groupes d'applications avec restrictions :

- <http://support.kaspersky.com/10905>

QUE FAIRE EN CAS D'INFECTION



Recommandations générales :

- Ne payer pas la rançon
- Installer un antivirus et réaliser une analyse complète
- En fonction de la menace découverte, vous pouvez utiliser nos outils de déchiffrement :
 - [RectorDecryptor](#)
 - [XoristDecryptor](#)
 - [RakhniDecryptor](#)
 - [ScatterDecryptor](#)
 - [ScraperDecryptor](#)
 - [RannohDecryptor](#)
- En cas de verrouillage système, utilisez notre outil [Windows Unlocker](#)
- Transmettre les échantillons de fichiers suspects [au laboratoire](#) pour analyse et/ou ouvrir un incident.

EN RÉSUMÉ



Composantes d'une protection efficace contre les cryptomalware :

- Protection Antivirus sur le flux de messagerie à différents niveaux de l'infrastructure
- Protection des postes de travail :
 - Analyse en temps réel des fichiers ([Antivirus Fichiers](#))
 - Analyse en temps réel du courrier ([Antivirus Courrier](#))
 - Analyse comportementale ([System Watcher](#))
 - Blocage du lancement d'applications pour les dossiers ([Contrôle du lancement des applications](#))
 - Protection des extensions de fichiers sensibles ([Contrôle de l'activité des applications](#))
- Sensibilisation des utilisateurs aux bonnes pratiques
- Sauvegarde protégée et régulière des données

MERCI, QUESTIONS ?

Kaspersky Lab France
2, rue Joseph Monier
92500 Rueil Malmaison
Tel : 0.825.888.612
www.kaspersky.fr

