

SAÉ 11: HYGIÈNE INFO ET CYBERSECURITÉ

**ÉTUDE DE
CYBERATTAQUES**



Incident	Victime	Contexte et motif	Date	Dommages	Vulnérabilités	Actions prises
Pirate informatique de SolarWinds	Agences gouvernementales américaines et entreprises privées	Espionnage via mises à jour logicielles compromises	Décembre 2020	Données sensibles de plusieurs organisations compromises	Faiblesses dans les mécanismes de mise à jour	Corrections et sécurité renforcée
Attaque par ransomware sur Colonial Pipeline	Colonial Pipeline	Extorsion financière perturbant l'approvisionnement en carburant	Mai 2021	Opérations arrêtées, rançon de 4,4 millions \$ payée	Mauvaise gestion des mots de passe	Paiement, restauration et renforcement
Violation des serveurs Microsoft Exchange	Microsoft et ses clients	Espionnage via exploitation de vulnérabilités zero-day	Mars 2021	Emails sensibles accessibles	Vulnérabilités logicielles non corrigées	Corrections d'urgence et surveillance accrue
Violation de données chez T-Mobile	T-Mobile	Vol de données pour revente lucrative	Mars 2021	Données de 50+ millions de clients exposées	Contrôles d'accès insuffisants	Amélioration de la sécurité et notification

Incident	Victime	Contexte et motif	Date	Dommages	Vulnérabilités	Actions prises
Fuite de données Facebook	Utilisateurs de Facebook	Scraping de données à des fins de marketing ou malveillantes	Avril 2021	533 millions d'utilisateurs affectés	Protection contre le scraping insuffisante	Renforcement des protections
Attaque par ransomware sur Kaseya	Kaseya et ses clients	Ransomware visant des entreprises IT et leurs clients	Juillet 2021	1 500 entreprises impactées	Mauvaises configurations des serveurs	Corrections appliquées et négociations
Attaque par ransomware sur JBS	JBS Foods	Extorsion via perturbation des chaînes alimentaires	Mai 2021	Rançon de 11 millions \$ payée	Segmentation réseau insuffisante	Paiement, restauration et défenses renforcées
Arnaque Bitcoin sur Twitter	L'utilisateur de twitteur	Arnaque cryptomonnaies via comptes piratés	Juillet 2020	120 000 \$ volés en Bitcoin	Ingénierie sociale auprès des employés	Contrôles internes améliorés

Incident	Victime	Contexte et motif	Date	Dommages	Vulnérabilités	Actions prises
Violation de données chez Marriott	Hôtels Marriott	Accès aux données clients pour vols d'identité ou fraudes	Janvier 2020	5,2 millions de clients affectés	Processus d'authentification faibles	Notification et sécurité renforcée
Violation de données Uber	Uber	Accès aux systèmes sensibles pour rançon et reconnaissance	Septembre 2022	Données des employés et clients exposées	Identifiants administratifs mal protégés	Réponse à l'incident et renforcement



Aux Etats Unis

Cyberattaque : Salt Typhoon sur les Télécommunications, 2024

BIN ZULKIFLI Muhammad Zikry



Chronologie de l'Attaque

Printemps
2024



Début des
infiltrations
réseau.

Juin 2024



Détection des
anomalies.

Octobre
2024



Confirmation
publique de
l'attaque.

Décembre
2024



Coordination
internationale
renforcée.

FBI Warns iPhone, Android Users—Change WhatsApp, Facebook Messenger, Signal Apps

Zak Doffman Contributor 

Zak Doffman writes about security, surveillance and privacy.

Follow



Dec 10, 2024, 01:54am EST

Liens des Références

1. https://apnews.com/article/88cabc592dae2fa870772c5ce4ace5ea?utm_source=chatgpt.com
2. https://www.politico.com/news/2024/12/03/chinese-hack-global-telecom-ongoing-00192410?utm_source=chatgpt.com
3. https://www.the-sun.com/tech/13033383/fbi-urges-iphone-and-android-users-to-ditch-texting-and-opt-for-certain-app-instead-after-spike-in-hacks/?utm_source=chatgpt.com
4. https://www.reuters.com/world/us-alleges-china-hacked-calls-very-senior-political-figures-official-says-2024-12-07/?utm_source=chatgpt.com
5. https://www.reuters.com/technology/cybersecurity/us-agencies-brief-house-chinese-salt-typhoon-telecom-hacking-2024-12-09/?utm_source=chatgpt.com
6. https://www.wired.com/story/senators-warn-pentagon-salt-typhoon-china-hacking?utm_source=chatgpt.com
7. https://www.theverge.com/2024/12/5/24314330/fcc-telecom-security-rule-salt-typhoon-hack?utm_source=chatgpt.com
8. https://www.voanews.com/a/us-senators-vow-action-after-briefing-on-chinese-salt-typhoon-telecom-hacking/7887625.html?utm_source=chatgpt.com
9. https://en.wikipedia.org/wiki/Salt_Typhoon?utm_source=chatgpt.com

Le Cible: Free Mobile

- Entreprise : Free Mobile, un grand fournisseur de télécommunications français.
- Services proposés : Services de télécommunications mobiles et fixes à des millions de clients à travers la France.



Contexte

- Outils de gestion interne et données sensibles des clients, y compris les informations personnelles des abonnés mobiles et fixes.
- Une dépendance accrue aux systèmes anciens crée des vulnérabilités lorsqu'ils ne sont pas correctement mis à jour.

Vulnérabilités trouvé avant l'attaque

- Contrôles d'accès faibles :
 - Mécanismes d'authentification inadéquats sur les outils de gestion interne.
 - Absence potentielle d'authentification à plusieurs facteurs (MFA).
- Systèmes anciens :
 - Systèmes obsolètes avec des mises à jour insuffisantes, créant des points d'entrée exploitables.
- Surveillance et détection insuffisantes :
 - Une détection retardée des accès non autorisés, permettant aux attaquants d'exfiltrer des données sans être immédiatement remarqués.

Déroulement de l'attaque

- Étape 1 : Intrusion
 - Les pirates ont obtenu un accès non autorisé grâce à des vulnérabilités dans les outils internes de Free Mobile.
- Étape 2 : Exploitation
 - Les attaquants ont extrait les données des clients, y compris les noms, adresses, informations de contact et peut-être les détails de facturation.
- Étape 3 : Vente de données
 - Les données volées ont été listées sur des forums cybercriminels, menant à la découverte publique de la violation.
- Étape 4 : Réponse
 - Free Mobile a identifié l'accès non autorisé et a commencé des efforts de confinement.

Dommages causés par l'attquant

- Compromission des données :

- Les détails personnels de millions de clients ont été exposés.
- Les abonnés mobiles et fixes ont été affectés.

- Dommages à la réputation :

- Perte de confiance parmi les clients.
- Augmentation de la surveillance par les organismes de régulation.

- Impact financier :

- Coûts potentiels pour les actions légales, les indemnisations et les améliorations de la cybersécurité.

- Risques pour la sécurité des clients :

- Les utilisateurs affectés ont fait face à des risques accrus de vol d'identité et d'attaques par hameçonnage.

Actions

Confinement et enquête

Notification et accompagnement des utilisateurs



Renforcement des mesures de sécurité

Conformité légale et réglementaire

Bonnes pratiques

1. Renforcement de la sécurité des systèmes de gestion et surveillance des forums du Dark Web pour détecter toute fuite de données.
2. Mise en place d'une authentification multi-facteurs (MFA) pour ajouter une couche de sécurité supplémentaire.
3. Communication rapide avec les clients en cas de fuite de données, pour limiter les dommages.

