Sujet : L’évolution des ransomwares et leurs nouvelles techniques d’attaque

A / Réalisation des étapes de la veille

1. Définir son besoin

Sujet choisi :

L’évolution des ransomwares et leurs nouvelles méthodes d’attaque.

Pourquoi ce sujet ?

Les ransomwares représentent aujourd’hui l’un des plus grands dangers informatiques pour les entreprises comme pour les particuliers. Les techniques évoluent très vite (double extorsion, vol de données, IA pour automatiser les attaques). Comprendre ces évolutions permet d’anticiper les risques et de mieux protéger les systèmes informatiques.

Questions que je me pose :

- Quelles sont les nouvelles formes de ransomwares ?
- Quelles techniques utilisent les cybercriminels aujourd’hui ?
- Quelles entreprises sont les plus touchées ?
- Quels impacts économiques et organisationnels ?
- Quelles solutions de protection existent ?
- Quels groupes (Lockbit, BlackCat…) sont les plus actifs ?

Mots-clés principaux

- ransomware
- rançongiciel
- attaque ransomware
- ransomware evolution
- ransomware trends
- ransomware 2024 / 2025
- ransomware-as-a-service (RaaS)
- RaaS
- double extorsion
- triple extorsion
- data exfiltration
- chiffrement malveillant

Groupes / familles à surveiller

- LockBit
- / ALPHV
- Medusa
- Rhysida
- Cl0p
- Conti (historique, mais utile)
- Royal ransomware
- Hive ransomware

Expliquer pourquoi et dire leurs évolutions

2. Identifier les source

Presse spécialisée présente au CDI :

- 01Net
- Le Monde Informatique
- ZDNet
- Science & Vie – hors-série tech
- Hackers & Security (si disponible)

Accès documentaires :

- Portail Esidoc du lycée (recherches : “ransomware”, “attaque informatique”, “cybersécurité”)
- Europresse (presse nationale et internationale sur les cyberattaques)

Sites internet utiles

- ANSSI (Agence Nationale de Sécurité des Systèmes d’Information)
- CERT-FR
- CNIL
- ZDNet Cybersécurité
- LeMagIT
- BleepingComputer
  Cybermalveillance.gouv.fr
- Blog Kaspersky / Avast / Malwarebytes
- The Hacker News (Cybersécurité)

3. Collecter les informations

Pour ma veille, je vais utiliser plusieurs méthodes :

- Sur Esidoc : j'entre les mots-clés "ransomware", "cyberattaque", "menaces numériques", "Lockbit" et j'épingle les articles.
- Sur Europresse : je recherche les actualités récentes et j'exporte en PDF les articles importants.
- Je feuillette régulièrement les magazines du CDI, je prends en photo les pages utiles.
- J'utilise Google News et Flipboard avec les mots-clés "cybersécurité", "attaque ransomware", "hacking".
- Je crée une Google Alert sur : "ransomware 2025 attaque France".
- J'utilise Feedly pour suivre les flux RSS de :
    - ANSSI
    - Le Monde Informatique
    - The Hacker News
-
- Je fais des captures d'écran de mes espaces de veille (Google Alert, Feedly, Europresse…).

4. Sélectionner et analyser

- Sur Esidoc : je lis les notices, je récupère les magazines au CDI et je scanne les articles utiles.
- Sur Europresse : j'exporte les articles les plus pertinents en PDF (ex : attaques récentes, nouvelles techniques, impacts économiques).
- Sur mes autres outils (Flipboard, Feedly, Google Alert), je garde les articles en favoris.
- Je compile toutes mes trouvailles dans un mur collaboratif (Padlet / Digipad / Teams).

Principales idées que j’analyse :

- Les ransomwares deviennent plus sophistiqués et utilisent parfois l’IA.
- Les groupes criminels fonctionnent comme de véritables entreprises (RaaS : Ransomware-as-a-Service).
- Beaucoup d’attaques utilisent la double extorsion (vol + chiffrement des données).
- Les impacts financiers sont énormes pour les entreprises attaquées.
- Les meilleures protections restent : sauvegardes déconnectées, MFA, correctifs réguliers, sensibilisation du personnel.

5. Diffuse

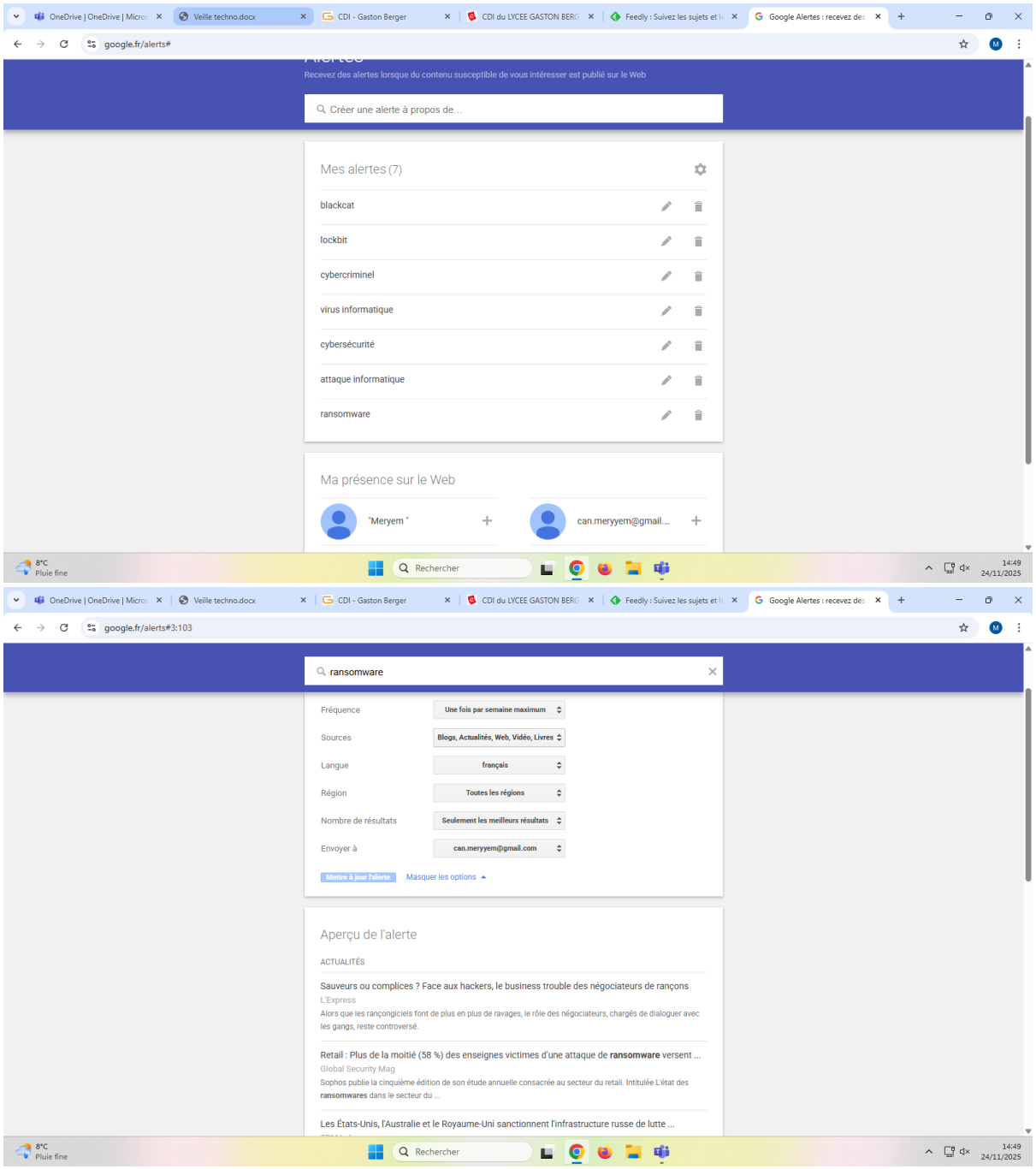
- Je fais des captures d’écran de toutes les étapes de mon travail
- Je dépose ces images dans l’espace Teams demandé par le professeur.

B / Planification de la veille régulière

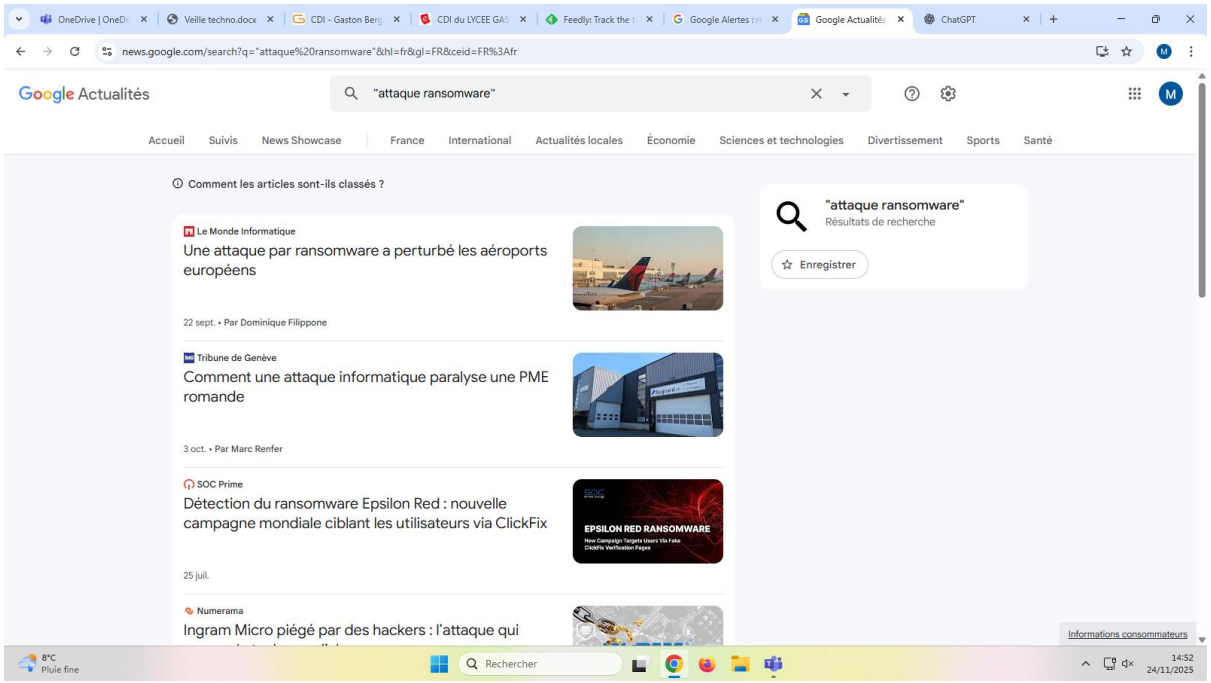
Je choisis un moment dans la semaine pour refaire les étapes 3 à 5.

Jour de la semaine : vendredi

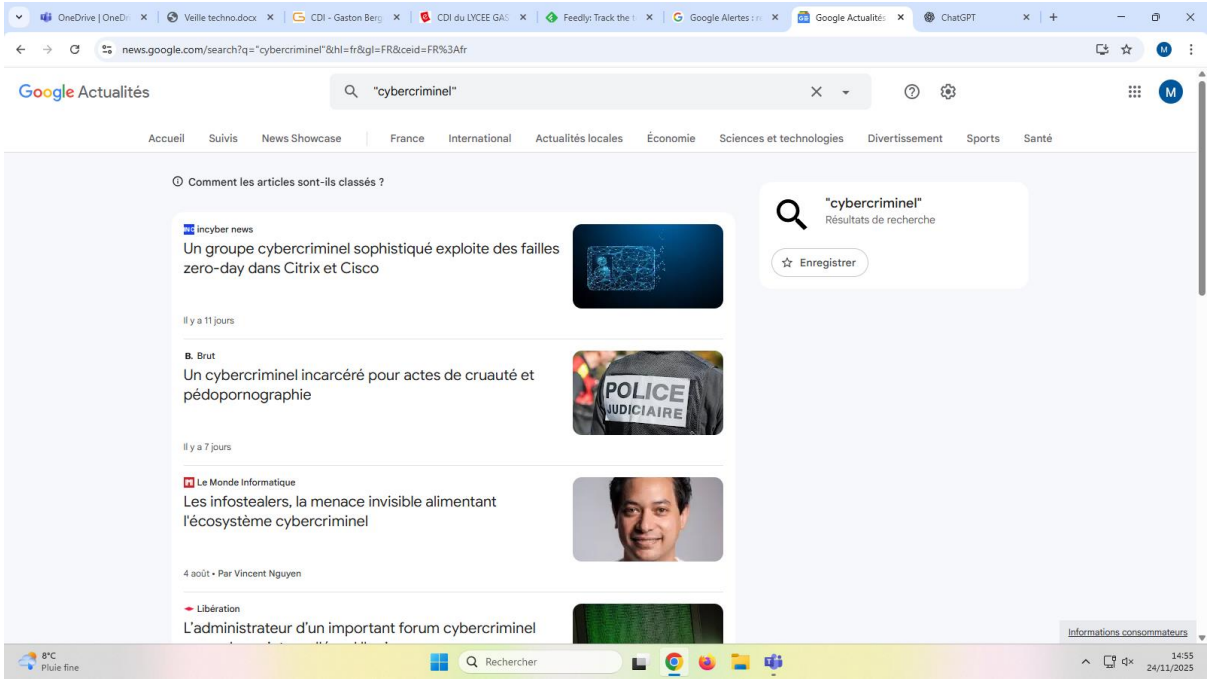
Heure : 17H30

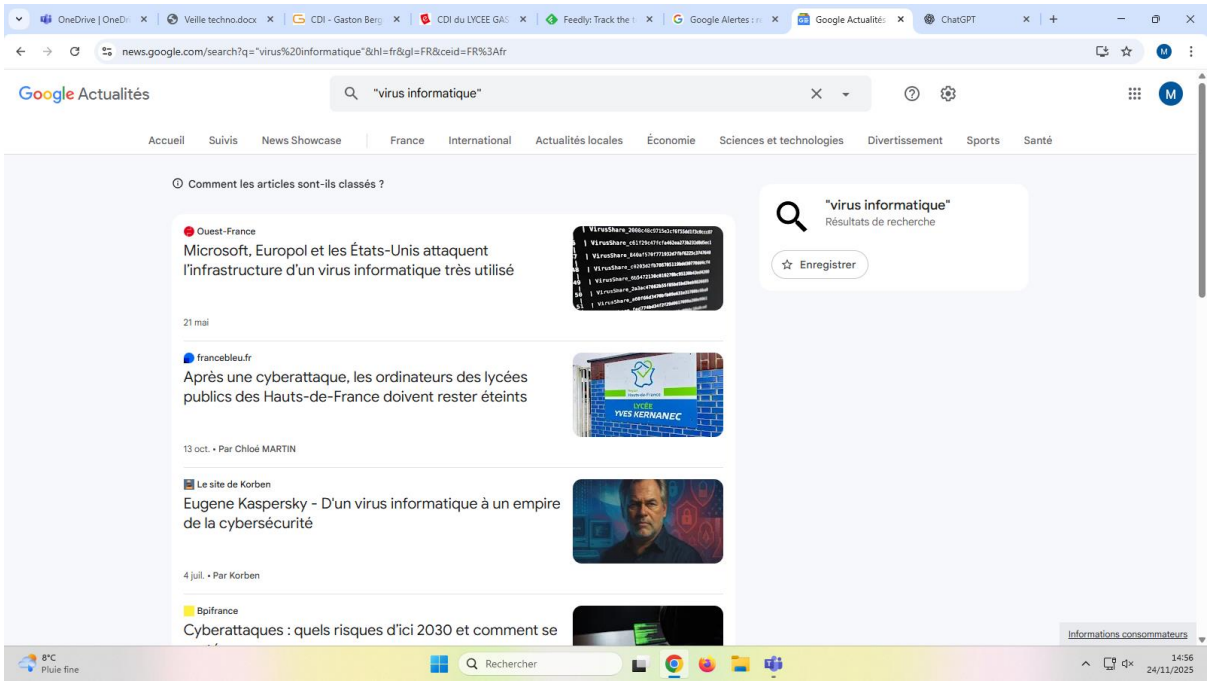


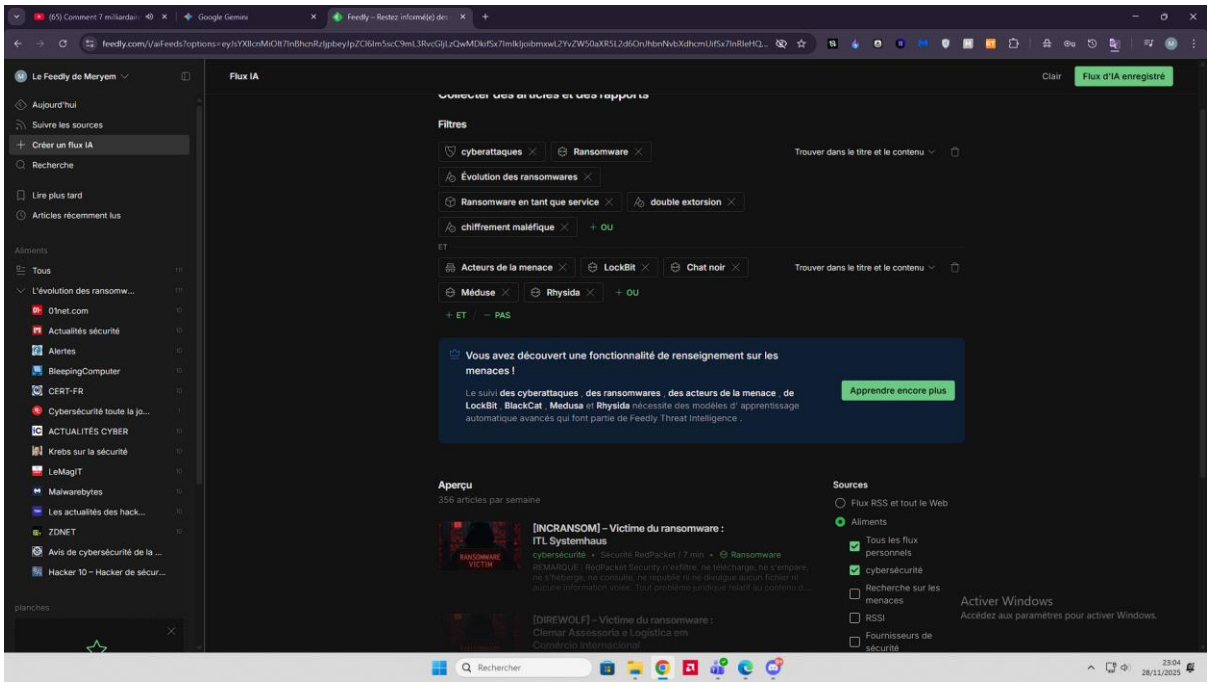
https://www.google.fr/alerts#



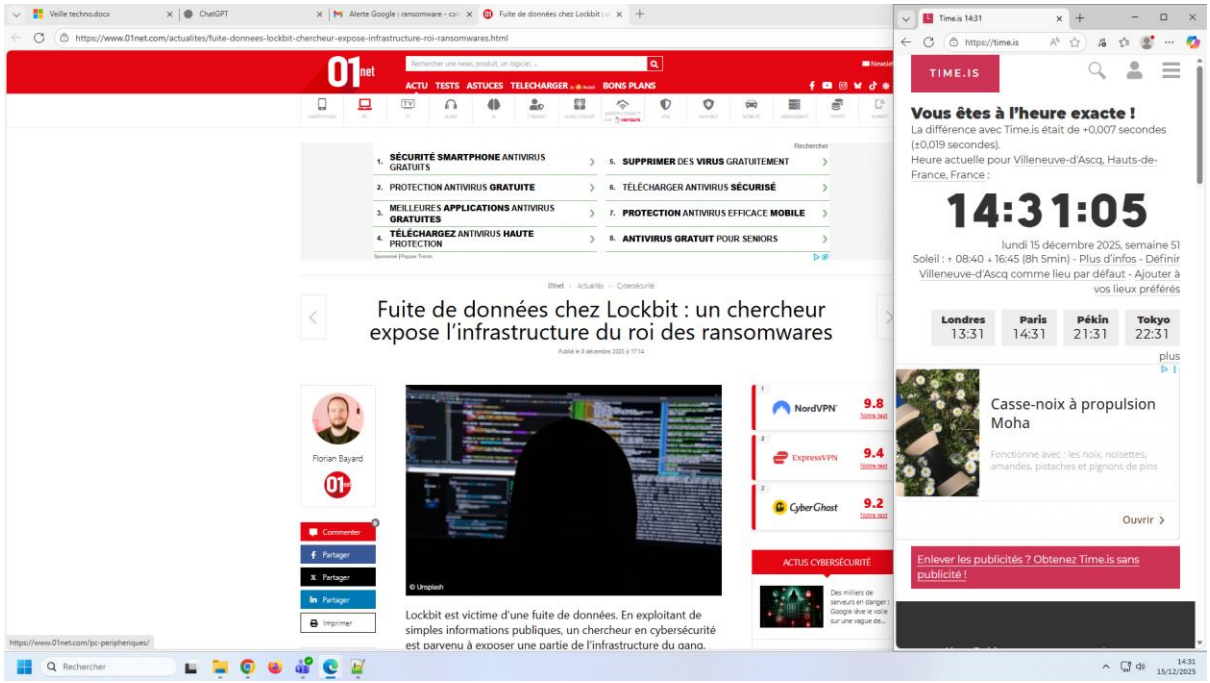
https://news.google.com/search?q=%22attaque%20ransomware%22&hl=fr&gl=FR&ceid=FR%3Afr



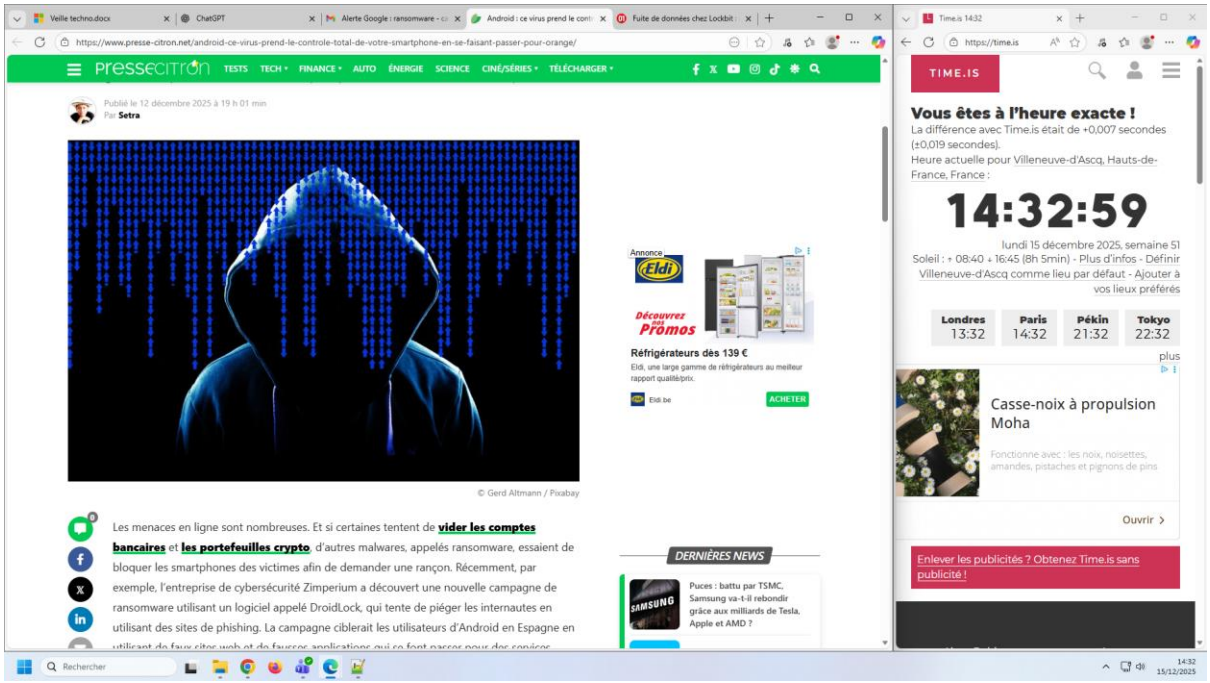

Google Actualités
"virus informatique"
Accueil
Suivis
News Showcase
France
International
Actualités locales
Économie
Sciences et technologies
Divertissement
Sports
Santé
Comment les articles sont-ils classés ?
"virus informatique"
Résultats de recherche
Enregistrer
Ouest-France
Microsoft, Europol et les États-Unis attaquent l'infrastructure d'un virus informatique très utilisé
21 mai
francebleu.fr
Après une cyberattaque, les ordinateurs des lycées publics des Hauts-de-France doivent rester éteints
13 oct. • Par Chloé MARTIN
Le site de Korben
Eugene Kaspersky - D'un virus informatique à un empire de la cybersécurité
4 juil. • Par Korben
Bpifrance
Cyberattaques : quels risques d'ici 2030 et comment se
Informations consommateurs


Le Feedly de Meryem
Flux IA
Clair
Flux d'IA enregistré
Filtres
cyberattaques
Ransomware
Trouver dans le titre et le contenu
Évolution des ransomwares
Ransomware en tant que service
double extorsion
chiffrement malefique
Acteurs de la menace
LockBit
Chat noir
Méduse
Rhysida
Vous avez découvert une fonctionnalité de renseignement sur les menaces !
Apprendre encore plus
Aperçu
356 articles par semaine
Sources
Flux RSS et tout le Web
Aliments
Activer Windows

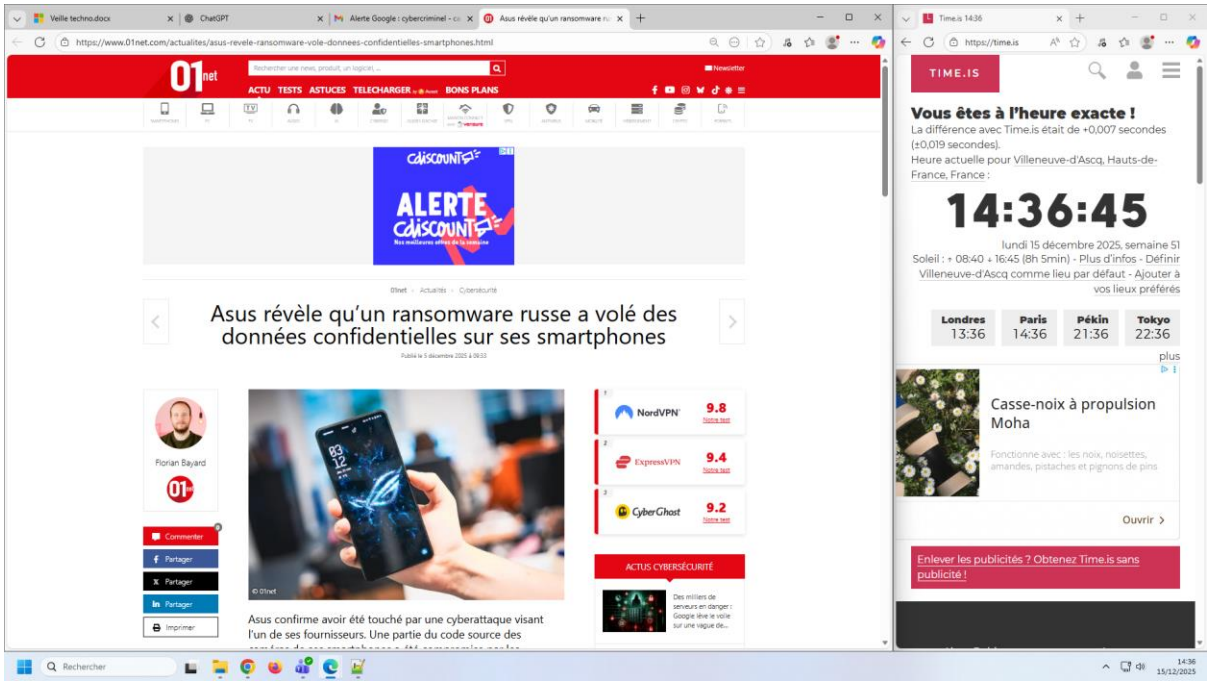
Feedly.com



L'article de 01net du 8 décembre 2025 explique qu'un chercheur en cybersécurité a réussi à exposer une partie de l'infrastructure du ransomware LockBit 5.0, considéré comme l'un des plus dangereux groupes de ransomware actuels. Il a identifié un serveur accessible publiquement via RDP, ce qui montre des failles importantes même chez les cybercriminels. Cette fuite peut aider les spécialistes de la sécurité à bloquer ou réduire l'impact de ce ransomware en identifiant et en mettant hors ligne les serveurs compromis.



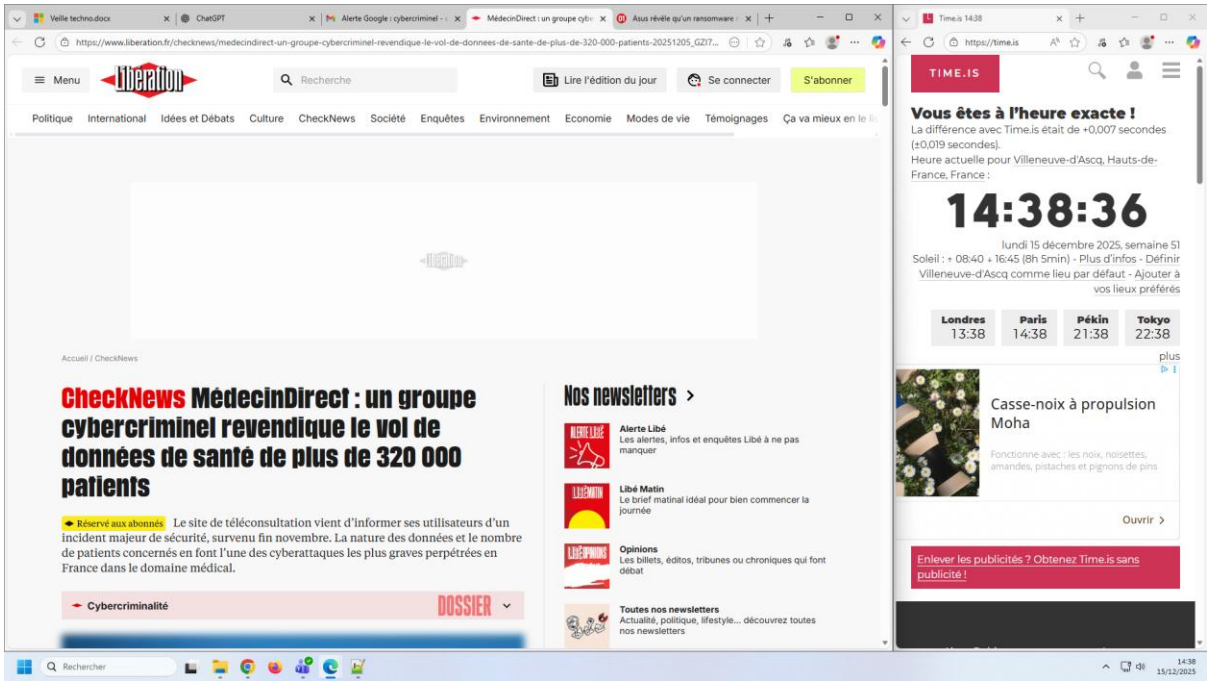
Une campagne de malware Android appelée *DroidLock* utilise des faux sites imitant des services comme Orange pour inciter les utilisateurs à installer une application malveillante. Une fois installée, cette application demande des permissions critiques qui lui permettent de prendre le contrôle total du smartphone, bloquer l'écran et afficher une demande de rançon. Ce type d'attaque mobile montre que les ransomwares évoluent aussi sur plateformes mobiles et exploitent le phishing et les permissions d'accessibilité pour nuire aux victimes.



Asus a confirmé qu'un de ses fournisseurs a été compromis par une attaque de ransomware revendiquée par le groupe Everest, un gang cybercriminel russe spécialisé dans l'extorsion et le chiffrement de données. Les attaquants ont réussi à voler plus d'un téraoctet de données, notamment une partie du code source des caméras de certains smartphones Asus.

Le ransomware a non seulement demandé une rançon, mais aussi potentiellement exfiltré des données sensibles, ce qui montre une pratique moderne de double extorsion (vol + chiffrement) souvent utilisée par les groupes criminels pour augmenter la pression sur leurs victimes.

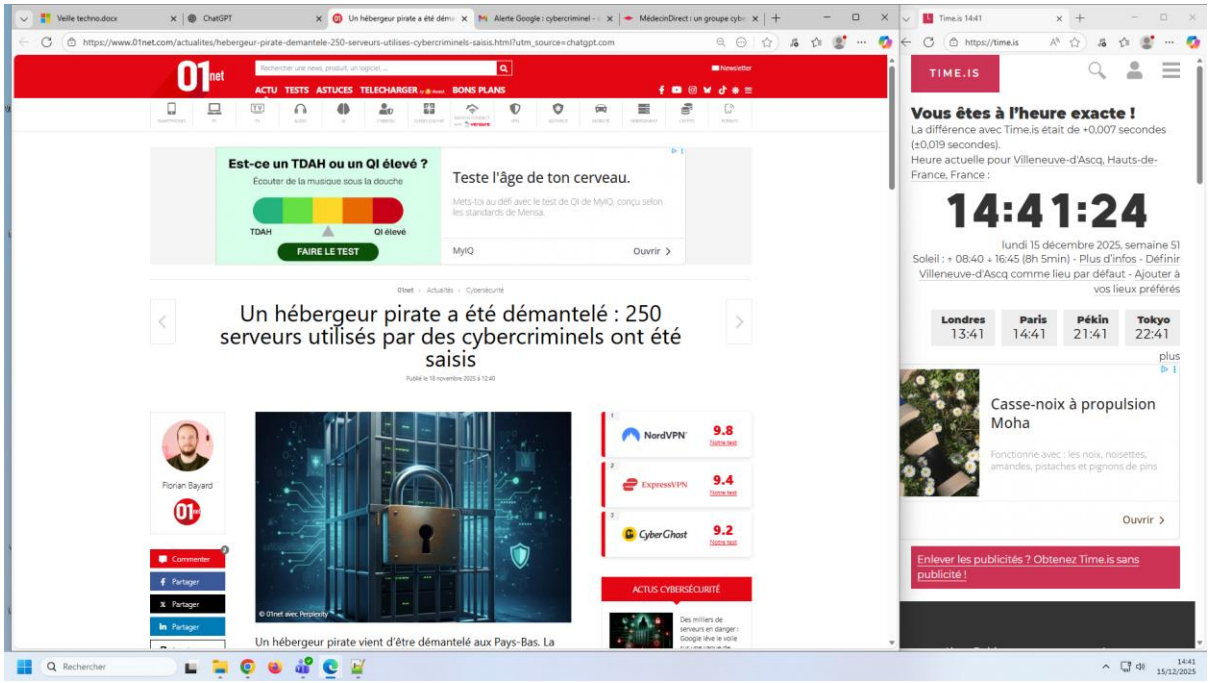
Asus affirme que ses produits et les données utilisateurs n'ont pas été affectés directement, mais que l'incident met en lumière la vulnérabilité des chaînes d'approvisionnement face aux attaques de ransomwares.



Une plateforme de téléconsultation médicale, MédecinDirect, a annoncé avoir subi une intrusion informatique fin novembre 2025, entraînant une fuite de données de santé personnelles. Environ 285 000 utilisateurs ont été informés que leurs comptes pourraient avoir été compromis, et un groupe cybercriminel revendique jusqu'à 323 069 données volées.

Les données potentiellement consultées comprennent des informations personnelles et médicales, notamment le motif de consultations, les réponses à des questionnaires de santé et, dans certains cas, des numéros de sécurité sociale — des données très sensibles.

Cette attaque illustre la convergence entre cybercriminalité et vol de données sensibles, correspondant à une évolution des techniques d'attaque au-delà du simple chiffrement de fichiers (ransomware) vers des attaques visant les données personnelles et médicales, qui peuvent ensuite être utilisées pour du chantage, de l'usurpation d'identité ou des campagnes de phishing.



Démantèlement d'un hébergeur pirate utilisé par des gangs de ransomware

Aux Pays-Bas, la police a saisi 250 serveurs utilisés par des groupes de ransomwares pour héberger leurs attaques. Cela montre que les autorités peuvent agir et perturber l'infrastructure des cybercriminels, mais aussi que ces infrastructures sont nombreuses.