# Prendre des fichiers en otage : un acte cybercriminel à l'aide de Ransomware ou Rançongiciel

**Pr Chérif DIALLO, CISSP**
Professeur Assimilé (LAFMC CAMES)
Laboratoire d'Algèbre, de Cryptographie, Codes et Applications (LACCA)
Dept Informatique, UFR Sciences Appliquées et Technologie (UFR SAT)
Université Gaston Berger (UGB), BP 234, Saint-Louis, Sénégal
E-mail: cherif.diallo@ugb.edu.sn

*"Rançon. Achat d'une chose qui n'appartient pas au vendeur, pas plus qu'elle n'appartient ensuite à l'acheteur."*
*Ambrose Bierce / Le dictionnaire du Diable*

---

**Résumé:** Face à la recrudescence des actes cybercriminels, ce bulletin mensuel de sécurité, qui est une communication de vulgarisation et de sensibilisation, présente une menace qui fait des ravages sur internet. Il s'agit des ransomwares qui ont pour objectif de bloquer l'accès aux fichiers de la victime en les cryptant moyennant un paiement de rançon pour le déblocage. Après une brève définition, nous donnerons les types de rançongiciels, les tendances actuelles de cette menace et les solutions. Enfin, nous donnerons le témoignage d'une victime récente de ransomware.

**Mots clés:** Ransomware, cybercriminalité.

---

## 1. Définition

Un ransomware ou rançongiciel est un type de logiciel malveillant (malware) utilisé par les cybercriminels. Si un ordinateur ou un réseau a été infecté par un ransomware, ce dernier bloque l'accès au système ou crypte ses données. Les cybercriminels exigent une rançon de leurs victimes en échange du déblocage de l'accès aux données. En quelque sorte, le cybercriminal prend en otage vos données et exige une rançon pour leur liberation. Les victimes d'attaques de ransomware ont souvent trois options après une infection : elles peuvent soit payer la rançon, essayer de supprimer le logiciel malveillant ou réinitialiser l'appareil et restaurer ses données. Les vecteurs d'attaque fréquemment utilisés par les ransomwares comprennent l'exploitation des faiblesses technologiques (notamment du RDP, le protocole de bureau à distance), les e-mails de phishing et les vulnérabilités logicielles. Une attaque de ransomware peut donc naturellement cibler à la fois les particuliers et les entreprises.

## 2. Types

En particulier, deux types de rançongiciels sont très populaires :

- **Rançongiciel Locker**. Ce type bloque les fonctions informatiques de base. Par exemple, l'accès au bureau de votre PC peut vous être refusé, tandis que la souris et le clavier sont partiellement désactivés. Cela vous permet de continuer à interagir avec la fenêtre contenant la demande de rançon afin d'effectuer le paiement demandé. En dehors de cela, l'ordinateur est inutilisable. Mais, les logiciels malveillants Locker ne ciblent généralement pas les fichiers critiques ; il veut généralement juste vous verrouiller. La destruction complète de vos données est donc peu probable.
- **Crypto-ransomware**. Le but du ransomware crypto est de crypter vos données importantes, telles que des documents, des images et des vidéos, mais pas d'interférer avec les fonctions informatiques de base. Cela sème la panique car les utilisateurs peuvent voir leurs fichiers mais ne peuvent pas y accéder. Les développeurs de crypto ajoutent souvent un compte à rebours à leur demande de rançon : "Si vous ne payez pas la rançon avant la date limite, tous vos fichiers seront supprimés." et donc, les crypto-ransomwares peuvent avoir un impact dévastateur. Par conséquent, de nombreuses victimes paient la rançon simplement pour récupérer leurs fichiers.

## 3. Tendances

Il y a eu une attaque de ransomware toutes les 10 secondes en 2020. Les tendances 2021 montrent une menace mondialisée accrue de ransomware, notamment :

- En septembre 2020, une clinique allemande (Düsseldorf) a été touchée par une attaque de ransomware qui a forcé le personnel à rediriger les patients d'urgence ailleurs. Par conséquent, une femme cherchant un traitement d'urgence pour une maladie potentiellement mortelle est décédée après avoir dû être transférée à plus d'une heure. La cyberattaque a détruit l'ensemble du réseau informatique de la clinique, entraînant des médecins et des infirmières incapables de communiquer entre eux ou d'accéder aux dossiers des patients.
- Les cybercriminels accèdent de plus en plus aux réseaux via le phishing, le vol d'informations d'identification, et en exploitant les vulnérabilités des logiciels.
- Le marché des rançongiciels devient de plus en plus "professionnel" et il y a eu une augmentation des services cybercriminels à louer. De plus en plus, les groupes de rançongiciels partagent entre eux des informations sur les victimes, y compris l'accès aux réseaux des victimes.
- Les cybercriminels diversifient leurs approches en extorquant de l'argent.
- Les groupes de ransomwares ont un impact croissant grâce à des approches ciblant le cloud, les fournisseurs de services gérés, les processus industriels et la chaîne d'approvisionnement en logiciels.
- Les groupes de rançongiciels ciblent de plus en plus les organisations les jours fériés et les week-ends.
- Au cours de la prochaine décennie, le coût des attaques de ransomware dépassera 265 milliards de dollars.

## 4. Solutions

Il est important de noter qu'il existe des mesures d'atténuation et des réponses appropriées aux attaques de rançongiciels. Les actions immédiates qui peuvent être prises garantissent la mise à jour rapide de tous les logiciels d'exploitation ; la mise en œuvre d'un programme de formation et de sensibilisation des utilisateurs comprenant la reconnaissance et le signalement des e-mails suspects ; sécurisation et surveillance du RDP, s'il est utilisé ; et maintenir une sauvegarde hors ligne de vos données.

Nous encourageons vivement tous les dirigeants à s'assurer que leur entreprise, organisation ou agence gouvernementale prend les mesures appropriées pour réduire les risques liés à la menace de rançongiciel.

Pour éviter les ransomwares et atténuer les dommages si vous êtes attaqué, suivez ces conseils :

- **Sauvegardez vos données**. La meilleure façon d'éviter la menace d'être verrouillé sur vos fichiers critiques est de vous assurer que vous en avez toujours des copies de sauvegarde, de préférence dans le cloud et sur un disque dur externe. De cette façon, si vous êtes infecté par un rançongiciel, vous pouvez nettoyer votre ordinateur ou votre appareil et réinstaller vos fichiers à partir de la sauvegarde. Cela protège vos données et vous ne serez pas tenté de récompenser les auteurs de logiciels malveillants en payant une rançon. Les sauvegardes n'empêcheront pas les ransomwares, mais elles peuvent atténuer les risques.
- **Sécurisez vos sauvegardes**. Assurez-vous que vos données de sauvegarde ne sont pas accessibles pour modification ou suppression à partir des systèmes sur lesquels résident les données. Les rançongiciels rechercheront les sauvegardes de données et les chiffreront ou les supprimeront afin qu'elles ne puissent pas être récupérées. Utilisez donc des systèmes de sauvegarde qui ne permettent pas un accès direct aux fichiers de sauvegarde.
- **Utilisez des logiciels de sécurité (proxy, firewall, IDS, IPS, antivirus, anti-malware, anti-spyware, anti-spam, etc.) et tenez-les à jour**. Assurez-vous que tous vos ordinateurs et appareils sont protégés par des logiciels de sécurité complets et maintenez tous vos logiciels à jour. Assurez-vous de mettre à jour le système de vos appareils tôt et souvent, car des correctifs (pour les défauts et vulnérabilités) sont généralement inclus dans chaque mise à jour.
- **Evitez de désactiver vos logiciels de sécurité**. En general les outils fiables n'exigent pas une désactivation préalable des logiciels de sécurité pour leur installation.
- **Pratiquez le surf en toute sécurité**. Faites attention où vous cliquez. Ne répondez pas aux e-mails et SMS de personnes que vous ne connaissez pas et téléchargez uniquement des applications provenant de sources fiables. Ceci est important car les auteurs de logiciels malveillants utilisent souvent l'ingénierie sociale pour essayer de vous inciter à installer des fichiers dangereux.
- **N'utilisez que des réseaux sécurisés**. Évitez d'utiliser les réseaux Wi-Fi publics, car nombre d'entre eux ne sont pas sécurisés et les cybercriminels peuvent espionner votre utilisation d'Internet. Au lieu de cela, envisagez d'installer un VPN, qui vous fournit une connexion sécurisée à Internet, où que vous alliez.
- **Rester informé**. Tenez-vous au courant des dernières menaces de ransomwares afin de savoir à quoi vous devez faire attention. Dans le cas où vous recevriez une infection par ransomware et que vous n'auriez pas sauvegardé tous vos fichiers, sachez que certains outils de décryptage sont mis à disposition par des entreprises technologiques pour aider les victimes.

- **Mettre en place un programme de sensibilisation à la sécurité**. Offrez une formation régulière de sensibilisation à la sécurité à chaque membre de votre organisation afin qu'il puisse éviter le phishing et d'autres attaques d'ingénierie sociale. Effectuez des exercices et des tests réguliers pour vous assurer que la formation est respectée.

## 5. Témoignage d'une victime

Nous avons recueilli le témoignage d'une victime de ransomware à l'Université Gaston Berger de Saint-Louis. Voici son récit*:*

*"Le 24 janvier 2022, j'étais à la recherche d'un logiciel pour le besoin de mon travail. Après plusieurs recherches sur le NET, j'ai fini par en télécharger un, pensant que le tour est joué, alors que c'est un ransomware que je venais malheureusement de télécharger à mon insu. Lorsque j'ai exécuté ce logiciel, j'ai été surpris car, à la fin de son installation, j'ai pas pu retrouver les fichiers d'installation sur mon PC. Mais à ce moment là, je n'avais toujours pas encore douté que je suis victime d'une attaque. Environ une heure après, tous mes fichiers étaient cryptés. Sur chacun des fichiers de mon ordinateur sauf certains de Windows, l'attaquant a ajouté un extension .NQHD. Sur chaque répertoire, il a ajouté un fichier readme notifiant que mes fichiers ont été cryptés et moyennant une somme de 980$USD (soit 566 000FCFA environ) pour les décrypter."*

Voici le contenu des fichiers readme :

ATTENTION!

Don't worry, you can return all your files!
All your files like pictures, databases, documents and other important are encrypted with strongest encryption and unique key.
The only method of recovering files is to purchase decrypt tool and unique key for you.
This software will decrypt all your encrypted files.
What guarantees you have?
You can send one of your encrypted file from your PC and we decrypt it for free.
But we can decrypt only 1 file for free. File must not contain valuable information.
You can get and look video overview decrypt tool:
https://we.tl/t-vrpzF37NH7
Price of private key and decrypt software is $980.
Discount 50% available if you contact us first 72 hours, that's price for you is $490.
Please note that you'll never restore your data without payment.
Check your e-mail "Spam" or "Junk" folder if you don't get answer more than 6 hours.

To get this software you need write on our e-mail:
manager@mailtemp.ch

Reserve e-mail address to contact us:
helprestoremanager@airmail.cc

Your personal ID:
0371UIhfSdSUdl1OmGEtnTuzAhKg6opDT1IROOCOtbNiRZa5si

## 6. Pour finir

Le rançongiciel est donc conçu pour crypter partiellement ou complètement le système de fichiers d'une victime, ce qui peut entraîner une perte irréversible de données. Ainsi, un nombre croissant de cybercriminels utilisent des rançongiciels pour soutirer de l'argent aux victimes. Certaines enquêtes ont montré que les pertes pour les entreprises peuvent atteindre en moyenne 2 500 dollars par incident; les entreprises étant prêtes à débourser des millions de dollars pour décrypter leurs données dans certains cas.

La menace ne fait que croître, comme le constatent certains rapports. Sonicwall, par exemple, a constaté que ce type d'attaque avait augmenté de plus de 140 % au cours du seul troisième trimestre de 2021. De plus, alors que les petites et moyennes entreprises étaient les plus à risque, les demandes de rançon atteignaient régulièrement sept, voire huit chiffres. La rançon la plus élevée confirmée avoir été payée pour le moment est de 40 millions de dollars américains, par CNA Financial, en mai 2021.