UNIVERSITÉ CÔTE D'AZUR

# Hygiène informatique & cybersécurité

SAE_11

# sommaire




Cette présentation vous sera présentée par :
> Jasmine Saoud ( 1er année BUT r&t)
> Jérémy Girard ( 1er année BUT r&t)

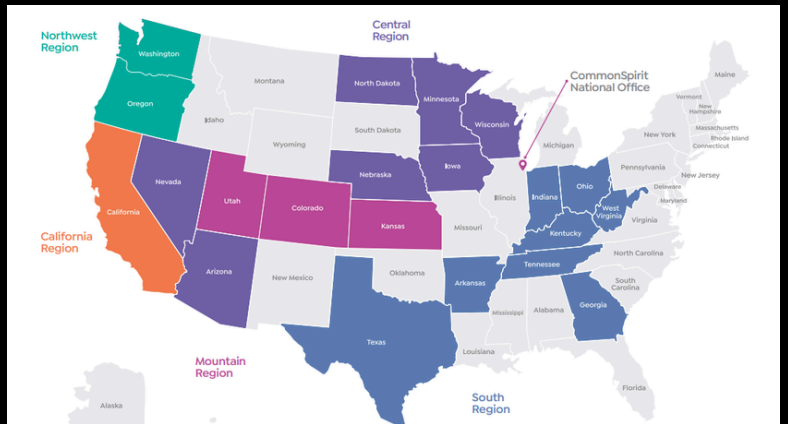
| Date | Cible | Contexte/Motivation | Pré-attaque | Dommages | Actions |
|---|---|---|---|---|---|
| Mars 2024 | Ubisoft | Dérober des données sensibles et liées à des nouveaux jeux. | Exploitation d'une faille dans les serveurs. | Vol de code source de jeux, impact sur les serveurs en ligne. | Renforcement de la sécurité et collaboration avec les autorités pour identifier les responsables. |
| Juin 2024 | T-Mobile | Accès à des données clients et des informations sensibles. | Exploitation d'une vulnérabilité du serveur. | Exposition de millions de données bancaires. | Renforcement de la protection des données et compensation des victimes. |
| Février 2024 | Viasat | Perturber des communications liées à l'Ukraine pendant la guerre. | Ransomware sophistiqué via satellite. | Impact sur des milliers de terminaux en Ukraine, perturbation des communications militaires. | Collaboration avec les agences de sécurité pour restaurer les services. |
| Avril 2024 | Gouvernement Costa Rica | Paralysation de l'administration par Conti. (groupe de hacker) | Exploitation d'une vulnérabilité informatique. | Perturbation des services publics, piratage des bases de données gouvernementales. | Mise en place d'un plan d'urgence et renforcement de la sécurité gouvernementale. |
| Mai 2023 | JBS Foods | Demande de rançon par le groupe REvil. | Introduction d'un ransomware dans le système. | Arrêt de plusieurs usines, perturbation de la production de viande aux États-Unis et au Canada. | Paiement d'une rançon de 11 millions de dollars et amélioration de la sécurité. |
| Juillet 2021 | Kaseya | Attaquer les clients de Kaseya, majoritairement des PME, via le groupe REvil. | Exploitation d'une vulnérabilité dans le logiciel. | Impact sur 1 500 entreprises dans 17 pays, données volées, systèmes paralysés. | Collaboration avec le FBI et des experts pour restaurer les services. |
| Juin 2022 | Sony PlayStation | Accéder aux informations personnelles des utilisateurs. | Exploitation d'une faiblesse dans le système PSN. | Exposition de millions de comptes utilisateurs et de données sensibles. | Renforcement de la sécurité en ligne et compensations pour les utilisateurs affectés. |
| Janvier 2023 | Facebook (Meta) | Exploiter une faille dans le système d'authentification pour accéder à des comptes utilisateurs. | Failles dans l'authentification à deux facteurs. | Vol d'informations personnelles, publications non autorisées, failles de sécurité sur le réseau. | Mise à jour immédiate de la sécurité et renforcement des mesures d'authentification. |
| Juin 2022 | Maersk | Attaque destructrice par NotPetya à large échelle. | Infection via une mise à jour compromise. | Perturbation des opérations mondiales, coût estimé à 300 millions de dollars. | Rétablissement des systèmes, enquête avec les autorités. |
| Juin 2022 | CommonSpirit Health | Motivation d'ordre financière ransomware. | Systèmes obsolètes, le phishing ciblant les employés, failles chez des prestataires. | Dans les soins, avec des retards et des annulations de traitements, ainsi qu'une interruption des systèmes critiques. | Common a isolé les systèmes affectés, fait appel à des experts en cybersécurité. |

# Date

≥ 3 octobre 2022 et à durer jusqu'au 21 octobre 2022.
www.techtarget.com

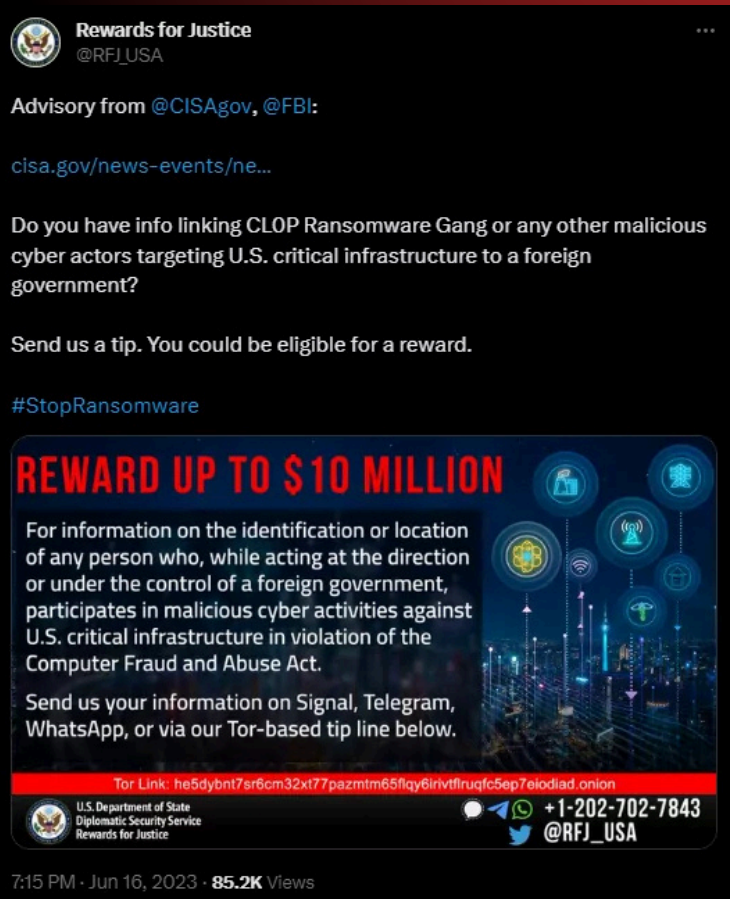
# Cible

> La cible des hackers était le réseau hospitalier "CommonSpirit Health"
www.techtarget.com




# Groupe de hacker

Les attaquants ont utilisé un ransomware sophistiqué (cryptoMix) développé par un groupe cybercriminel Clop. www.techtarget.com ; www-malwarebytes



## Contexte

Leurs motivations était surtout financière.
www.cisa.gov

## Avant

Avant l'attaque, CommonSpirit soufrer de failles de logiciels (innovacer) logiciel de planning non mis à jour, des mots de passe faibles en bref un réseau vieillissant.
www.cisa.gov


## Pendant

1. **Intrusion** : Le ransomware pénètre les systèmes le 3 octobre.
2. **Propagation** : L'attaque affecte plus de 160 établissements de santé.
3. **Exposition des données** : Des informations personnelles de 600 000 patients sont compromises.
4. **Réaction** : Les équipes rétablissent l'accès aux systèmes 21 octobre.
5. **Impact** : Des retards dans les soins et recours à des solutions manuelles.

www-malwarebytes

## Dommages

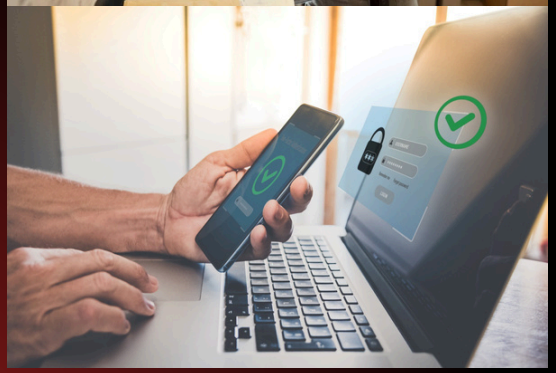
L’attaque contre CommonSpirit Health a entraîné l’annulation de soins, le détournement d’ambulances, et le vol de données sensibles.
www.techtarget.com

## Actions

Après l’attaque, CommonSpirit Health a isolé les systèmes touchés, engagé des experts en cybersécurité, collaboré avec le FBI.
www.techtarget.com

## Bonnes pratiques

CommonSpirit Health à mise en place la double authentification, formé le personnel contre le phishing et effectue des test de cybersécurité régulièrement.
www.techtarget.com

# Schématique de l'attaque