Évolution des cyberattaques de type ransomwares en entreprise

BTS SIO SISR

Promotion 2025 - 2027

POSTIC Valentin

PICARD SURGELES

Plan de la situation

1. Qu'est-ce qu'une attaque par ransomware ?

1.1 Introduction

Avec la transformation numérique des organisations, les systèmes d'information sont devenus essentiels au fonctionnement des entreprises. Ils permettent de gérer les données, les communications, les transactions financières et les infrastructures techniques. Cependant, cette dépendance aux technologies informatiques expose les organisations à des cybermenaces de plus en plus nombreuses.

Parmi ces menaces, les ransomwares, également appelés rançongiciels, représentent aujourd'hui l'une des formes d'attaque les plus dangereuses pour les entreprises. Ces logiciels malveillants ont pour objectif de bloquer l'accès aux systèmes informatiques ou de chiffrer les données d'une victime afin d'exiger une rançon en échange de leur récupération.

Au cours des dernières années, les attaques par ransomware ont fortement augmenté et se sont professionnalisées. Les cybercriminels ciblent désormais principalement les entreprises, les administrations publiques, les hôpitaux ou encore les infrastructures critiques, car ces organisations dépendent fortement de leurs systèmes informatiques et sont plus susceptibles de payer une rançon pour rétablir rapidement leurs activités.

Selon les rapports de cybersécurité publiés par plusieurs organismes spécialisés, les ransomwares représentent aujourd'hui une part importante des incidents de sécurité signalés dans le monde. Les pertes financières liées à ces attaques peuvent atteindre plusieurs millions d'euros, sans compter les impacts sur l'image de l'entreprise et la perte de confiance des clients.

Dans ce contexte, il est essentiel pour les professionnels de l'informatique, notamment dans les domaines de l'administration système et réseau, de comprendre le fonctionnement de ces attaques afin de mettre en place des stratégies de protection efficaces.

Face à l'augmentation des attaques informatiques et à l'évolution constante des techniques utilisées par les cybercriminels, les ransomwares représentent aujourd'hui une menace majeure pour les entreprises.

La question principale qui se pose est donc : Comment les ransomwares ont-ils évolué au cours des dernières années et quelles solutions les entreprises peuvent-elles mettre en place pour se protéger efficacement contre ces cyberattaques ?

Pour répondre à cette problématique, cette veille technologique analysera :

le fonctionnement des ransomwares

des exemples d'attaques majeures

les impacts pour les entreprises

les moyens de protection

les évolutions récentes de ces cybermenaces.

1.2 Définition des ransomwares

Qu'est-ce qu'un ransomware ? Un ransomware est un type de malware (logiciel malveillant) qui empêche l'accès aux données ou au système informatique d'une victime en exigeant le paiement d'une rançon.

Le principe de fonctionnement repose généralement sur le chiffrement des fichiers de la victime. Les cybercriminels utilisent des algorithmes de cryptographie avancés afin de rendre les données inaccessibles.

La victime reçoit ensuite un message lui demandant de payer une rançon, généralement en crypto monnaie, afin d'obtenir la clé de déchiffrement permettant de récupérer les fichiers.

On distingue principalement deux catégories de ransomwares :

- Les ransomwares de verrouillage

Ces ransomwares bloquent l'accès à l'ordinateur ou au système d'exploitation.

Dans ce cas :

- l'utilisateur ne peut plus utiliser sa machine
- un message de rançon apparaît à l'écran.

Cependant, les fichiers ne sont pas toujours chiffrés.

- Les ransomwares de chiffrement

Les ransomwares de chiffre sont aujourd'hui les plus répandus.

Dans ce cas :

les fichiers sont chiffrés

la victime peut plus à ses données

une clé de déchiffrement est nécessaire pour récupérer les fichiers.

Les cybercriminels utilisent souvent des algorithmes comme :

AES (Norme de chiffrement avancée)

RSA (Rivest-Shamir-Adleman)

Ces algorithmes sont très robustes et rendent la récupération des données presque impossible sans la clé privée.

2. Fonctionnement d'une attaque par ransomware

2.1 Phase d'intrusion

La première étape consiste à pénétrer dans le système informatique de la victime.

Les méthodes les plus courantes sont :

- **Hameçonnage**

Le phishing consiste à envoyer un email frauduleux contenant :

une pièce jointe malveillante

un lien vers un site infecté.

Lorsque l'utilisateur ouvre la pièce jointe ou clique sur le lien, le malware s'installe sur la machine.

- Exploitation de vulnérabilités

Les cybercriminels exploitent des failles de sécurité dans des logiciels non mis à jour.

Ces vulnérabilités peuvent concerner :

les systèmes d'exploitation

serveurs web

les logiciels métiers.

- Compromis d'accès à distance

Les services d'accès distant comme **RDP (Remote Desktop Protocol)** sont souvent ciblés.

Les pirates utilisent :

des attaques par force brute

des identifiants volés.

2.2 Phase de reconnaissance

Une fois à l'intérieur du réseau, les attaquants analysent l'infrastructure informatique.

Ils recherchent notamment :

les serveurs

les bases de données

les systèmes de sauvegarde

les contrôleurs de domaine.

2.3 Phase d'élévation de privilèges

Les cybercriminels tentent ensuite d'obtenir des privilèges administrateur afin de contrôler l'ensemble du réseau.

Ils peuvent utiliser :

des outils d'administration détournés

des exploits de sécurité

des techniques de vol d'identifiants.

2.4 Propagation de phase

Le ransomware se propage dans le réseau afin d'infecter un maximum de machines.

Cela permet de maximiser l'impact de l'attaque.

2.5 Phase de chiffrement

Le malware commence alors à chiffrer les fichiers présents sur les machines.

Les fichiers ciblés incluent :

documents

bases de données

archives

fichiers professionnels.

2.6 Demande de rançon

Une fois les fichiers chiffrés, un message apparaît sur l'écran de la victime.

Ce message indique :

que les données ont été chiffrées

le montant de la rançon

la procédure pour payer.

Le paiement est généralement demandé en Bitcoin ou en Monero.

2.7. Impacts des ransomwares sur les entreprises

- Impacts sur les financiers

Les coûts peuvent inclure :

paiement de la rançon

restauration des systèmes

perte de production.

Certaines attaques ont coûté plusieurs millions d'euros aux entreprises.

- Interruption d'activité

Une attaque peut bloquer complètement l'activité d'une entreprise pendant plusieurs jours.

Cela peut entraîner :

une perte de chiffre d'affaires

un arrêt de production.

- Perte de données

Les cybercriminels peuvent :

supprimer les données

les divulguer publiément

les vendre sur le dark web.

- Atteinte à la réputation

Une cyberattaque peut nuire à l'image de l'entreprise et entraîner une perte de confiance des clients.

3. Exemples d'attaques majeures

3.1. WannaCry (2017)

WannaCry est l'une des attaques les plus importantes de l'histoire de la cybersécurité.

Elle exploitait une vulnérabilité du protocole SMB de Windows.

Conséquences :

plus de 200 000 ordinateurs infectés

150 pays touchés

hôpitaux et entreprises paralysés.

3.2 NotPetya (2017)

NotPetya est une cyberattaque très destructrice qui touche principalement l'Ukraine.

Contrairement aux ransomwares classiques, l'objectif n'était pas de récupérer de l'argent mais de détruire les systèmes informatiques.

Les pertes financières ont été estimées à plusieurs milliards de dollars.

3.3 Attaques contre les hôpitaux

Le secteur de la santé est particulièrement vulnérable aux ransomwares.

Plusieurs hôpitaux ont été victimes d'attaques ayant entraîné :

l'interruption de services médicaux

le rapport d'opérations

des risques pour les patients.

4. Moyens de protection - Rôle du technicien SISR

4.1 Sauvegardes régulières

Les sauvegardes permettent de restaurer les données sans payer la rançon.

Il est recommandé de suivre la règle 3-2-1 :

3 copies des données

2 supports différents

1 sauvegarde hors ligne.

4.2 Mise à jour des systèmes

Les mises à jour corrigent les vulnérabilités exploitées par les cybercriminels.

4.3 Sensibilisation des utilisateurs

La formation des employés est essentielle pour réduire les risques liés au phishing.

4.4 Authentification multifactorielle

L'authentification multifactorielle permet de sécuriser les accès aux systèmes.

4.5 Solutions de cybersécurité

Les entreprises peuvent utiliser :

- antivirus
- EDR
- pare-feu
- systèmes de détection d'intrusion.

5. Évolutions des ransomwares

5.1 Ransomware en tant que service (RaaS)

Le modèle RaaS permet aux cybercriminels de louer des ransomwares.

Ce système fonctionne comme un service :

un groupe développe le ransomware

d'autres cybercriminels l'utilisent

les bénéfices sont partagés.

5.2 Double extorsion

Les pirates volent les données avant de les chiffrer.

Ils menacent ensuite de publier ces données si la rançon n'est pas payée.

5.3 Attaques ciblées

Les cybercriminels ciblent désormais :

les grandes entreprises

les administrations

les infrastructures critiques.

5.4 Automatisation des attaques

Les ransomwares deviennent de plus en plus automatisés et gérés.

Les cybercriminels utilisent des outils avancés pour :

scanner les réseaux

exploiter les vulnérabilités

déploiement des logiciels malveillants.

6. Conclusion

6.1. Organisation de la veille technologique

Les ransomwares représentent aujourd'hui l'une des cybermenaces les plus importantes pour les entreprises et les organisations publiques.

L'évolution des techniques utilisées par les cybercriminels, la professionnalisation des groupes de hackers et l'augmentation des attaques ciblées rendent ces menaces particulièrement difficiles à combattre.

Les conséquences peuvent être très graves :

pertes financières importantes

interruption d'activité

fuite de données sensibles.

Pour faire face à ces risques, les entreprises doivent adopter une stratégie de cybersécurité globale comprenant :

la prévention

la détection

la réaction aux incidents.

La mise en place de bonnes pratiques, telles que les sauvegardes régulières, les mises à jour de sécurité et la formation des utilisateurs, constituent un élément essentiel pour réduire les risques liés aux ransomwares.

Dans un contexte où les cybermenaces continuent d'évoluer rapidement, la cybersécurité devient un enjeu stratégique majeur pour assurer la protection des systèmes d'information et la continuité des activités des entreprises.

6.2. Sources

rapports cybersécurité ANSSI

rapports IBM Security

rapporte Cybersecurity Ventures

études sur les ransomwares

documentation cybersécurité