LES ATTAQUES DE CRYPTOMALWARE

Kaspersky Lab France

SOMMAIRE

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

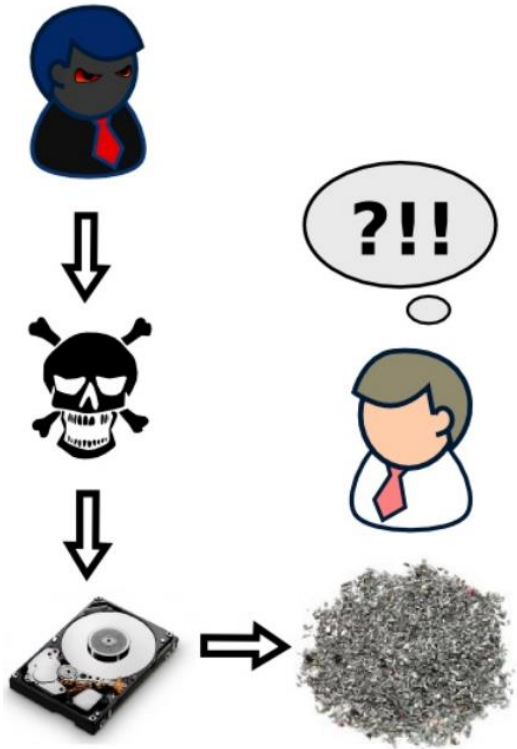
1. System Lockers

2. Data Encoders

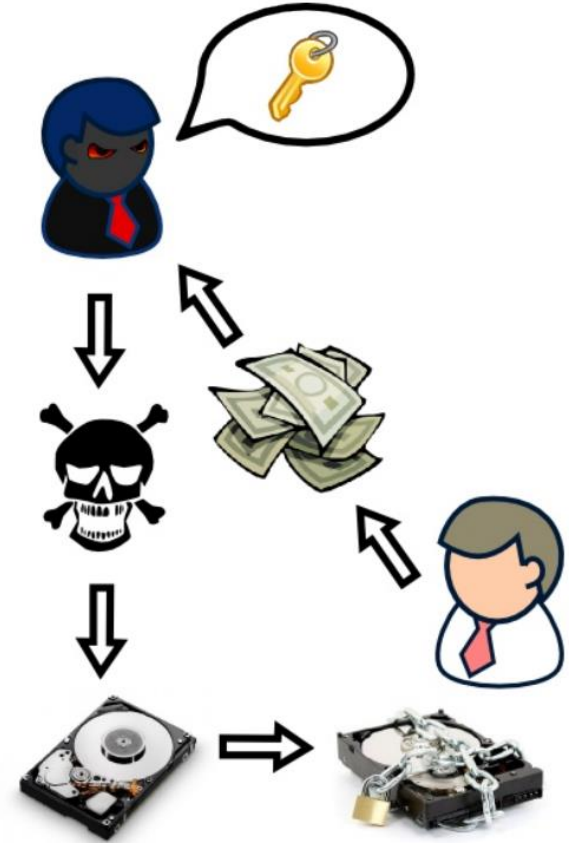
KASPERSKY lab

POURQUOI LES RANSOMWARE

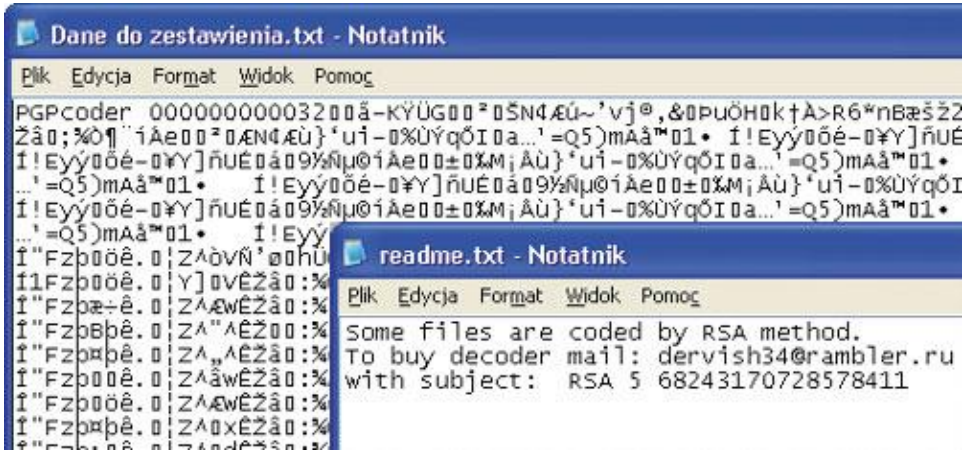
Malware destructeur « classique »



Ransomware



GPCODE : LE 1ER RANSOMWARE



Emérgence des premiers codes malicieux maître-chanteurs en Russie.

- Décembre 2004 : 1ère variante de Gpcode
- Juin 2005 : nouvelle vague d'attaques sur l'Internet Russe après + de 25 modifications du malware
- Janvier 2006 : 1ère 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

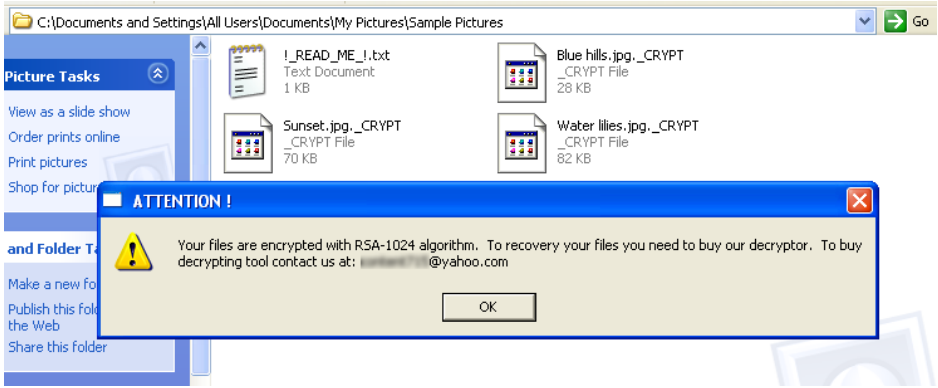
```
How to pay to get your information back.

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 co
    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 th
       box below.
    6.  The last step click "Open"
```

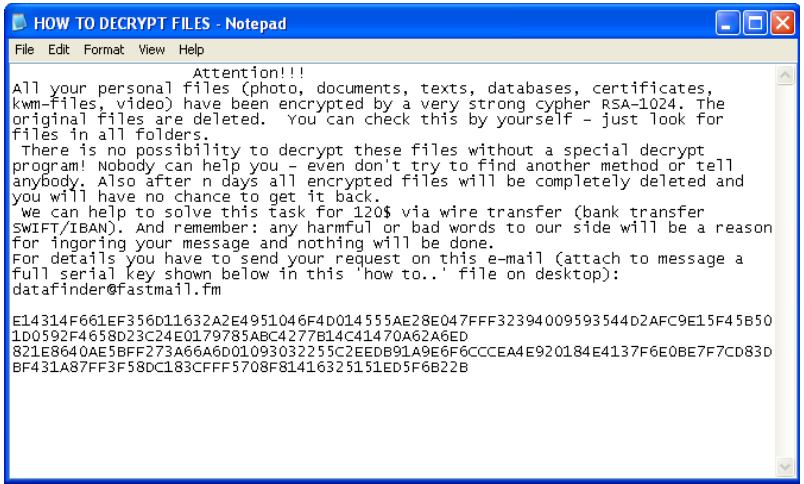
Une autre technique de chantage.

- 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$

KASPERSKY lab

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

KASPERSKY lab

LES FAUX MESSAGES DE VERROUILLAGE

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 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.

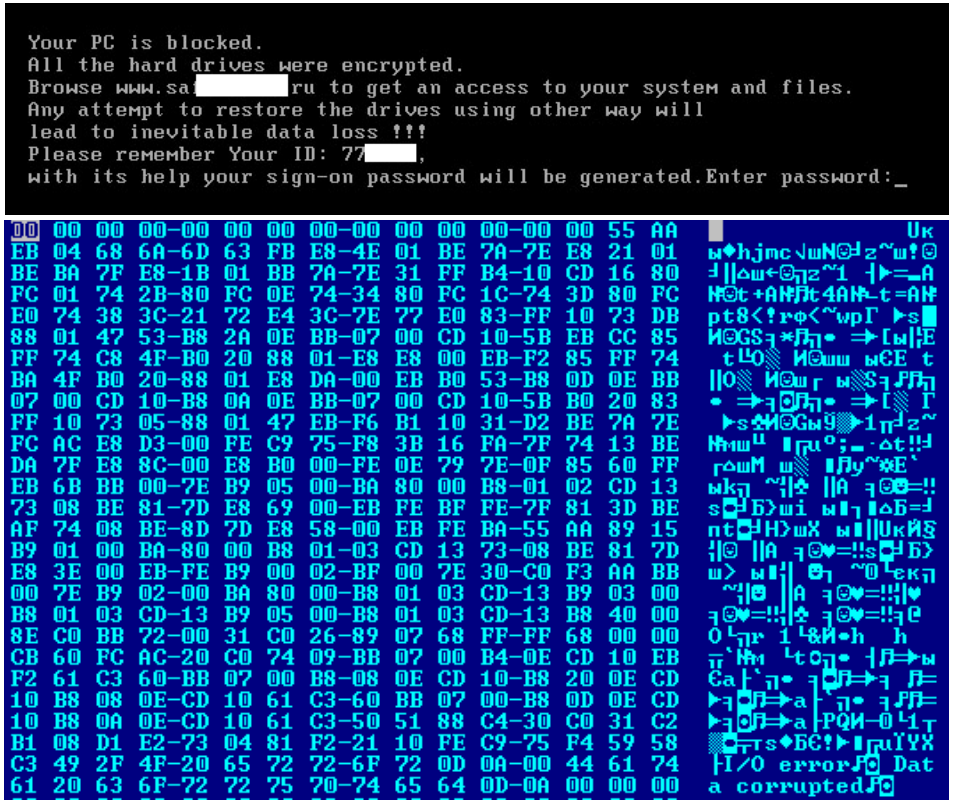
Pour débloquer votre ordinateur, vous devez payer 200 € dans les 3 jours prochaines. Si vous ne payez pas dans dans le délai précisé, votre ordinateur sera confisqués et votre cas sera soumis au tribunal.

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 valuers 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



Blocage au démarrage de la machine.

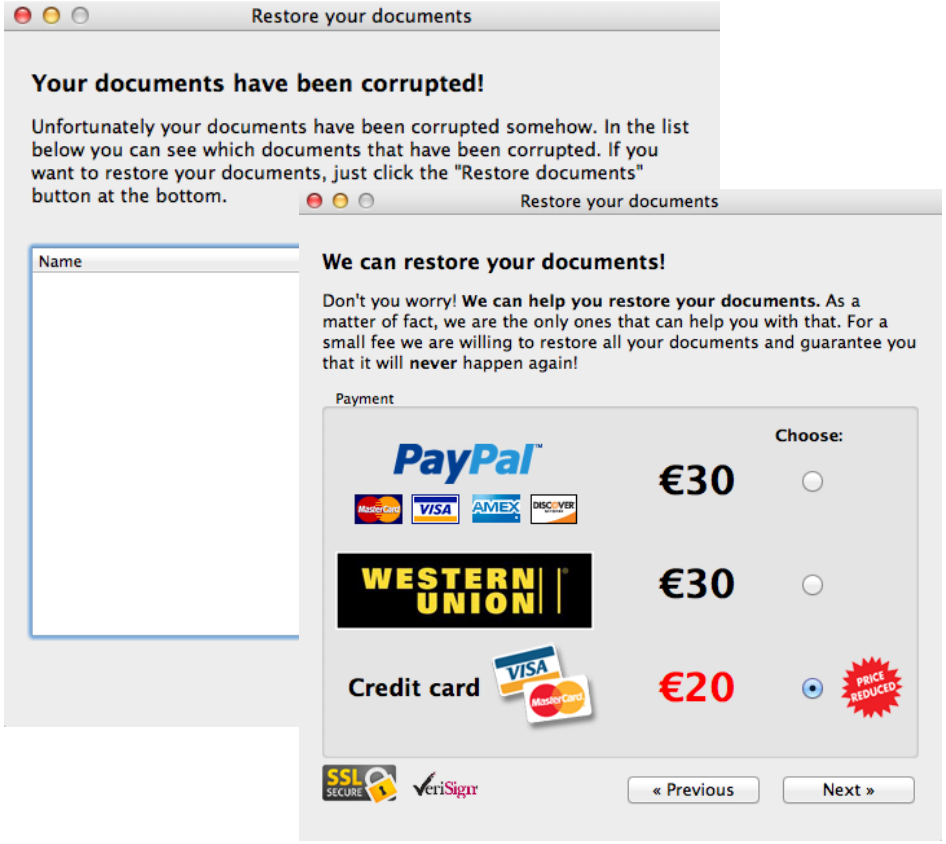
- Après 3 mots de passe incorrects la machine redémarre et le même message apparaît
- Les données ne sont pas chiffrées contrairement à ce qu'indique le message
- Demande de rançon de 100$

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)

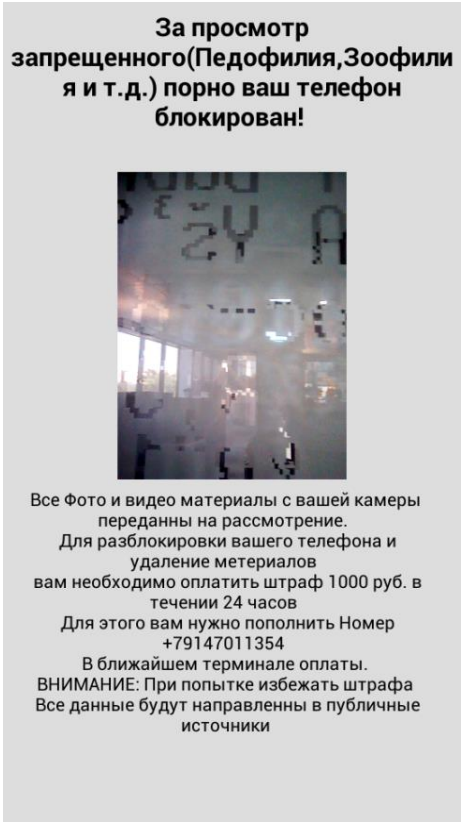
RANSOMWARE OSX

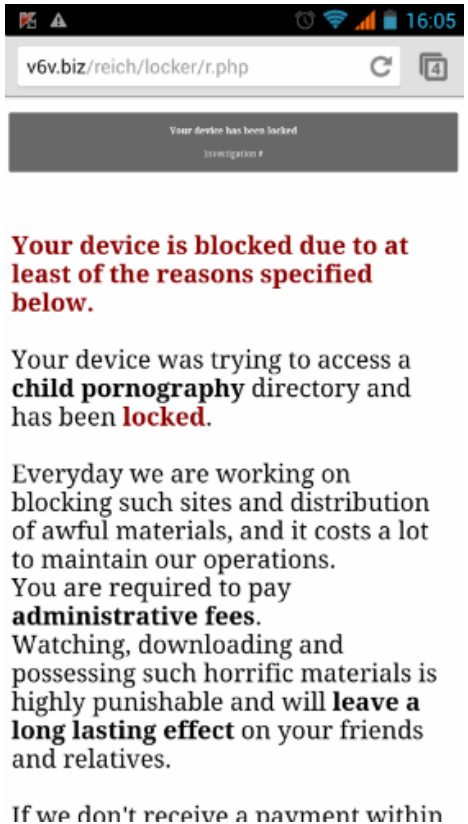


Une preuve de concept

- 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





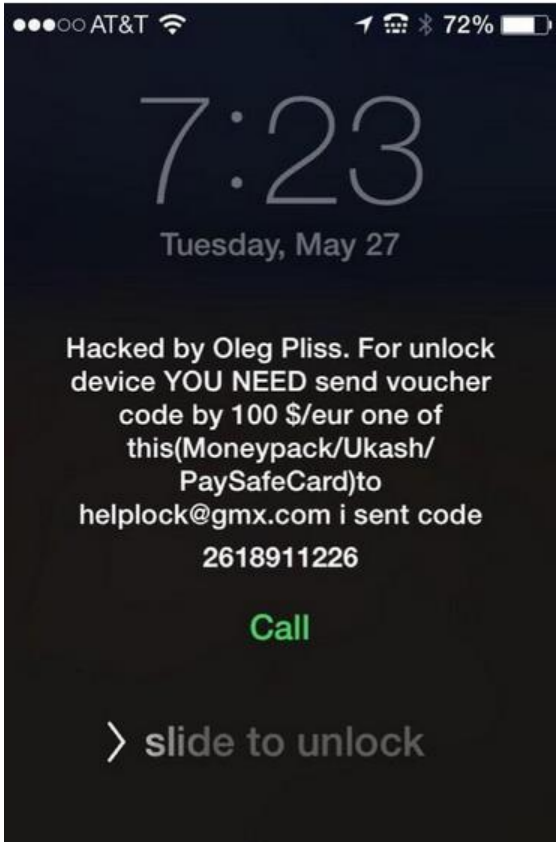
Pletor.

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

SVPENG.

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

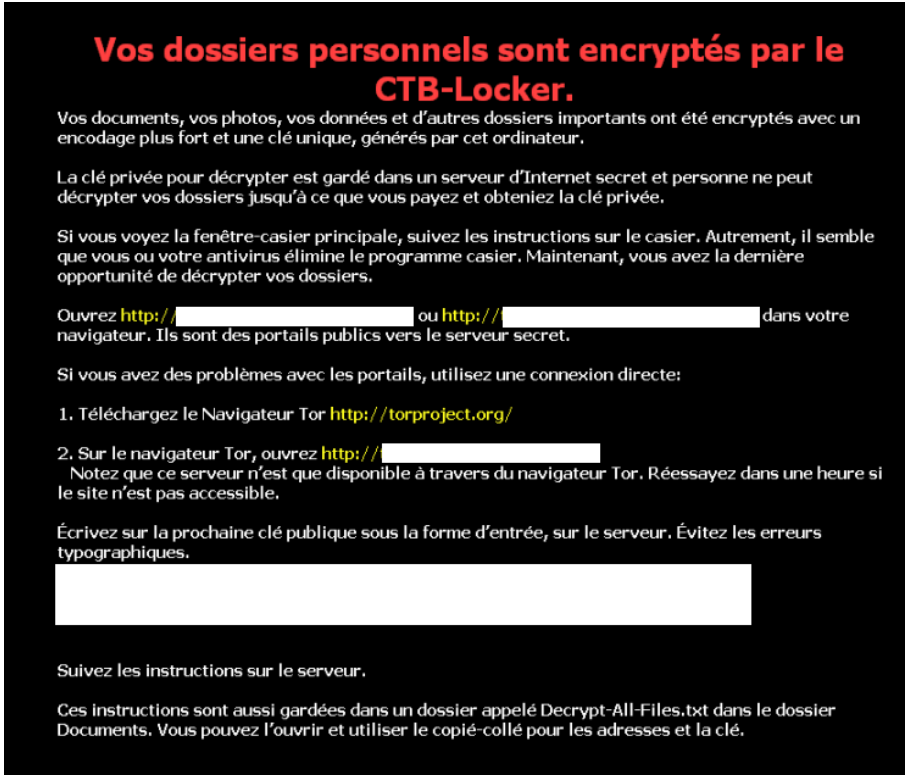
RANSOMWARE IOS



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



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

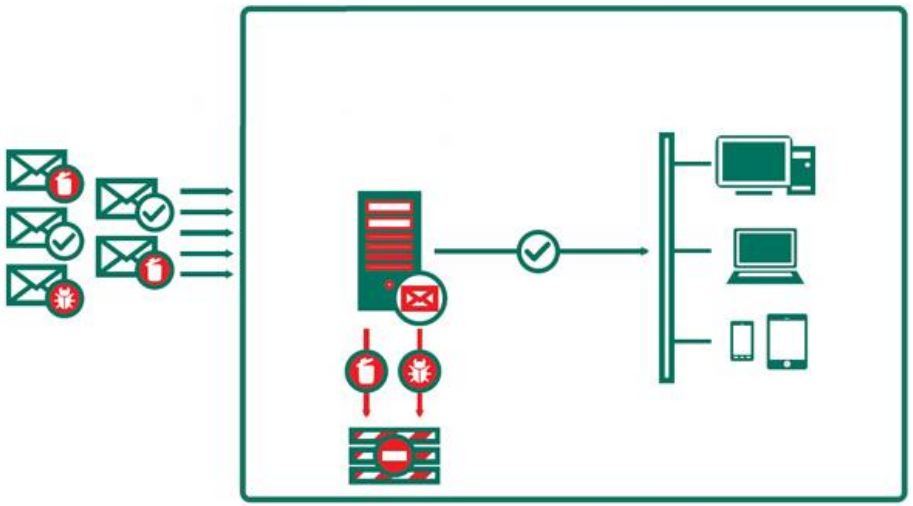
Des conseils pour les administrateurs et les utilisateurs

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

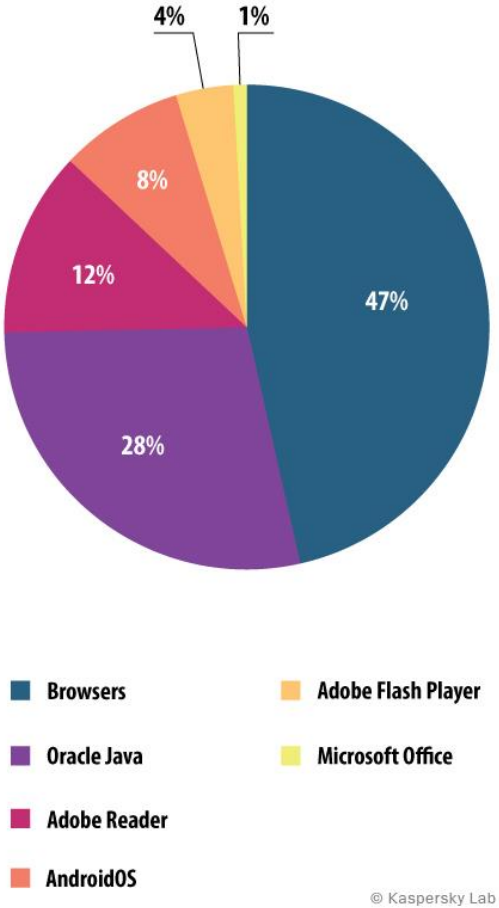
PROTECTION DES FLUX DE MESSAGERIE



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



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

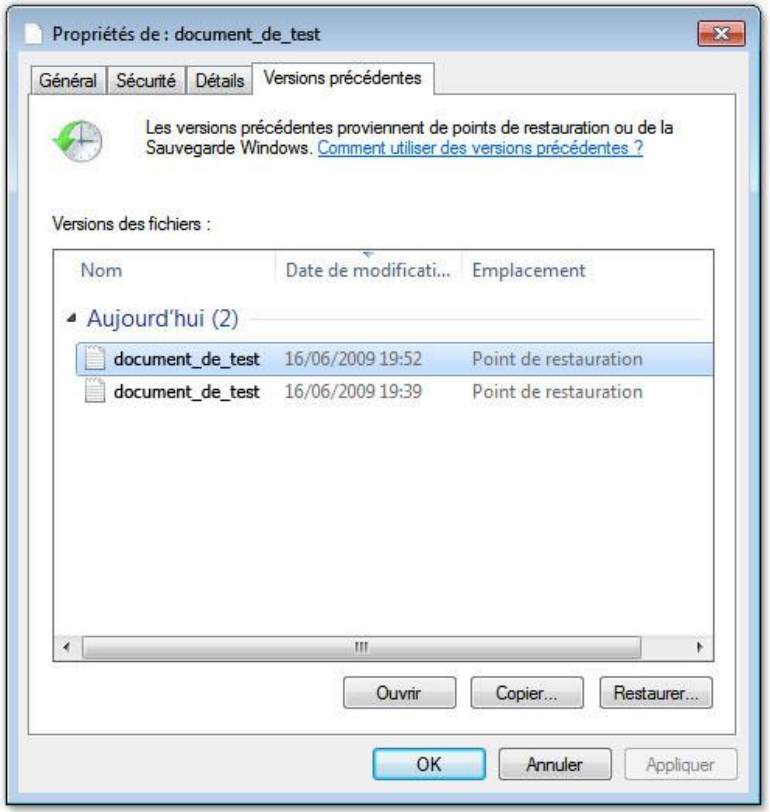
La dernière ligne de défense.

- 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

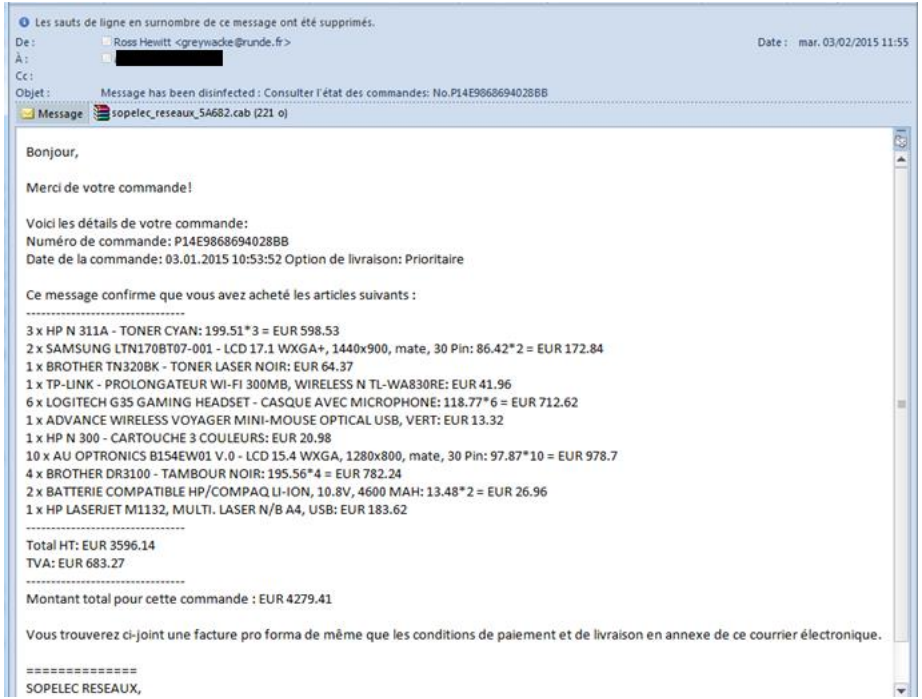
- Installer un antivirus pour une analyse temps réel des applications installées
- Ne téléchargez pas d'applications depuis des forums, des sites Web externes, etc. Utilisez uniquement des sources fiables : dans les paramètres de sécurité, désactivez l'option d'installation des applications tierces
- 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



Les sauts de ligne en surnombre de ce message ont été supprimés.

De : Ross Hewitt <greywacke@runde.fr>
Date : mar. 03/02/2015 11:55
À : [redacted]
Cc :
Objet : Message has been disinfected : Consulter l'état des commandes: No.P14E9868694028BB

Message | sopelec_reseaux_5A682.cab (221 o)

Bonjour,

Merci de votre commande!

Voici les détails de votre commande:
Numéro de commande: P14E9868694028BB
Date de la commande: 03.01.2015 10:53:52 Option de livraison: Prioritaire

Ce message confirme que vous avez acheté les articles suivants :
---
3 x HP N 311A - TONER CYAN: 199.51*3 = EUR 598.53
2 x SAMSUNG LTN170BT07-001 - LCD 17.1 WXGA+, 1440x900, mate, 30 Pin: 86.42*2 = EUR 172.84
1 x BROTHER TN320BK - TONER LASER NOIR: EUR 64.37
1 x TP-LINK - PROLONGATEUR WI-FI 300MB, WIRELESS N TL-WA830RE: EUR 41.96
6 x LOGITECH G35 GAMING HEADSET - CASQUE AVEC MICROPHONE: 118.77*6 = EUR 712.62
1 x ADVANCE WIRELESS VOYAGER MINI-MOUSE OPTICAL USB, VERT: EUR 13.32
1 x HP N 300 - CARTOUCHE 3 COULEURS: EUR 20.98
10 x AU OPTRONICS B154EW01 V.0 - LCD 15.4 WXGA, 1280x800, mate, 30 Pin: 97.87*10 = EUR 978.7
4 x BROTHER DR3100 - TAMBOUR NOIR: 195.56*4 = EUR 782.24
2 x BATTERIE COMPATIBLE HP/COMPAQ LI-ION, 10.8V, 4600 MAH: 13.48*2 = EUR 26.96
1 x HP LASERJET M1132, MULTI. LASER N/B A4, USB: EUR 183.62

Total HT: EUR 3596.14
TVA: EUR 683.27

Montant total pour cette commande : EUR 4279.41

Vous trouverez ci-joint une facture pro forma de même que les conditions de paiement et de livraison en annexe de ce courrier électronique.

==========
SOPELEC RESEAUX,

Eduquez les utilisateurs à la sécurité informatique.

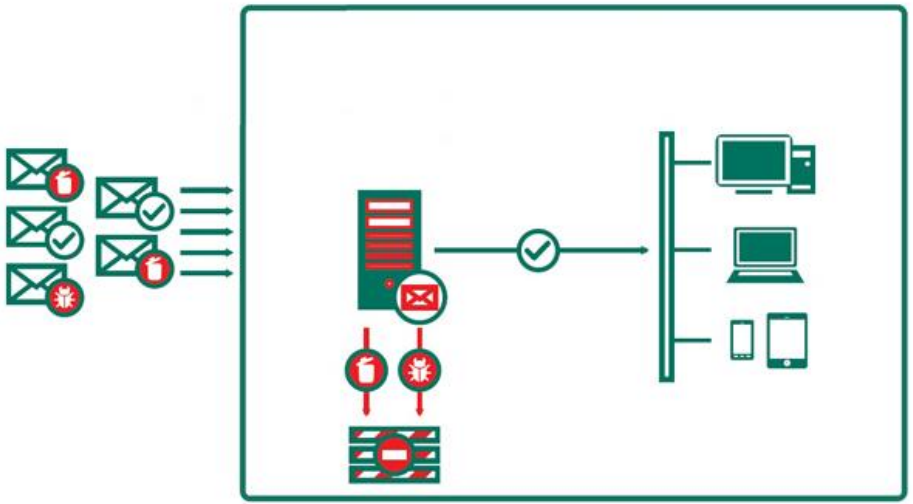
- Ne pas ouvrir les pièces jointes dans les emails en provenant d'inconnus
- Ne pas cliquer sur les liens suspects
- Attendre la mise à jour de l'antivirus le matin avant de lire ses emails

KASPERSKY lab

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

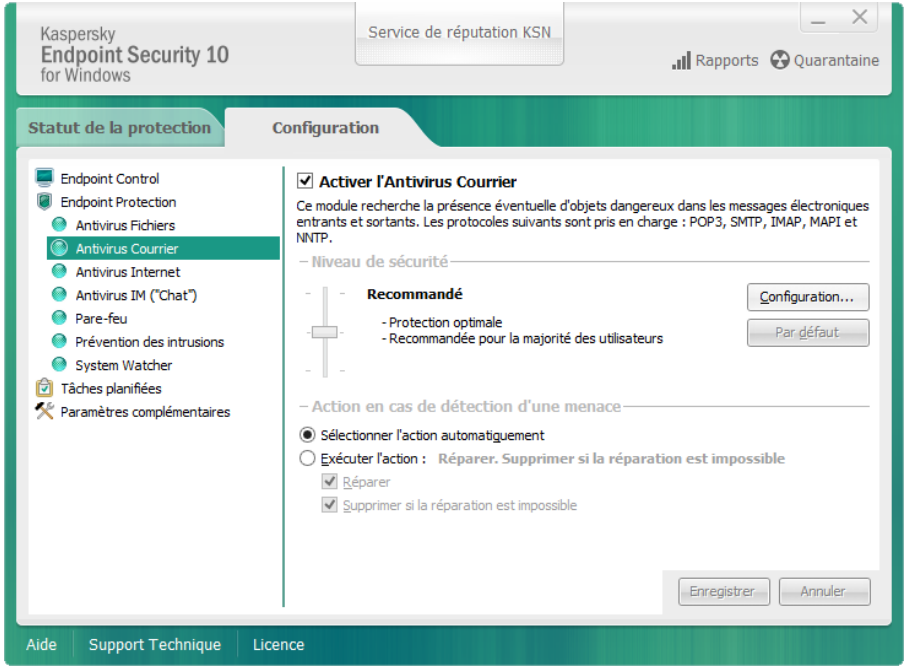
PROTECTION DES FLUX DE MESSAGERIE SUR LES SERVEURS

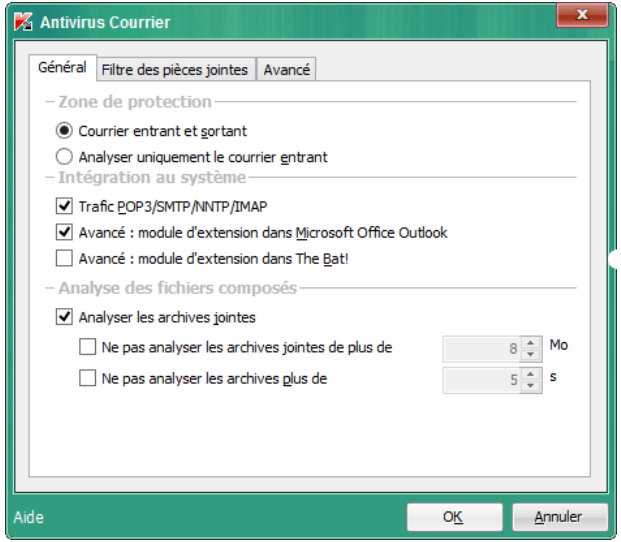


Une analyse approfondie des messages.

- 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

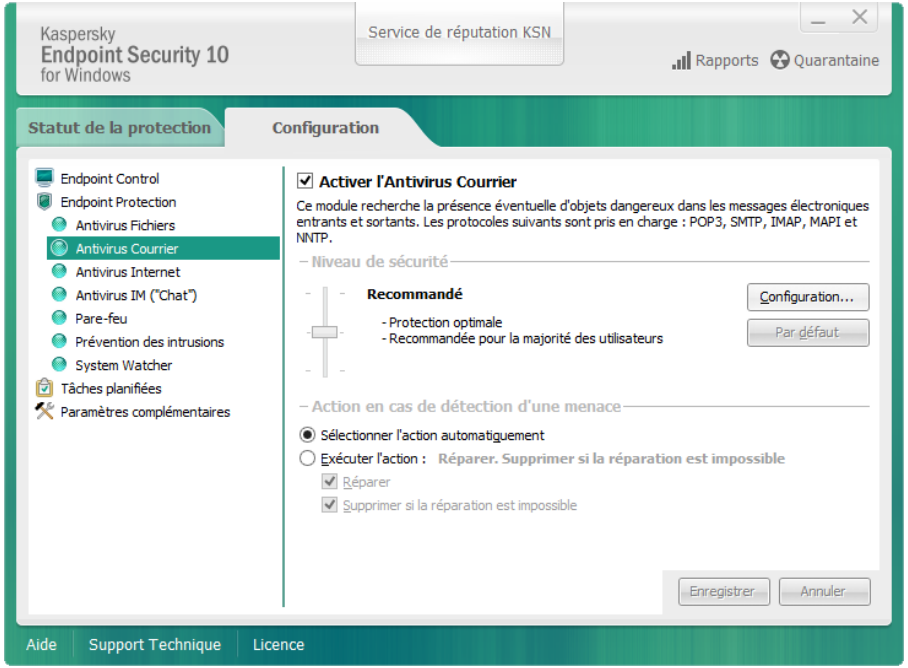
PROTECTION DES FLUX DE MESSAGERIE SUR LES POSTES DE TRAVAIL : ANALYSE DES FLUX

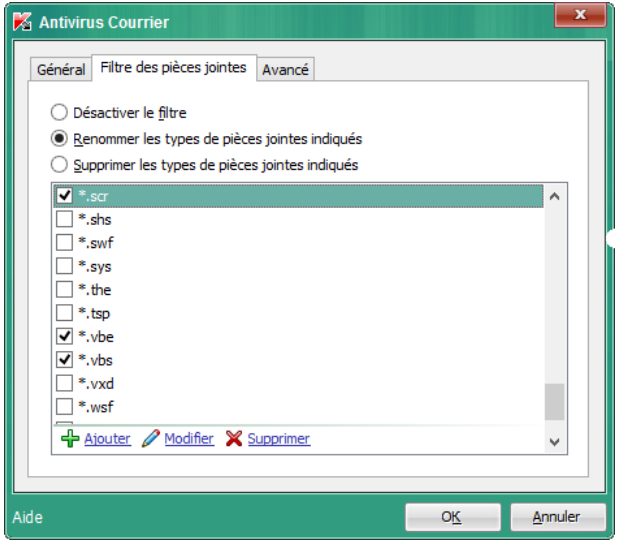




- **Analyse des flux POP3/IMAP/MAPI**
- **Analyse des archives jointes**

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





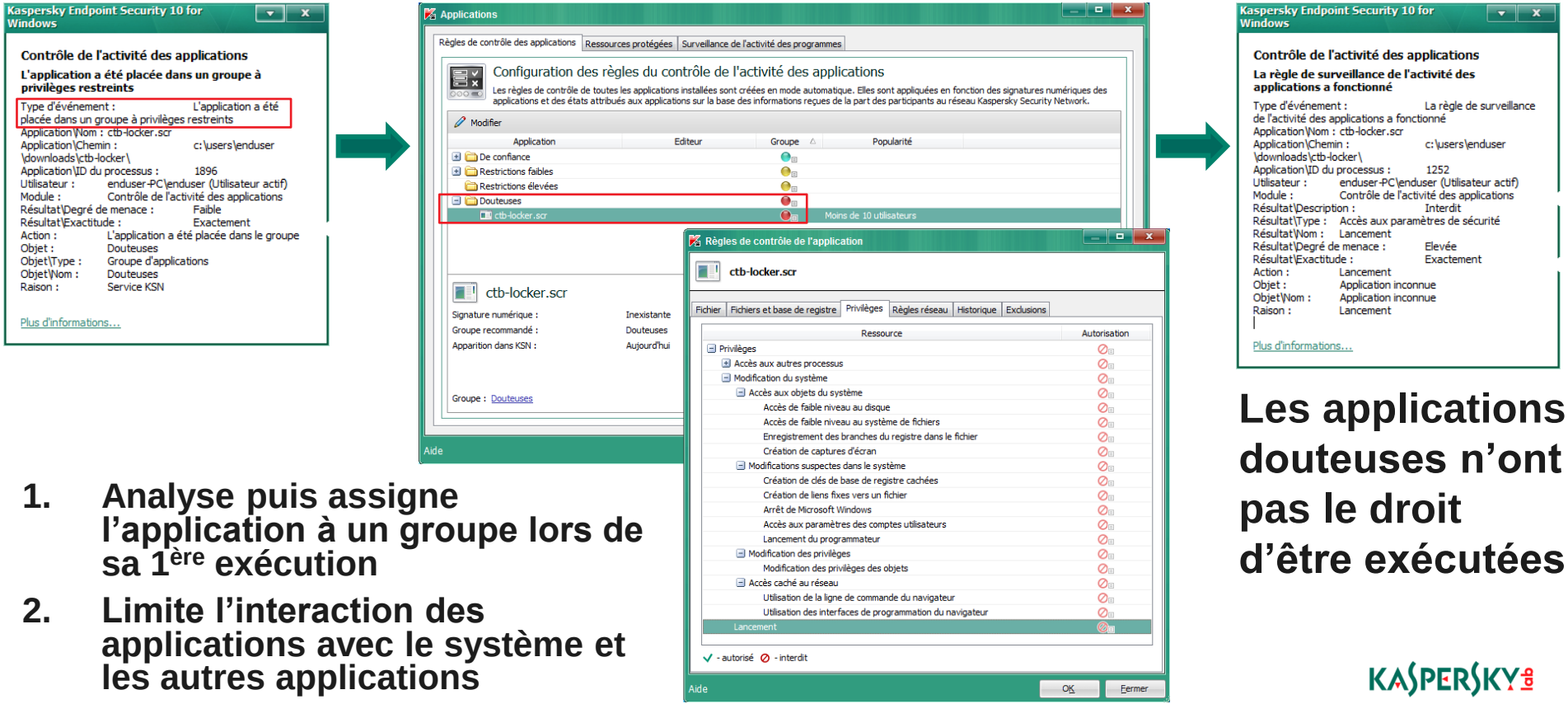
- Filtrage / Renommage / Suppression des pièces jointes selon une liste d'extension configurable

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



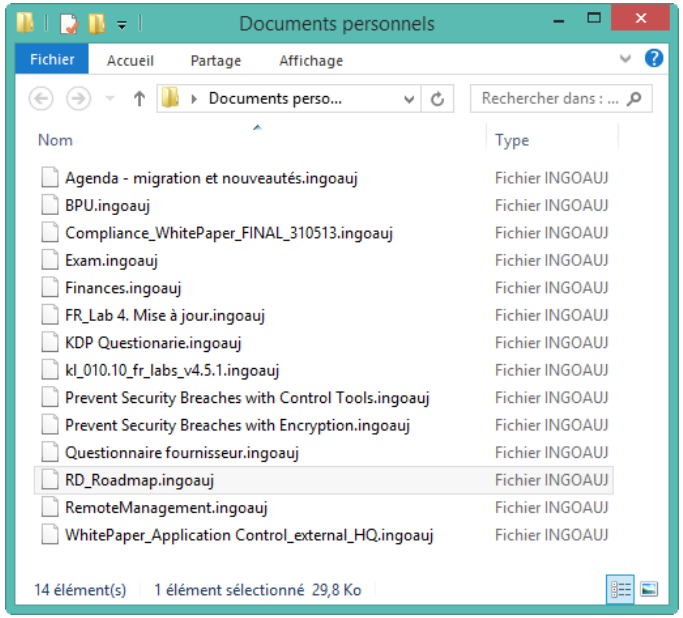
1. **Analyse puis assigne l'application à un groupe lors de sa 1ère exécution**
2. **Limite l'interaction des applications avec le système et les autres applications**

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

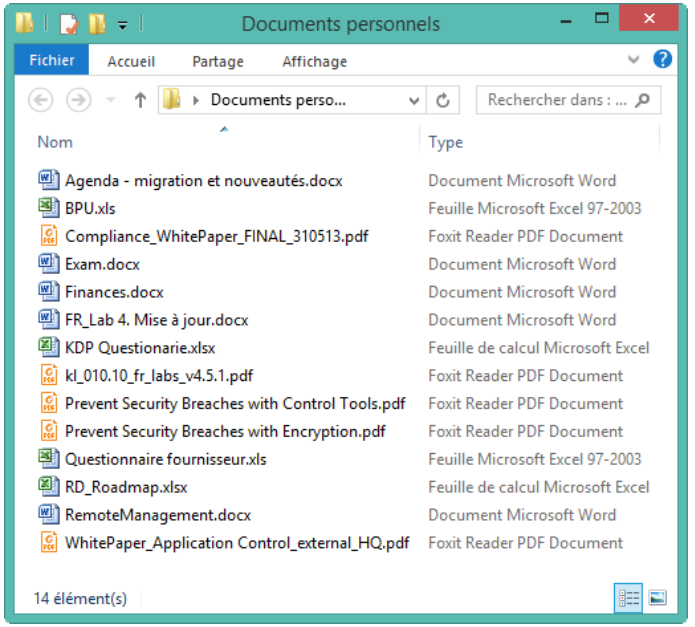
SYSTEM WATCHER : ANALYSE COMPORTEMENTALE

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

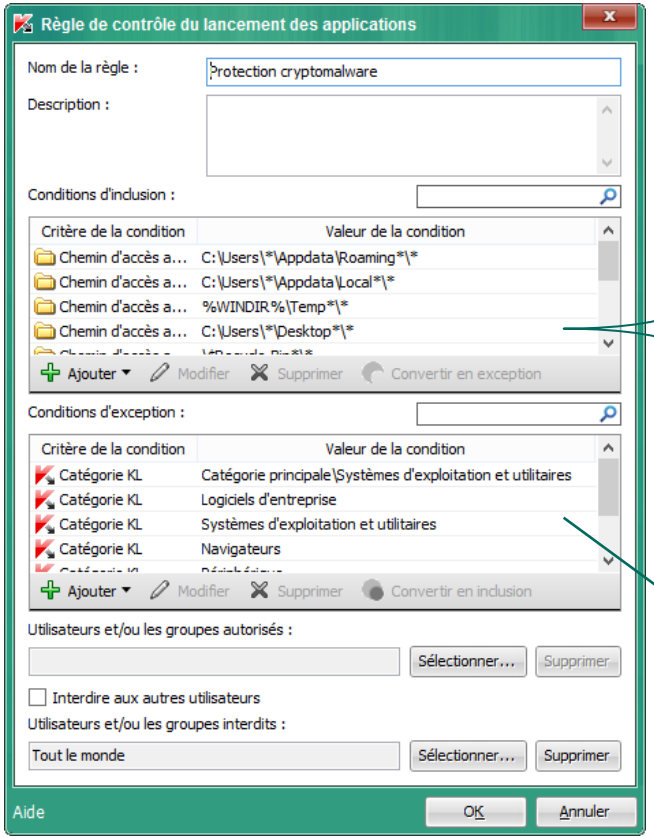
SYSTEM WATCHER : RESTAURATION DES FICHIERS CHIFFRÉS



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



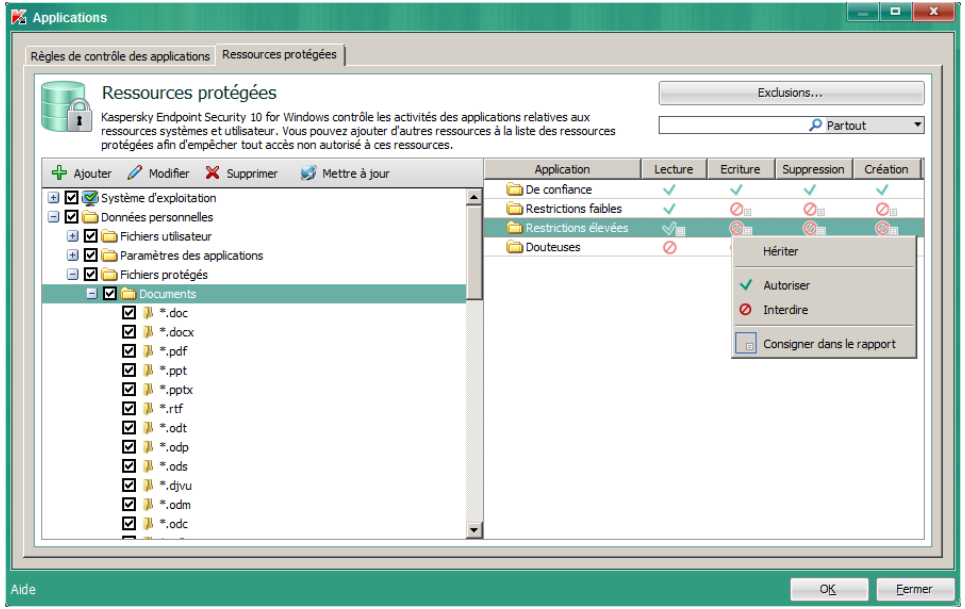
Bloquer le lancement d'applications dans certains répertoires :

- 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



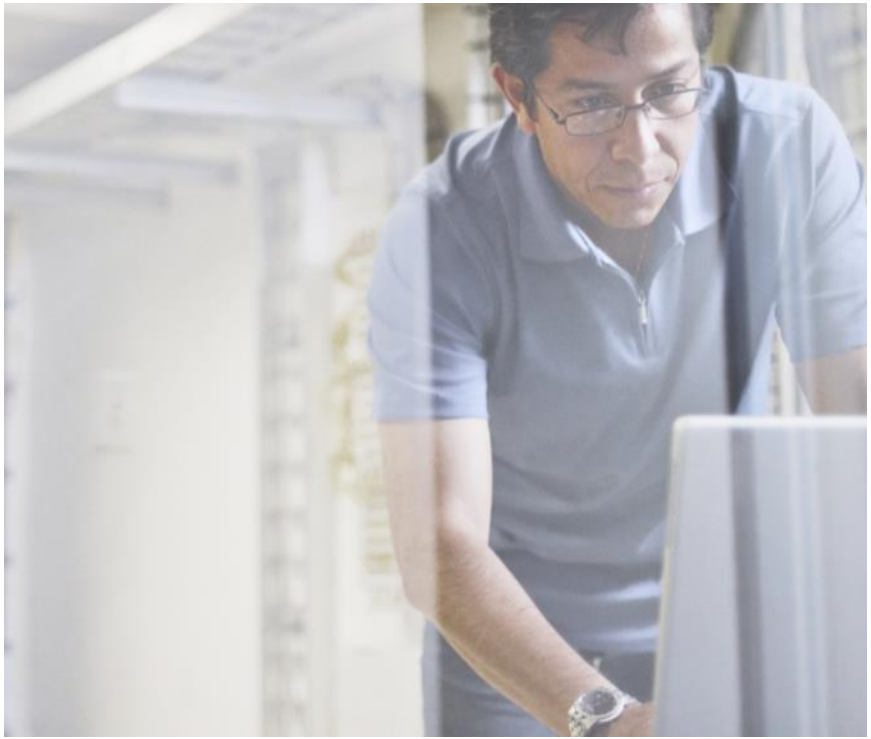
Référencer les extensions de fichiers sensibles :

- 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