

# Tableau récapitulatif pour les 10 cyberattaques

	DATE/CIBLE	MOTIVATION	PRE-ATTAQUE	DOMMAGES	ACTIONS
MOLOTOV	<ul style="list-style-type: none"><li>Début octobre en 2024</li><li>Service de télévision en streaming français</li></ul>	<ul style="list-style-type: none"><li>Vulnérabilité</li><li>Attaque par ransomware, donc motivation financière</li></ul>	<ul style="list-style-type: none"><li>Exploitation des failles</li><li>Phishing</li></ul>	<ul style="list-style-type: none"><li>Opérationnel</li><li>Infos personnelles exposées</li><li>Reputation</li><li>Financier</li></ul>	<ul style="list-style-type: none"><li>Investigation</li><li>Securité renforcer</li><li>Sensibilisation</li></ul>
CRYPTO.COM	<ul style="list-style-type: none"><li>Janvier 2022</li><li>Plateforme d'échange de cryptomonnaies majeure</li></ul>	<ul style="list-style-type: none"><li>Vulnérabilité</li><li>Vol financier</li><li>Anonymat</li></ul>	<ul style="list-style-type: none"><li>Exploitation des failles</li><li>Phishing</li></ul>	<ul style="list-style-type: none"><li>Vol de fonds</li><li>Perturbation des services</li><li>Reputation</li></ul>	<ul style="list-style-type: none"><li>Authentification</li><li>Worldwide Account Protection Program</li></ul>
MEDIBOARD	<ul style="list-style-type: none"><li>19 Novembre 2024</li><li>Hopital Franais (Ile de France)</li></ul>	<ul style="list-style-type: none"><li>Financier</li><li>Infos personnelles</li></ul>	<ul style="list-style-type: none"><li>Vol d'identifiant</li></ul>	<ul style="list-style-type: none"><li>Exposition d'infos personnelles</li><li>Réputation</li></ul>	<ul style="list-style-type: none"><li>Investigation</li><li>Rassurent les patients</li></ul>
HYP CREDIT GUARD	<ul style="list-style-type: none"><li>10 Novembre 2024</li><li>Societe qui permet de gerer les cartes de credits</li></ul>	<ul style="list-style-type: none"><li>Pénétrer les défenses cybernétiques d'Israel</li><li>Endommager le pays</li></ul>	<ul style="list-style-type: none"><li>Aucune information/Non précisé</li></ul>	<ul style="list-style-type: none"><li>Opérationnel</li><li>Financier</li></ul>	<ul style="list-style-type: none"><li>Contré l'attaque</li><li>Investigation</li></ul>
FREE	<ul style="list-style-type: none"><li>Fin Octobre 2024</li><li>Principal fournissuers d'accès internet en France</li></ul>	<ul style="list-style-type: none"><li>Beaucoup d'information personnelles</li><li>Financier</li></ul>	<ul style="list-style-type: none"><li>Phishing</li></ul>	<ul style="list-style-type: none"><li>Vol de 19.2 millions infos personnelles</li><li>Vol de 5 millions IBAN</li><li>Reputation</li></ul>	<ul style="list-style-type: none"><li>Investigation</li><li>PDG de Twitter mis en prison</li></ul>

# Tableau récapitulatif pour les 10 cyberattaques

	DATE/CIBLE	MOTIVATION	PRE-ATTAQUE	DOMMAGES	ACTIONS
<b>NASA and the DoD Hack</b>	<ul style="list-style-type: none"> <li>Début octobre en 1999</li> <li>NASA et</li> </ul>	<ul style="list-style-type: none"> <li>Auto-Promo</li> <li>Voler des logiciels très couteux (\$1.7 million )</li> </ul>	<ul style="list-style-type: none"> <li>faille de sécurité</li> <li>backdoor sur un serveur du DOD</li> </ul>	<ul style="list-style-type: none"> <li>\$41,000 de dégat</li> <li>21 jours de suspend sur tout le reseau de la NASA</li> </ul>	<ul style="list-style-type: none"> <li>Verification metuculeuse des failles</li> </ul>
<b>Estate Wealth Network Leak</b>	<ul style="list-style-type: none"> <li>vpnMentor</li> <li>décembre 2023</li> </ul>	<ul style="list-style-type: none"> <li>Voler des données touchant des millions de personnes</li> </ul>	<ul style="list-style-type: none"> <li>Une base de donnée sans protection par mot de passe</li> </ul>	<ul style="list-style-type: none"> <li>1,5 milliard de dossiers exposés</li> </ul>	<ul style="list-style-type: none"> <li>bloque l'accès au public</li> <li>aide d'un chercheur externe Jeremiah Fowler</li> </ul>
<b>OPÉRATION AURORA</b>	<ul style="list-style-type: none"> <li>34 grosses organisations américaines</li> <li>réveler le 12 janvier 2010 par <u>Google</u></li> </ul>	<ul style="list-style-type: none"> <li>Espionnage</li> <li>Vol de secrets industriel et autre info sensible</li> </ul>	<ul style="list-style-type: none"> <li>Systems out dated</li> <li>Faille zero-day dans internet explorer</li> </ul>	<ul style="list-style-type: none"> <li>Degradation des relations geopolitique</li> <li>perte de confiance en vers les entreprises</li> <li>Perturbation des systèmes de diagnostic et pharmaceutique</li> </ul>	
<b>TORONTO SICKKIDS</b>	<ul style="list-style-type: none"> <li>Fin 2022</li> <li>hôpital SickKids de Toronto</li> </ul>	<ul style="list-style-type: none"> <li>financières</li> </ul>	<ul style="list-style-type: none"> <li>Aucune information/Non précisé</li> </ul>		<ul style="list-style-type: none"> <li>Engager des experts en cyber</li> <li>investissement pour la cyber</li> </ul>
<b>FRANCE</b>	<ul style="list-style-type: none"> <li>Janvier 2024</li> <li>assurance santé Viamedis et Almerys</li> </ul>	<ul style="list-style-type: none"> <li>Beaucoup d'information personnelles</li> <li>Financier</li> </ul>	<ul style="list-style-type: none"> <li>phishing ciblant les professionnels de santé</li> </ul>	<ul style="list-style-type: none"> <li>donnée de 33 millions de personnes volé (la moitié de tout les français)</li> </ul>	<ul style="list-style-type: none"> <li>Enquête contre les assureurs par le CNIL</li> </ul>

# MOLTOV

- Début octobre en 2024
- Molotov service de télévision en streaming français
- RaaS (Ransomware-as-a-Service), des cybercriminels spécialisés dans les attaques par ransomware
- Motivations
  - Beaucoup d'informations personnelles
  - Aspect financier



# SCHEMA DE L'ATTQUE



1.Failles:  
Systèmes de gestion des accès et dans les logiciels non mis à jour.



2.Phishing:  
envois de mail frauduleux aux employés



3.Exfiltration/Ransomware:  
Exfiltration de données sensible/ encryption de données



4.Interruption des systèmes:  
les systèmes de Molotov hors service



5.Rançon:  
pour fournir la clé de déchiffrement

# DOMMAGES

# ACTIONS



- Impact sur les services
- Exposition des données personnelles
- Réputation endommagé
- Financier



- Investigation interne
- Renforcement de la sécurité
- Sensibilisation

# 33 million de Français

Le cas Viamedis et Almerys





**Date**

Janvier 2024

**Cible**

Assurance santé Viamedis et  
Almerys

**Hacker**

Malgres l'enquête de la CNIL,  
les hackers restent inconnus

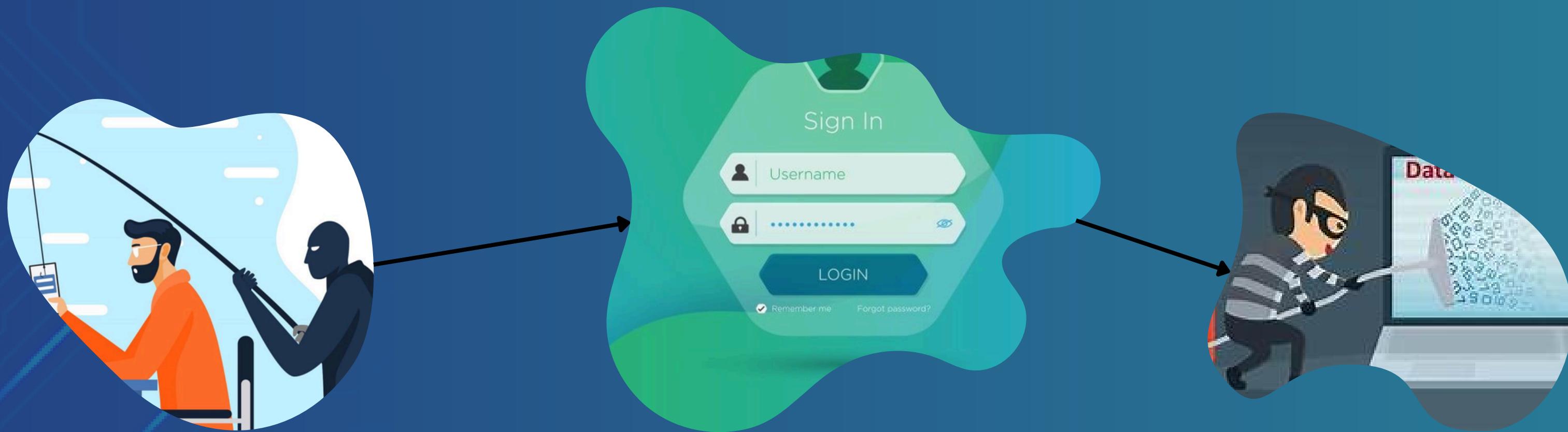
**Motivation**

Domaine de la santé regorge  
d'information personnel

**Failles**

Spécialistes de santé non  
informés aux risques

# Schéma de l'attaque



Phishing sur des  
professionnels de santé

Prise de contrôle des  
portails sécurisés  
sensible

Exfiltration des données



50% de la population  
Française touché

Des informations concernant  
33 millions de français incluant :

- Numéro de sécurité sociale
- statuts civils
- informations sur les assureurs

Cette fuite expose les victimes à des risques accrus



**Usurcation Identité**



**Phishing**



**Fraude**

# Enquête mené par la CNIL



Commission nationale  
de l'informatique et des libertés

# Bonnes pratiques

1

Sensibiliser les personnes à  
risque

2

Attribuer moins de priviléges

3

Des normes plus strictes

# SOURCES

- [https://www.frandroid.com/services/svod/2400398\\_fuites-de-donnees-en-serie-apres-free-et-picard-molotov-est-a-son-tour-victime-dune-cyberattaque](https://www.frandroid.com/services/svod/2400398_fuites-de-donnees-en-serie-apres-free-et-picard-molotov-est-a-son-tour-victime-dune-cyberattaque)
- <https://konbriefing.com/en-topics/cyber-attacks.html>
- <https://www.cbsnews.com/news/crypto-com-hack-bitcoin-ethereum-30-million/>
- <https://www.ouest-france.fr/societe/cyberattaque/cyberattaque-de-free-comment-savoir-et-que-faire-si-vous-etes-victime-du-vol-de-donnees-c7957a5a-96cd-11ef-9921-e056d0673e10>
- [https://www.lemonde.fr/pixels/article/2024/02/09/donnees-volees-aux-mutuelles-de-sante-le-parquet-de-paris-ouvre-une-enquete-apres-les-cyberattaques-de-viamedis-et-almerys\\_6215719\\_4408996.html](https://www.lemonde.fr/pixels/article/2024/02/09/donnees-volees-aux-mutuelles-de-sante-le-parquet-de-paris-ouvre-une-enquete-apres-les-cyberattaques-de-viamedis-et-almerys_6215719_4408996.html)
- <https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2024/fallout-from-viamedis-almerys-attack-does-not-end-with-the-data-leak>
- <https://emag.directindustry.com/2024/02/08/health-insurance-cyberattack-33-million-french-citizens-fall-victim-to-data-theft/>