WWW.DUDIX-CONSULTING.FR

DUDIX Consulting

Les Nouvelles du Front

DUDIX CTI

Secteur stratégique:

Santé

29 août 2025

HORS SERIE

BASÉ SUR UN CLUSTER OPENCTI ENRICHI EN TEMPS RÉEL, AUTO-HÉBERGÉ ET AFFUTÉ CHAQUE JOUR

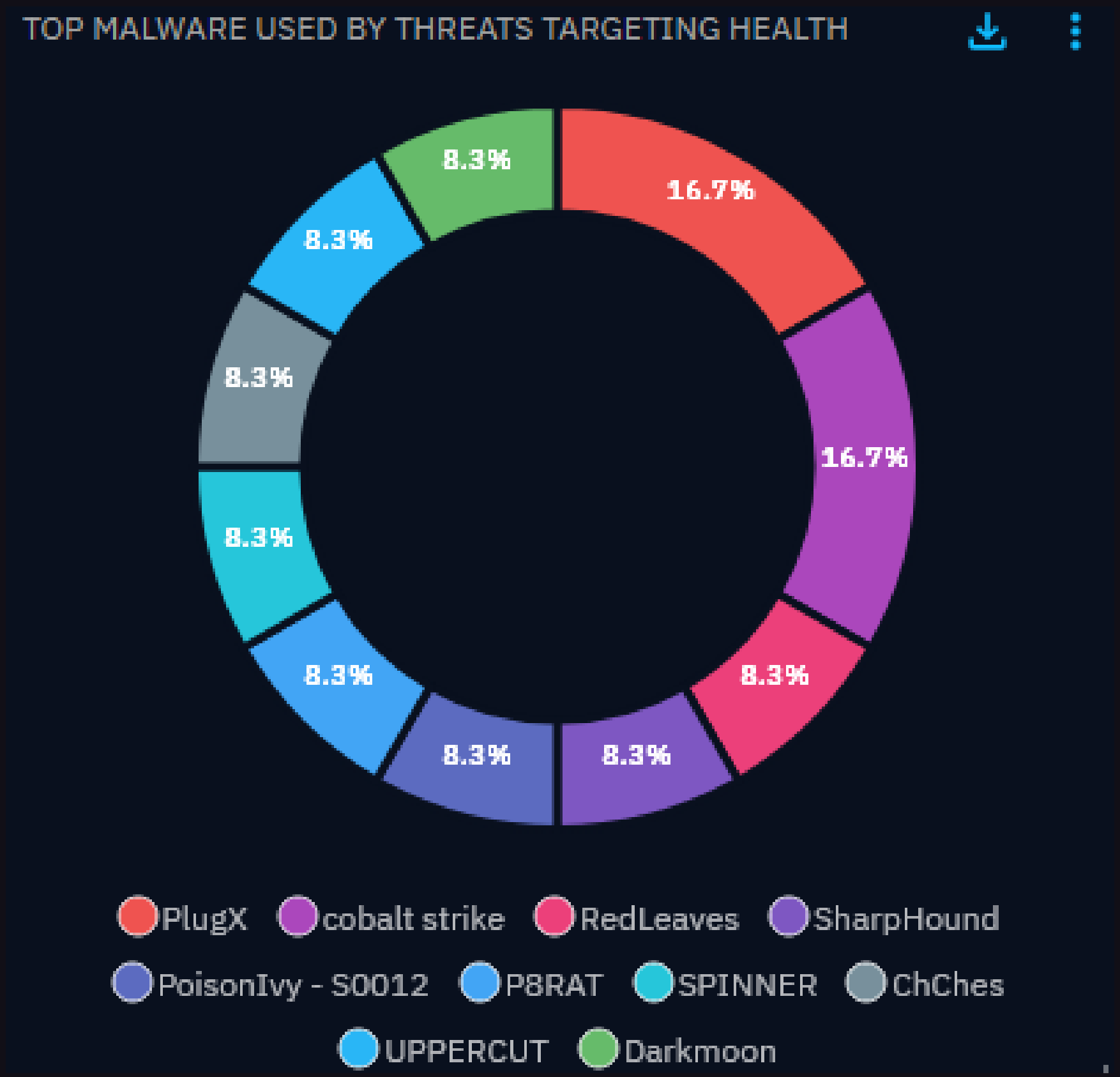
TOP THREAT

Top targeted country: USA
Top threat: QILIN
Active TTP: T1059, T1140

Top threats

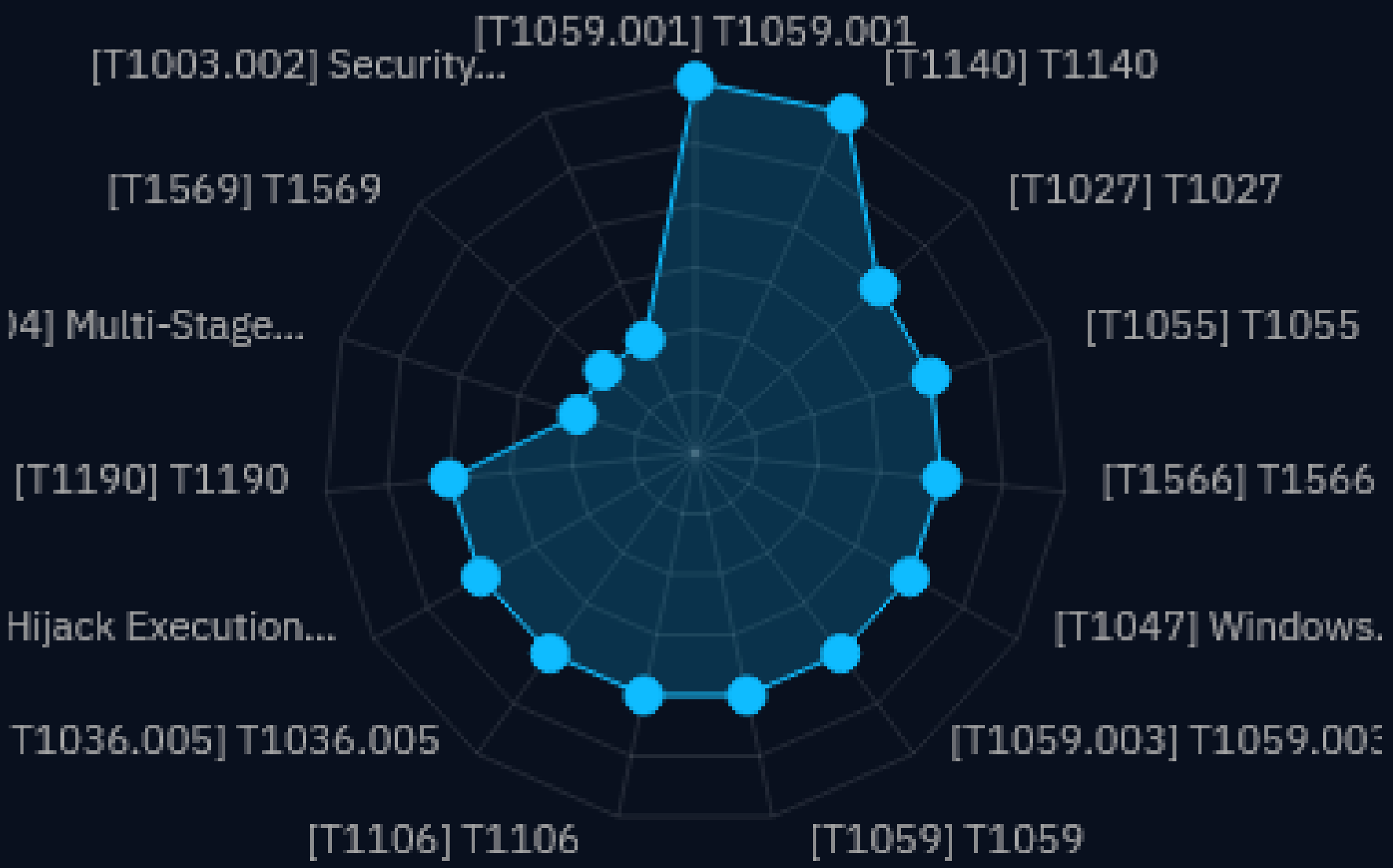

TOP THREATS TARGETING HEALTH
Twisted Panda
UNC4990
menuPass
0
1

Top malware

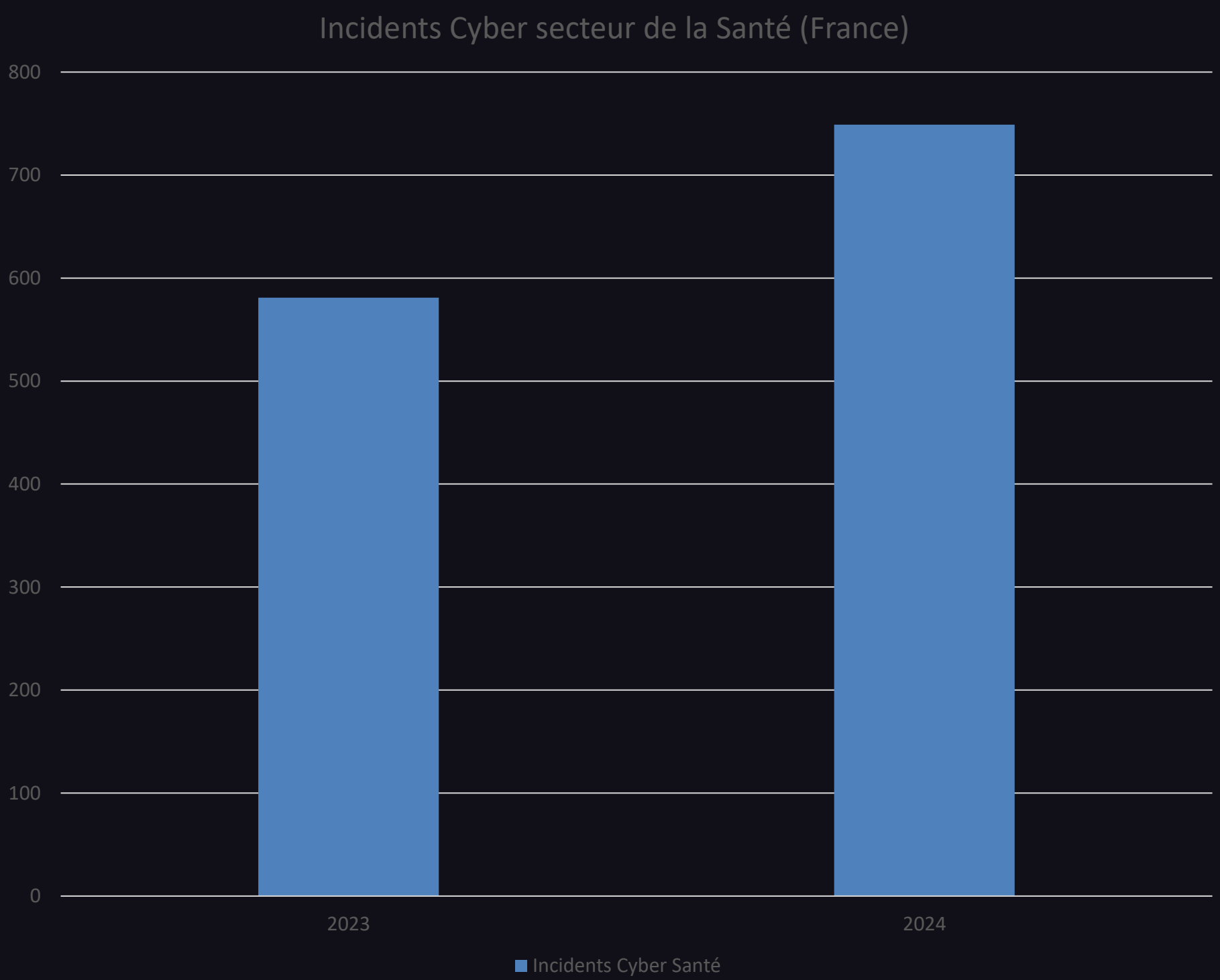

TOP MALWARE USED BY THREATS TARGETING HEALTH
8.3%
16.7%
8.3%
8.3%
16.7%
8.3%
8.3%
8.3%
8.3%
8.3%
PlugX
cobalt strike
RedLeaves
SharpHound
PoisonIvy - SO012
P8RAT
SPINNER
ChChes
UPPERCUT
Darkmoon

Top TTPS

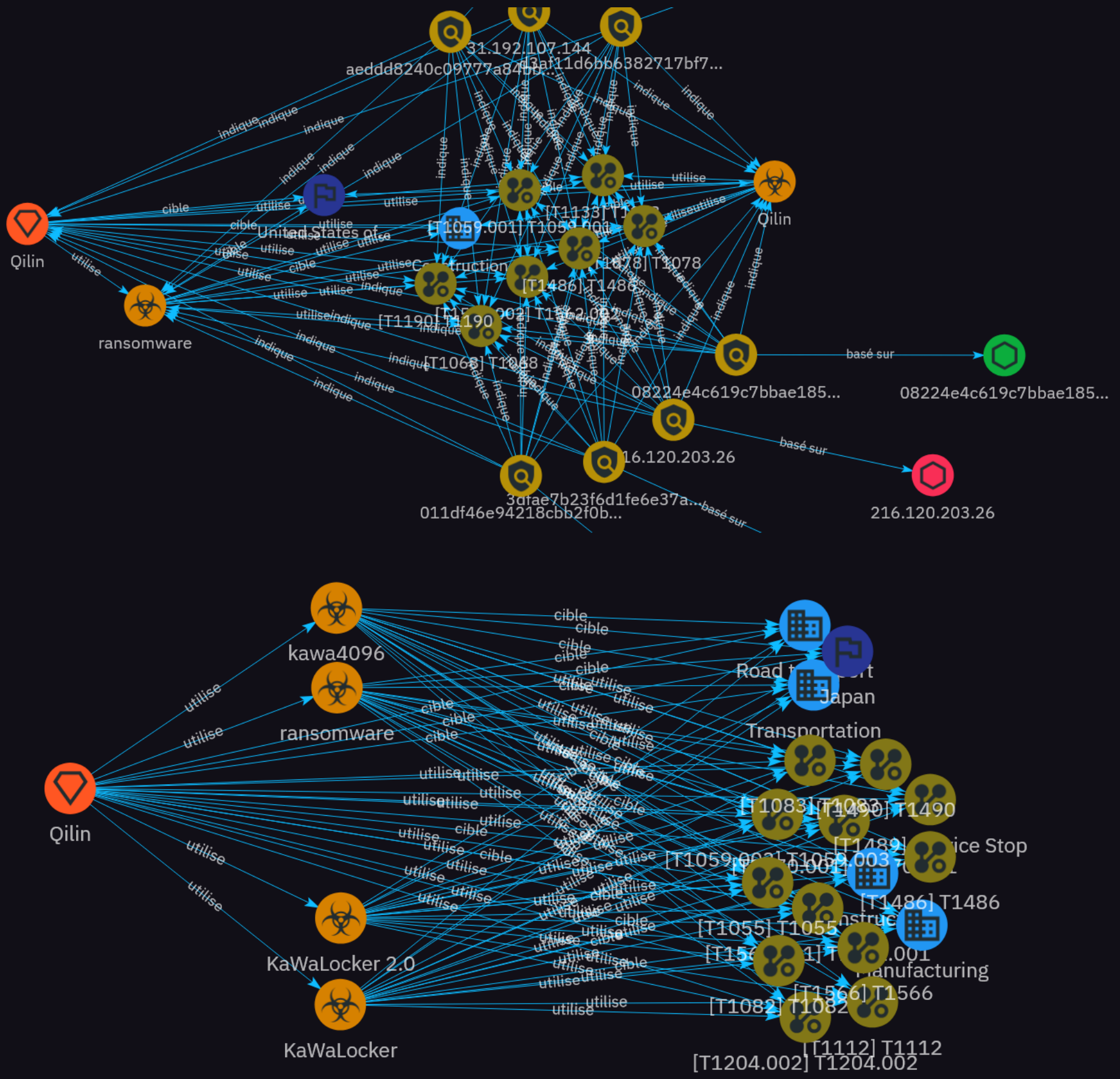
TOP TECHNIQUES USED BY THREATS TARGETING HEALTH



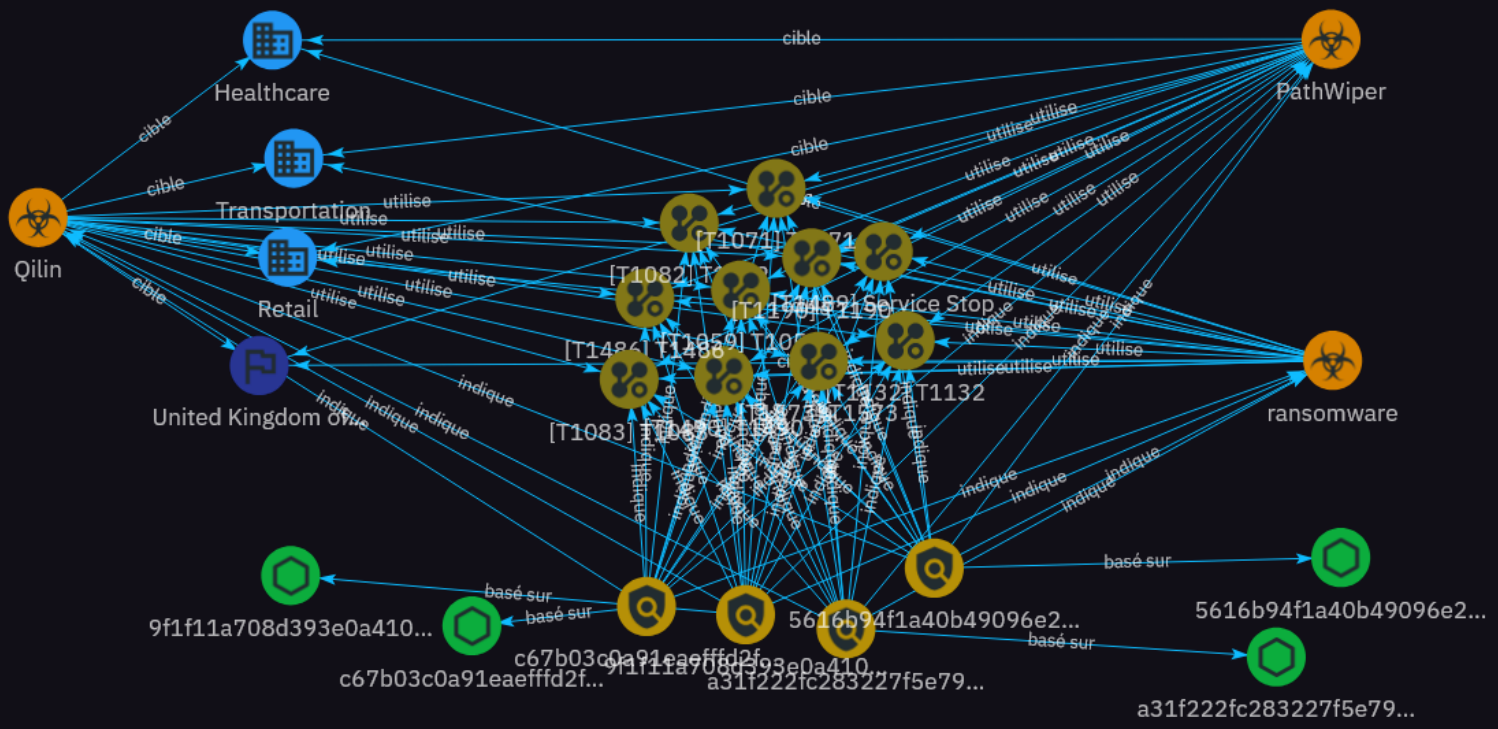
Evolution


Incidents Cyber secteur de la Santé (France)
800
700
600
500
400
300
200
100
0
2023
2024
Incidents Cyber Santé

ACTIVITIE OF THREAT : QILIN



ACTIVITIE OF THREAT : QILIN



Le ransomware le plus utilisé et impactant dans le secteur de la santé en France en 2024-2025 est notamment le groupe Qilin, qui a supplanté le ransomware Play depuis mai 2025.

Tendances 2024-2025

En 2024, environ 67% des établissements de santé ont été touchés par un ransomware, contre 60% en 2023, avec un taux d'attaque pratiquement doublé depuis 2021.

Les ransomwares représentent la menace la plus dangereuse, avec un fort taux de chiffrement des données (74% des attaques en 2024 aboutissent au chiffrement).

Malgré une légère baisse globale du nombre d'attaques par ransomware en France en 2024 (-13%), la menace reste très active et cause des impacts lourds sur les établissements, notamment dans la santé.

Le coût moyen de récupération après une attaque est en hausse, atteignant 2,57 millions de dollars en 2024 dans le secteur de la santé.

Parmi les groupes de ransomwares en activité récente, Clop, connu pour sa campagne MOVEit de 2023, demeure une référence internationale majeure.

D'autres familles populaires, comme LockBit ou Conti, continuent d'évoluer et de cibler la santé dans leurs campagnes.

Résumé

Étendue des cyberattaques

En 2024, 749 incidents de cybersécurité ont été déclarés dans 558 établissements de santé en France, soit une hausse de 29% en un an.

Toutefois, le nombre d'incidents majeurs a baissé, signe d'une meilleure préparation des hôpitaux face aux attaques.

Les ransomwares, principale menace
Les rançongiciels restent la menace la plus redoutée en santé, responsables de la majorité des perturbations graves.

En 2024, environ 67% des établissements de santé français ont subi une attaque liée à un ransomware, avec un taux d'attaque doublé par rapport à 2021.

Le coût moyen de récupération après une attaque ransomware atteint 2,57 millions de dollars.

Parmi les familles les plus actives figurent Qilin, qui a émergé en 2025, ainsi que des groupes comme Clop et LockBit.

Autres techniques d'attaque

Phishing et ingénierie sociale : vecteurs clés pour compromettre les accès aux réseaux hospitaliers, responsables de 70% des cyberattaques réussies.

Exploitation de vulnérabilités logicielles, notamment dans les dispositifs médicaux connectés, utilisés pour obtenir un accès non autorisé.

Exfiltration et vol de données sensibles, qui sont ensuite vendues sur le dark web pour des fraudes et usurpations d'identité.

Résumé

Impact et conséquences

- Paralysie des systèmes informatiques hospitaliers, notamment urgences, radiologie, et gestion des dossiers médicaux.
- Risque accru pour la sécurité et la vie des patients, avec des cas réels d'interruptions critiques des soins rapportés.
- Coûts financiers et réputationnels lourds, ainsi qu'un impact négatif sur la confiance du public.

Facteurs aggravants

- Infrastructures IT vieillissantes et sous-investissement chronique dans la cybersécurité, seuls 7% des établissements ont un responsable cybersécurité dédié à temps plein.
- Le facteur humain reste un point faible majeur, avec une mauvaise gestion des mots de passe et un manque de sensibilisation régulière.

Réponses en cours

- Renforcement des réglementations, comme la directive européenne NIS 2, exigeant des mesures rigoureuses pour les infrastructures critiques.
- Investissements publics massifs, notamment via le plan national cybersécurité santé (350 millions d'euros) pour moderniser les systèmes et former les équipes.
- Coordination accrue entre agences gouvernementales (ANSSI, CERT Santé, Agence du numérique en santé) et les établissements pour détection, réponse et prévention.

Résumé

Le secteur de la santé est aujourd'hui exposé à une menace cyber croissante et sophistiquée.

Les ransomwares dominent avec des groupes comme Qilin, LockBit et Clop, causant des perturbations graves et des pertes financières importantes.

Le facteur humain et les systèmes vieillissants accentuent cette vulnérabilité.

Toutefois, des efforts accrus en gouvernance, formation et réponse collective montrent des premiers résultats encourageants pour renforcer la résilience face aux cyberattaques.