Ransomware : Beaucoup de victimes, très peu de solutions

La renaissance d'une attaque lucrative

Connus depuis longtemps, ces attaques sont très utilisés par leur aspect lucratif ainsi que leur propagation rapide et dévastatrice. Aujourd'hui, nous assistons à une recrudescence de ces menaces. Comme l'indique l'ANSSI, **le nombre d'attaques a progressé de 37% entre 2020 et 2021**. De même, il y a une tendance qui se confirme dans le temps avec le Ransomware as a Service (RaaS).

Un ransomware est un logiciel malveillant qui prend en otage des données.

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

La deuxième : la plus néfaste les *Crypto-ransomwares* ou *Cryptowares* **chiffrent les documents de votre ordinateur** les rendant illisibles sans la clé de déchiffrement détenue par le pirate qui exige alors une rançon en échange de cette clé.

Pour la dernière catégorie qui est plus récente, le malware **exfiltre des données et menace leur divulgation** au propriétaire en échange de bitcoins.

7 000 euros

Coût médian d'une cyberattaque

Source : https://www.usine-digitale.fr/article/ransomware-la-cybermenace-numero-un-en-france.N1784337

Le ciblage d'infrastructures critiques à des fins de sabotage demeure une menace constante.

SELON DATOS101 **LES ATTAQUES DE RANSOMWARE ONT AUGMENTÉ DE 253%**

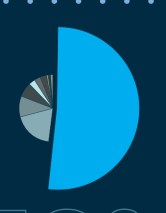
NOUS SOMMES **TOUS CONCERNÉS**

Particuliers & Entreprises de tous secteurs et tailles

Près de deux tiers des victimes de ransomware l'ont été par le biais du phishing (65%), loin devant le vol d'identifiants (39%) selon un rapport de Hiscox.

UNE FAMILLE ACTIVE ET VARIÉE

...
GPcode (.AG, .AK)
LOCKBIT 2.0
TROJ.RANSOM.A
Archiveus
Krotten
RSA4096
Cerber
Cryzip
MayArchive
Petya
CryptoLocker
TorrentLocker
Cryptowall
TeslaCrypt
Locky Ransomware
KeRanger
CTB-Locker
WinLock
Reveton
Winwebsec
...



52% des victimes sont des PME

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
Les différentes campagnes de ransomwares sont aujourd'hui par non plus un seul groupe mais **par plusieurs groupes de hackers**.

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.**

LES CRYPTOWARES
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.

UN CONSTAT
Ce type d'attaque est en constante augmentation (nouvelles attaques ou variantes)

CRÉER SON PROPRE RANSOMWARE SANS CONNAISSANCE TECHNIQUE

RANSOMWARE-AS-A-SERVICE

A présent tout à chacun peut y accéder car ***la génération de code malveillant est disponible en service*** *sur le Dark Web.*

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.

LOCKBIT 2.0

LockBit est un groupe de cybercriminels opérant selon un modèle de ransomware-as-a-service (RaaS).

Le ransomware LockBit 2.0 continue de s'adapter et d'évoluer aujourd'hui avec des attaques ciblées aux Etats-Unis, Canada ou encore l'Europe.

Les variantes les plus récentes ont adopté le modèle de la double extorsion : d'abord localiser et exfiltrer les données avant de chiffrer les systèmes.

POUR EN SAVOIR PLUS

Découvrez comment l'attaque LockBit menace les infrastructures avec **l'exfiltration et le chiffrement des données.**

Et la réponse de Stormshield avec la brique de protection **antiransomware de sa solution Endpoint Security Evolution.**

Etape 1 — Personnalisation

1. Le Hacker choisit **la méthode d'attaque**
   - [x] Blocage
   - [x] Chiffrement
   - [ ] Compte-rebours
2. puis rédige **le message**

   Message
   Vos données personnelles sont cryptées
   Vous venez de subir le verrouillage de votre poste. Pour récupérer vos données, effectuez un versement de 200€ à cette adresse :
3. ensuite renseigne **les informations de paiement**

   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 RANSOMWARES NE SE DIFFUSENT PLUS SEULEMENT PAR E-MAIL

- 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)...

COMPUTER WORM
E-MAIL MALWARE
FILELESS ATTACK
HACKER
INFECTED DEVICES
SOFTWARE VULNERABILITIES
TROJAN

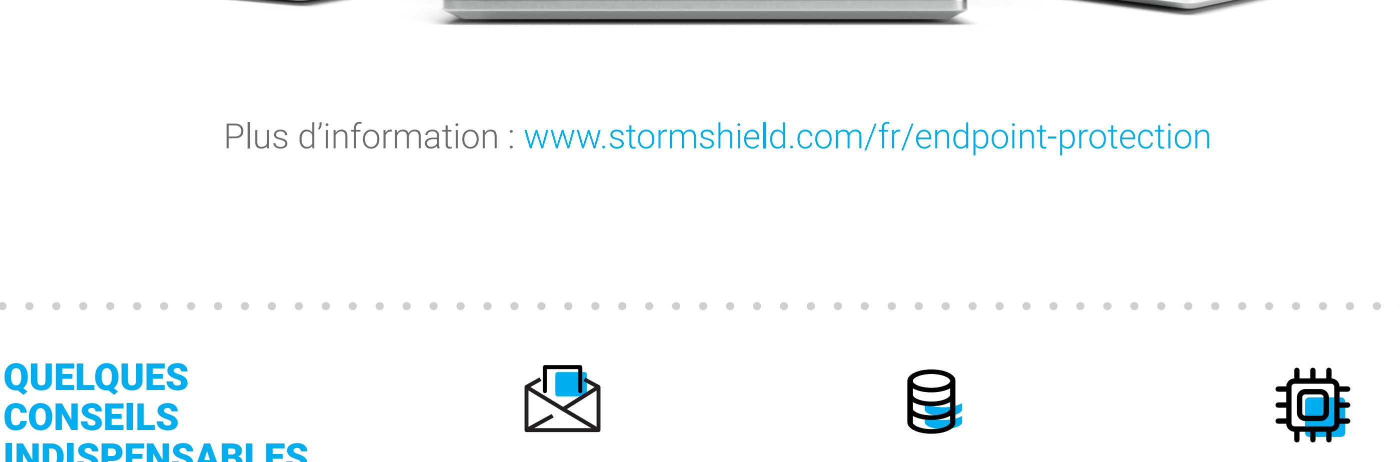
DES SOLUTIONS CONTRE LES RANSOMWARES EXISTENT

STORMSHIELD
Endpoint Security Evolution

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

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

Votre **entreprise** Grâce à **Stormshield Endpoint Security Evolution** est protégée contre les ransomwares



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

QUELQUES CONSEILS INDISPENSABLES
Pour vous protéger des ransomwares

- **Méfiez-vous** des emails suspects avec des pièces jointes
- **Sauvegardez** régulièrement
- **Mettez à jour** vos applications, plugins et systèmes d'exploitation

Copyright © Stormshield 2017-2022