

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 sources

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 feuilleter 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

The screenshot shows a web browser window with multiple tabs open. The active tab is 'google.fr/alerts#'. The main content area displays the 'Mes alertes' section with seven alerts listed:

- blackcat
- lockbit
- cybercriminel
- virus informatique
- cybersécurité
- attaque informatique
- ransomware

Below this is the 'Ma présence sur le Web' section, which shows two entries:

- 'Meryem' (with a blue profile icon)
- can.meryem@gmail.com (with a blue profile icon)

At the bottom of the page, there is a search bar with the query 'ransomware' and several filter options:

- Fréquence: Une fois par semaine maximum
- Sources: Blogs, Actualités, Web, Vidéo, Livres
- Langue: français
- Région: Toutes les régions
- Nombre de résultats: Seulement les meilleurs résultats
- Envoyer à: can.meryem@gmail.com

Below the filters, there is a preview section titled 'Aperçu de l'alerte' under the heading 'ACTUALITÉS'. It lists several news items related to ransomware:

- Sauveurs ou complices ? Face aux hackers, le business trouble des négociateurs de rançons L'Express
- Alors que les rançongiciels font de plus en plus de ravages, le rôle des négociateurs, chargés de dialoguer avec les gangs, reste controversé.
- Retail : Plus de la moitié (58 %) des enseignes victimes d'une attaque de ransomware versent... Global Security Mag
- Sophos publie la cinquième édition de son étude annuelle consacrée au secteur du retail. Intitulée L'état des ransomwares dans le secteur du ...
- Les États-Unis, l'Australie et le Royaume-Uni sanctionnent l'infrastructure russe de lutte ...

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

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

Google Actualités

"attaque ransomware"

Comment les articles sont-ils classés ?

Le Monde Informatique
Une attaque par ransomware a perturbé les aéroports européens

Tribune de Genève
Comment une attaque informatique paralyse une PME romande

SOC Prime
Détection du ransomware Epsilon Red : nouvelle campagne mondiale ciblant les utilisateurs via ClickFix

Numerama
Ingram Micro piégé par des hackers : l'attaque qui

Rechercher

Enregistrer

Informations consommateurs

8°C Pluie fine

14:52 24/11/2025

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

news.google.com/search?q="cybercriminel"&hl=fr&gl=FR&ceid=FR%3Afr

Google Actualités

"cybercriminel"

Comment les articles sont-ils classés ?

incyber news
Un groupe cybercriminel sophistiqué exploite des failles zero-day dans Citrix et Cisco

B. Brut
Un cybercriminel incarcéré pour actes de cruauté et pédopornographie

Le Monde Informatique
Les infostealers, la menace invisible alimentant l'écosystème cybercriminel

Liberation
L'administrateur d'un important forum cybercriminel

Rechercher

Enregistrer

Informations consommateurs

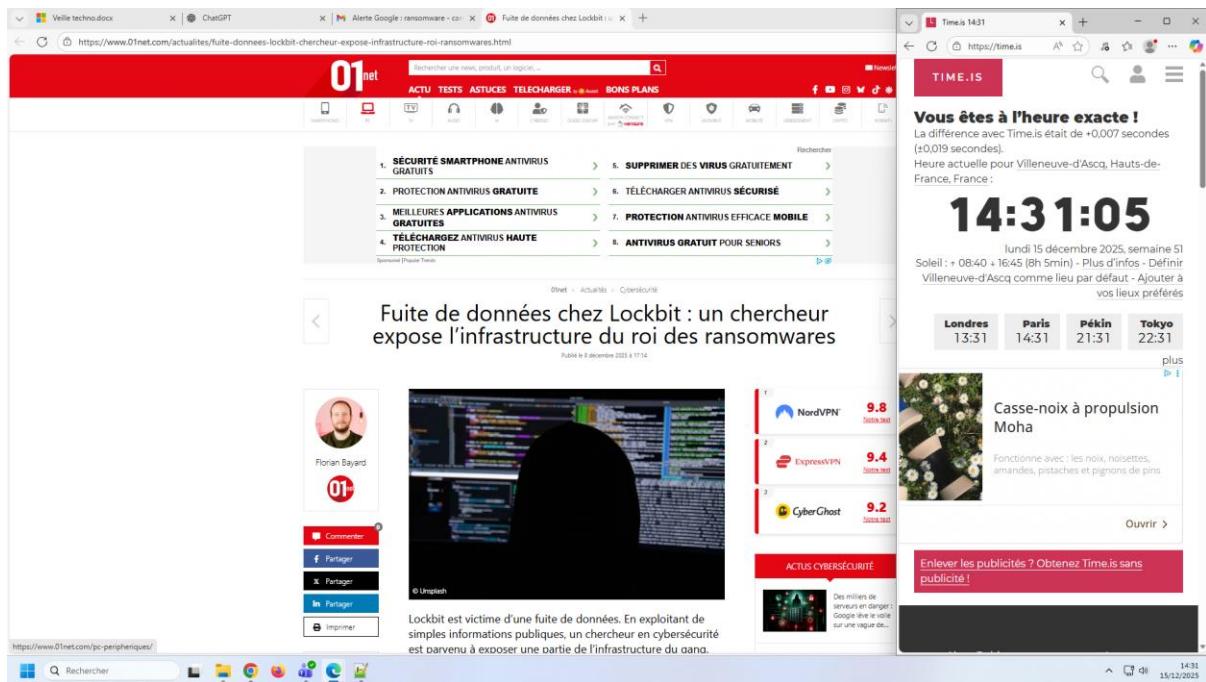
8°C Pluie fine

14:55 24/11/2025

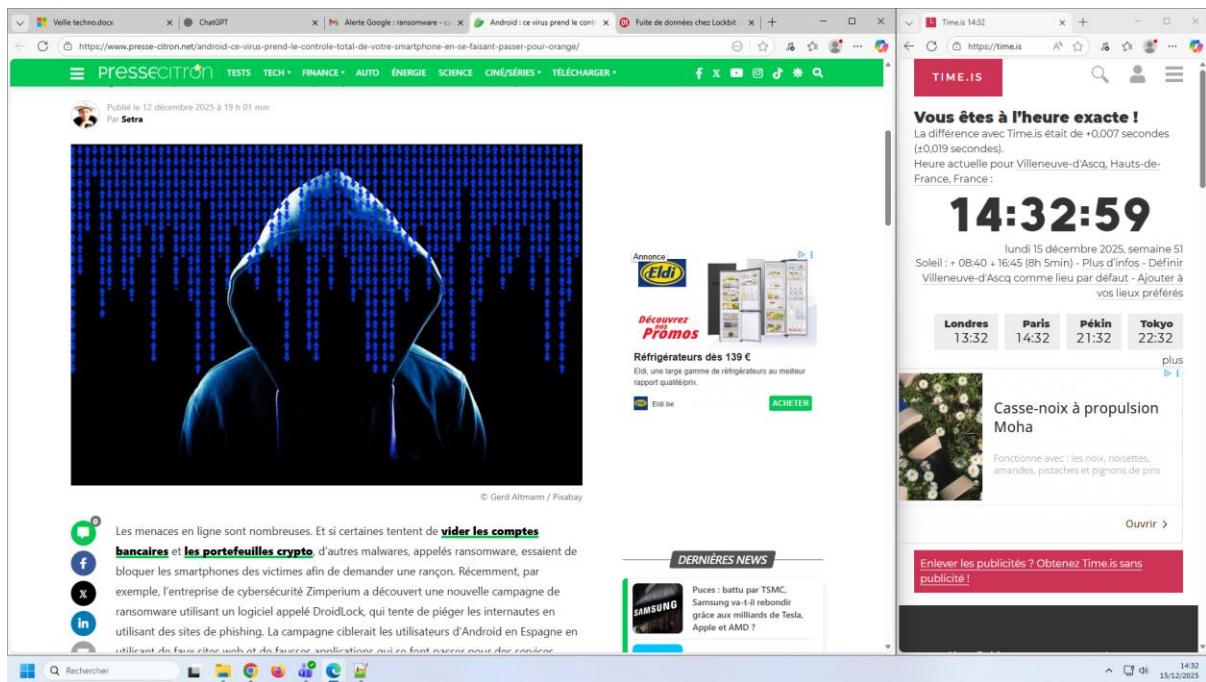
The screenshot shows a Microsoft Edge browser window with multiple tabs open. The active tab is a Google News search for "virus informatique". The search results page displays several news articles from various sources like Ouest-France, francebleu.fr, Le site de Korben, and Bpifrance. The interface includes a sidebar with navigation links such as Accueil, Suivis, News Showcase, France, International, Actualités locales, Économie, Sciences et technologies, Divertissement, Sports, and Santé. A right-hand sidebar shows a search summary for "virus informatique" with a button to "Enregistrer". The bottom of the screen shows the Windows taskbar with icons for File Explorer, Task View, and other pinned apps.

The screenshot shows a Microsoft Edge browser window displaying the Feedly.com interface. The left sidebar shows a navigation menu with "Le Feedly de Moryom" selected, followed by "Aujourd'hui", "Suivre les sources", "Créer un flux IA", "Recherche", "Lire plus tard", and "Articles récemment lus". Below this is a section for "Aliments" with various news items. The main content area is titled "Flux IA" and shows a search interface for "cyberattaques" and "Ransomware". It displays a news article snippet about ITL Systemhaus being a victim of ransomware. The right sidebar shows "Sources" options like "Flux RSS et tout le Web", "Aliments", "Tous les flux personnels", "cybersecurite", "Recherche sur les menaces", "RSSI", and "Fournisseurs de securite". The bottom of the screen shows the Windows taskbar.

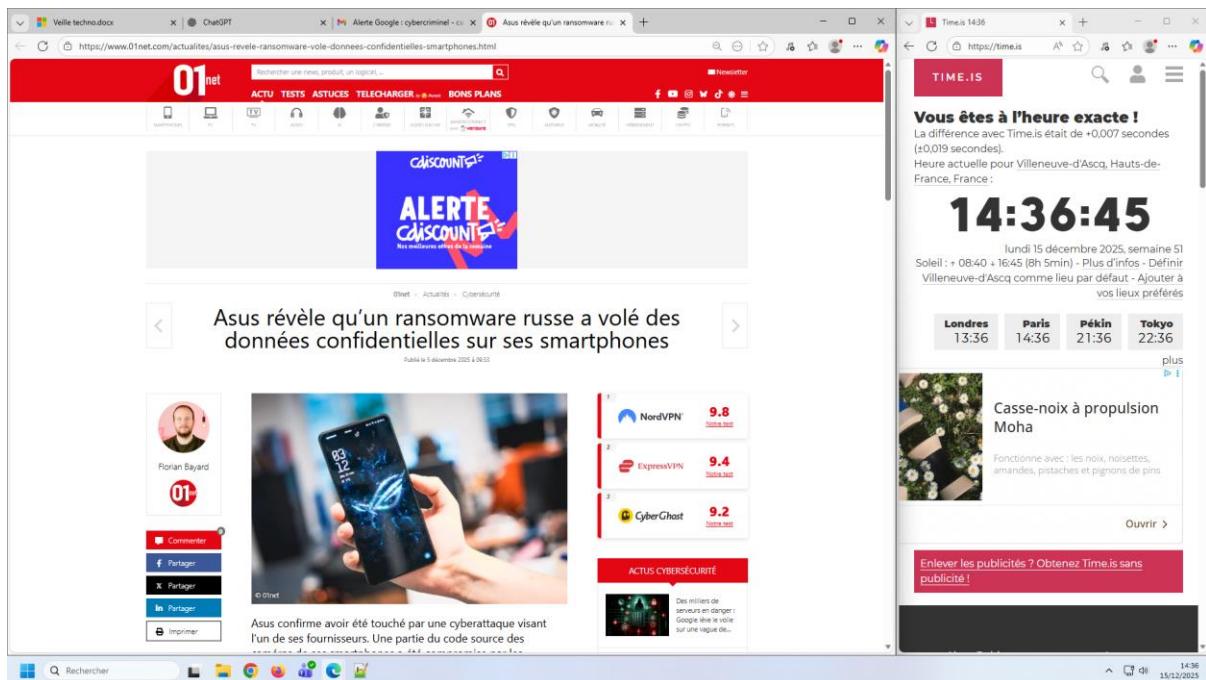
Feedly.com



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.



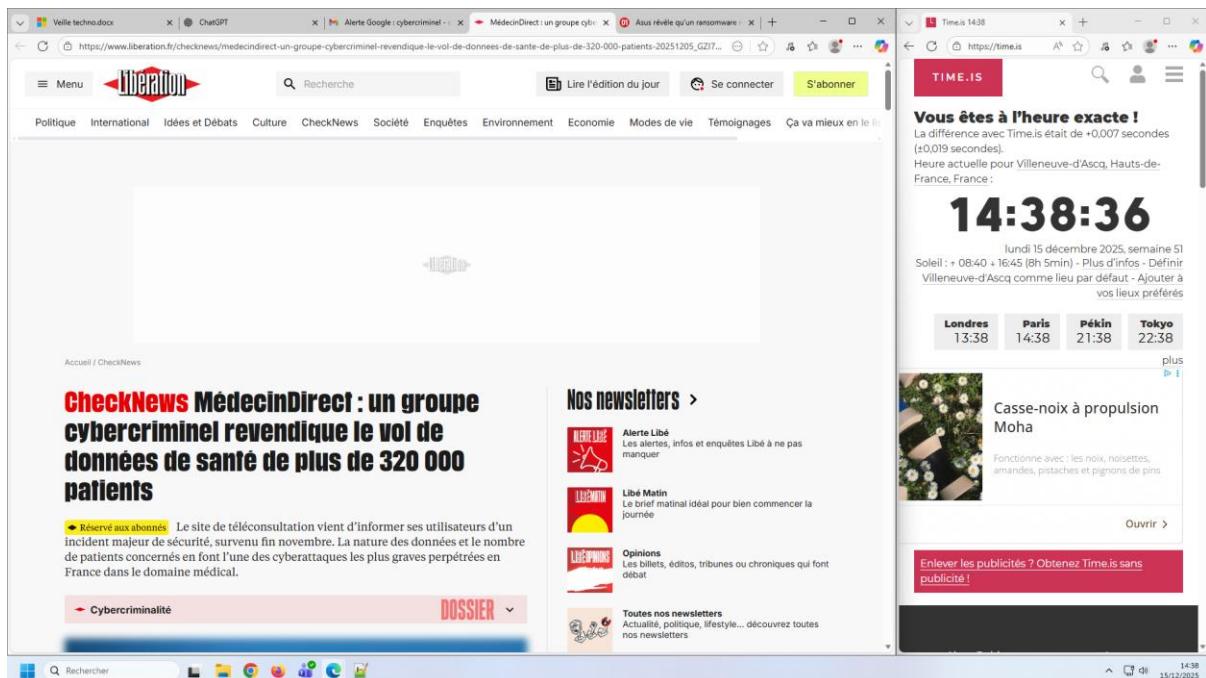
Une campagne de malware Android appelée *DroidLock* utilise des faux sites imitant des services comme Orange pour inciter les utilisateurs à installer une application malveillante. Une fois installée, cette application demande des permissions critiques qui lui permettent de prendre le contrôle total 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'accès 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.

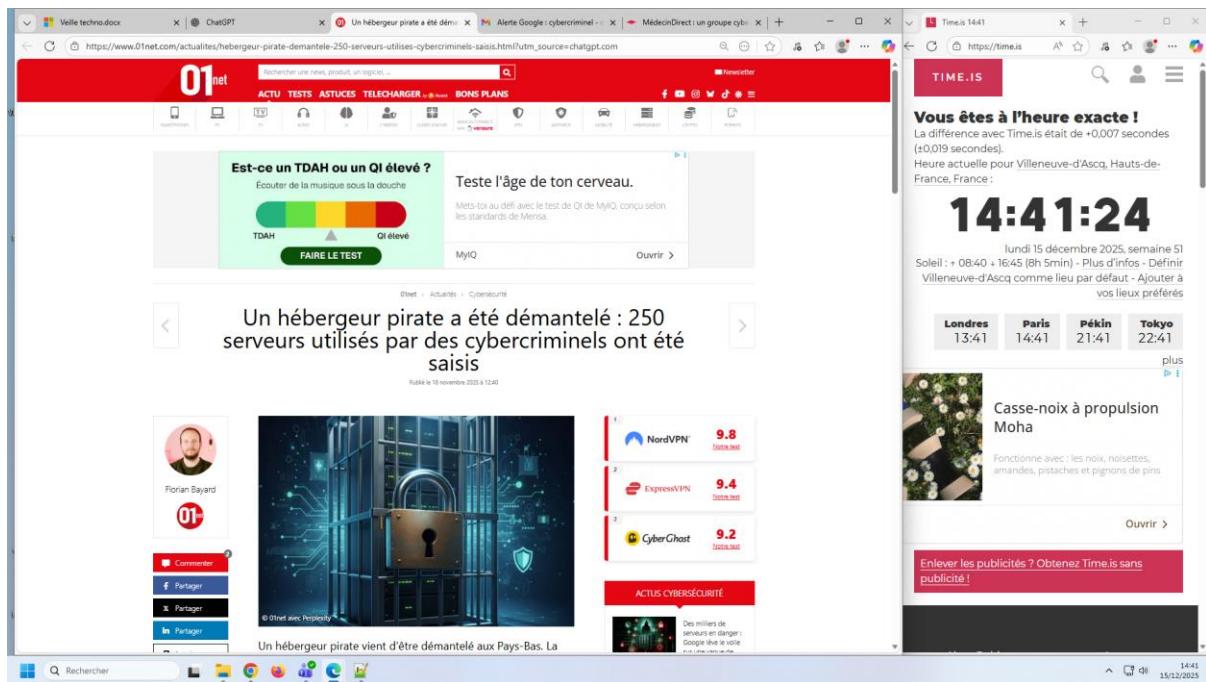
Asus affirme que ses produits et les données utilisateurs n'ont pas été affectés directement, mais que l'incident met en lumière la vulnérabilité des chaînes d'approvisionnement face aux attaques de ransomwares.



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.