Ransomware : Beaucoup de victimes, très peu de solutions

Ransomware.
Renaissance d'une attaque lucrative

Depuis quelques mois, nous assistons à l'explosion de ransomware. Avec des attaques telles que CryptoLocker ou plus récemment Petya, les ransomwares sont très médiatisés par leur aspect lucratif ainsi que leur propagation rapide et dévastatrice.

En quelques mots

Un ransomware, ou rançongiciel, est un logiciel malveillant qui **prend en otage des données personnelles**.

Ce malware chiffre des données personnelles et, par un message, demande au propriétaire **d'envoyer de l'argent en échange de la clé** qui permettra de les déchiffrer.

2 types de ransomwares :

La première catégorie : Celle des ransomwares classiques dits « policiers » qui figent votre navigateur (appelés Browlock) ou paralysent entièrement votre ordinateur.

La deuxième, de plus en plus répandue et probablement la plus néfaste, comprend les « Crypto-ransomwares » ou « cryptowares ». Le logiciel malveillant va chiffrer les documents contenus sur votre ordinateur les rendant illisibles sans la clé de déchiffrement détenue par le pirate qui exige alors une rançon en échange de cette clé.

NAISSANCE DU PREMIER RANSOMWARE

Nom	Fonctionnement	Rançon exigée	Création
PC Cyborg Trojan.	Avertissait que la licence d'un logiciel avait expiré	189$	par Joseph Popp en 1989

2012
120 000
RANSOMWARES

VS

2015
+18 000 000
RANSOMWARES

x150

UNE FAMILLE ACTIVE ET VARIÉE

...
GPcode (.AG, .AK)
Magnitude
TROJ.RANSOM.A
Archiveus
Krotten
RSA4096
Cerber
Cryzip
MayArchive
Petya
CryptoLocker
TorrentLocker
Cryptowall
TeslaCrypt
Locky Ransomware
KeRanger
CTB-Locker
WinLock
Reveton
Winwebsec
...

UN CONSTAT

Ce type d'attaque est en constante augmentation (Nouvelles attaques ou variantes)

NOUS SOMMES TOUS CONCERNÉS

Particuliers
& Entreprises de tous secteurs et tailles

Tous OS sont touchés

KERANGER
LE PREMIER RANSOMWARE VISANT LES SYSTÈMES MACOSX (2016)

CTB-LOCKER
(VARIANTE)
VISE LES SERVEURS WEB SOUS GNU/LINUX

COMMUNAUTÉ DE HACKERS

Ce n'est plus par un seul groupe mais par plusieurs groupes de personnes que sont menées les différentes campagnes de Ransomwares.

LES CAMPAGNES SONT CIBLÉES
Un exemple parlant : Locky

Visant les entreprises, la propagation de Locky est faite via des campagnes d'emails malicieux en français (mails fausses factures, free mobile etc.).

L'efficacité est ainsi redoublée par la personnalisation.

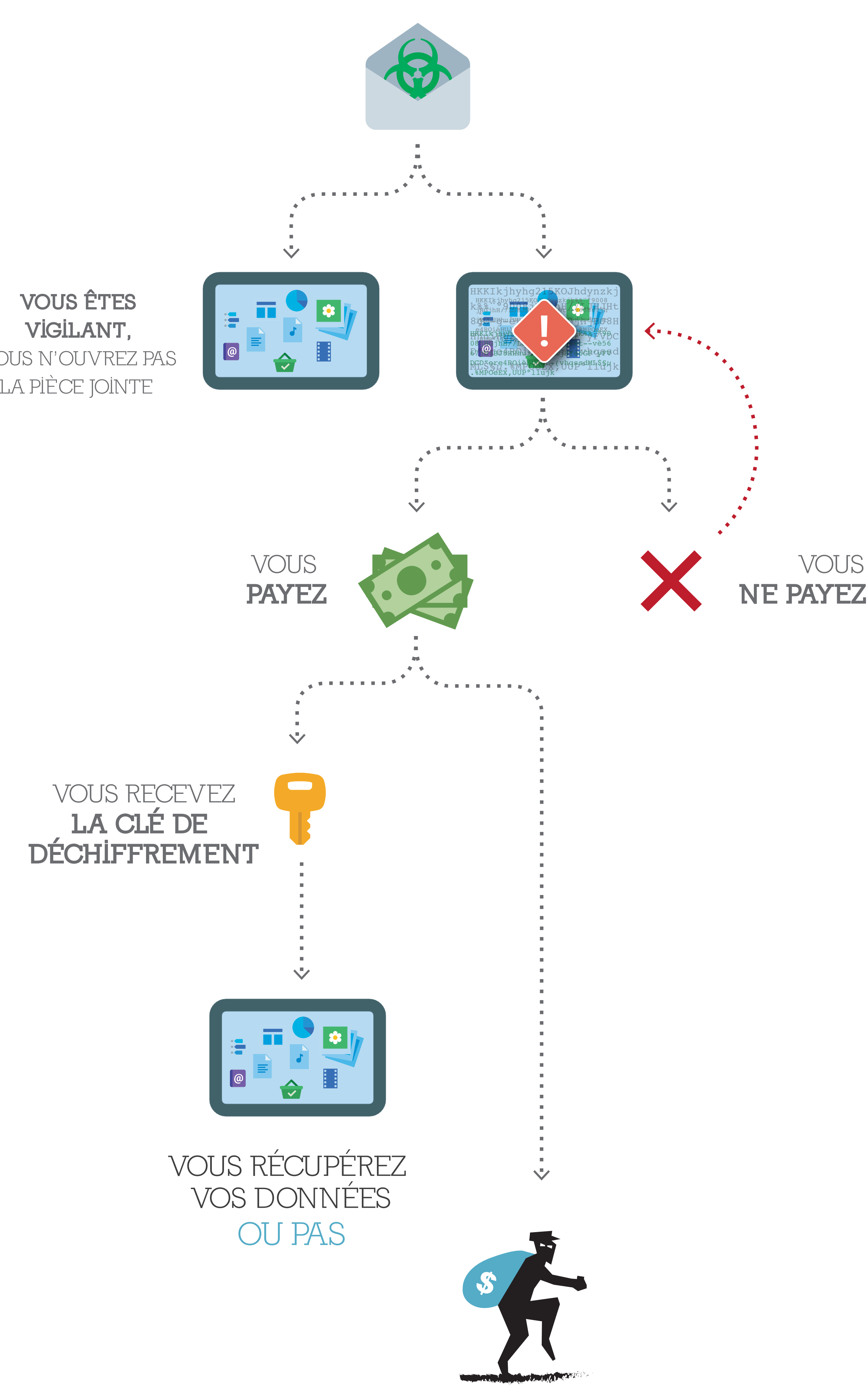
COMPLEXITÉ DU CHIFFREMENT

Les Ransomwares sont de plus en plus difficiles à déchiffrer, réduisant les chances de retrouver ses données sans payer la rançon exigée.

En très peu de temps la taille et la force des clés ont considérablement augmenté.

660 bits 2006 > 1024 bits 2008

EXPLICATION D'UNE ATTAQUE SIMPLE
DIFFUSION D'UN RANSOMWARE PAR EMAIL



LE RANÇONNEUR, LUI, RÉCUPÈRE VOTRE ARGENT

DES MÉTHODES DIFFÉRENTES

LA POP-UP DE NOTIFICATION

Un message apparaît invitant l'utilisateur à réactiver le système d'exploitation (par ex. le Windows Product Activation) ou à installer une mise à jour (par ex. le logiciel Transmission sur OSX).

Confiant, l'utilisateur va cliquer sur l'invite sans plus de vérification et ainsi déclencher l'attaque qui en quelques secondes va chiffrer l'ensemble de ses données personnelles ou une partie du système d'exploitation.

LA NOUVEAUTÉ JIGSAW

Les ransomwares sont de plus en plus sophistiqués et de nouvelles techniques apparaissent. La dernière en date avec Jigsaw qui est un ransomware avec un compte à rebours.

Si le versement de 150$ en Bitcoins n'est pas effectué dans le délai imparti, un compte-à-rebours est enclenché pour procéder à la destruction des données personnelles chiffrées.

Ainsi l'utilisateur, maintenu dans un état de stress et dans un temps de réflexion réduit, va privilégier le paiement de la rançon.

JOUER SUR LES PEURS

Certains ransomwares ne chiffrent pas les données, ils utilisent la légalité pour extorquer les utilisateurs en affichant des images à caractère pornographique ou pédo-pornographique.

Pour déverrouiller leurs postes, les utilisateurs doivent envoyer un SMS à un numéro surtaxé. Cette arnaque aurait rapporté près de 14 millions d'euros.

CRÉER SON PROPRE RANSOMWARE SANS CONNAISSANCE TECHNIQUE
RANSOMWARE AS A SERVICE

COMME UN SERVICE ?

La création des codes malveillants n'est plus le talent de quelques personnes. A présent tout à chacun peut y accéder car la génération de code malveillant est disponible en service sur le Dark Web. De fait, le niveau des menaces augmentera fortement dans les prochains mois.

COMMENT ÇA MARCHE ?

Avec des outils étape-par-étape très simples, le hacker peut élaborer rapidement son propre ransomware. Il rétribue le fournisseur de ce service en lui reversant 25% des transactions réalisées par la campagne.

Etape 1
Personnalisation

❶ Le Hacker choisit **la méthode d'attaque**

☑ Blocage
☑ Chiffrement
☐ Compte-rebours

❷ puis rédige **le message**

Message
Vos données personnelles sont cryptées
Vous venez de subir le

❸ ensuite renseigne **les informations de paiment**

bitcoin

Etape 2
Création

④ Le service **prépare le malware** selon les choix effectués

⑤ Le code est **prêt à l'emploi**

</>

Etape 3
Diffusion

C'EST PARTI !
Pour la propagation, le ransomware va utiliser de multiples méthodes comme utiliser un « exploit kit » afin d'exploiter une vulnérabilité.

...

- LES RANSOMWARE NE SE DIFFUSENT PLUS SEULEMENT PAR E-MAIL -

De multiples vecteurs d'infection

- un site internet compromis ou malveillant,
- une clé USB,
- une installation de logiciel/application de source non fiable,
- les réseaux sociaux (qui facilitent le social engineering)...

LES TÉLÉPHONES SONT MENACÉS

ANDROID, ENJEU DE MASSE.

Notre téléphone, aujourd'hui, n'est plus seulement un téléphone : y sont stockées notre répertoire et toutes ses informations (contacts, numéros, adresses, anniversaires, etc.), nos messages, nos mémos, nos photos ou encore les applications. Imaginez le potentiel pour les hackers.

Récemment est apparu un ransomware, Dogspectus, qui prend en otage les informations sur les smartphones Android pour les versions antérieures à la version 4.4.

DES SOLUTIONS
CONTRE LES RANSOMWARES

POUR UNE RÉELLE PROTECTION, IL EXISTE UNE SOLUTION PROACTIVE

Stormshield Endpoint Security

Cette protection proactive empêche le logiciel malveillant de s'exécuter sur votre ordinateur et/ou l'exploitation de la vulnérabilité (via un exploit kit).

Stormshield Endpoint Security avec sa technologie d'identification proactive de comportements malicieux permet de bloquer la majorité des ransomwares avant même qu'ils ne soient identifiés par la communauté cybersécurité.

Plus d'information :
www.stormshield.eu/fr/endpoint-protection

STORMSHIELD
COLLABORATIVE SECURITY

Stormshield, filiale à 100% d'Airbus Defence and Space, propose des solutions de sécurité de bout-en-bout innovantes pour protéger :

les réseaux
(Stormshield Network Security),
les postes de travail
(Stormshield Endpoint Security)
les données
(Stormshield Data Security).
www.stormshield.eu

QUELQUES CONSEILS INDISPENSABLES
Pour vous protéger des ransomwares

- Méfiez-vous des emails suspects avec des pièces jointes ou des sites douteux.
- Effectuer régulièrement des sauvegardes.
- Mettez à jour vos applications, plugins et systèmes d'exploitation.