

ISTÈRE D'LA DÉFENSE

Les Nouvelles du Front

Secteur strategique:

Défense

29 Juillet 2025

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



TOP THREAT

Top targeted country: USA
Top threat: Earth Longzhi

Top malware: Cobalt Strike

Active vuln: CVE-2023-42793

Active TTP: T1027, T1140, T1105

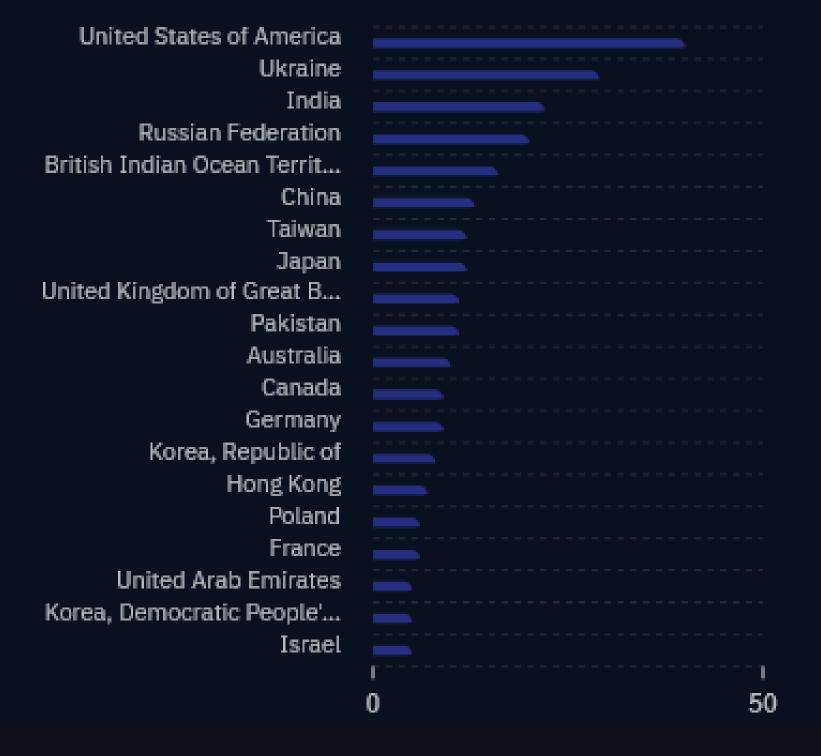


Top targeted country

THREATS TARGETING DEFENSE BY REGIONS







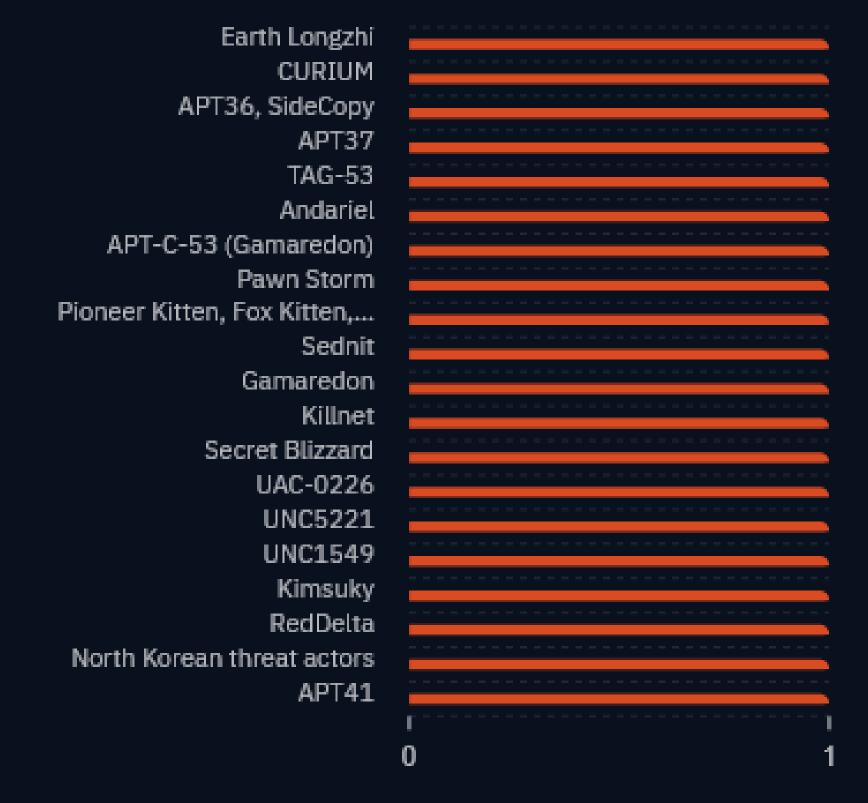


Top threats

TOP 20 THREATS TARGETING DEFENSE







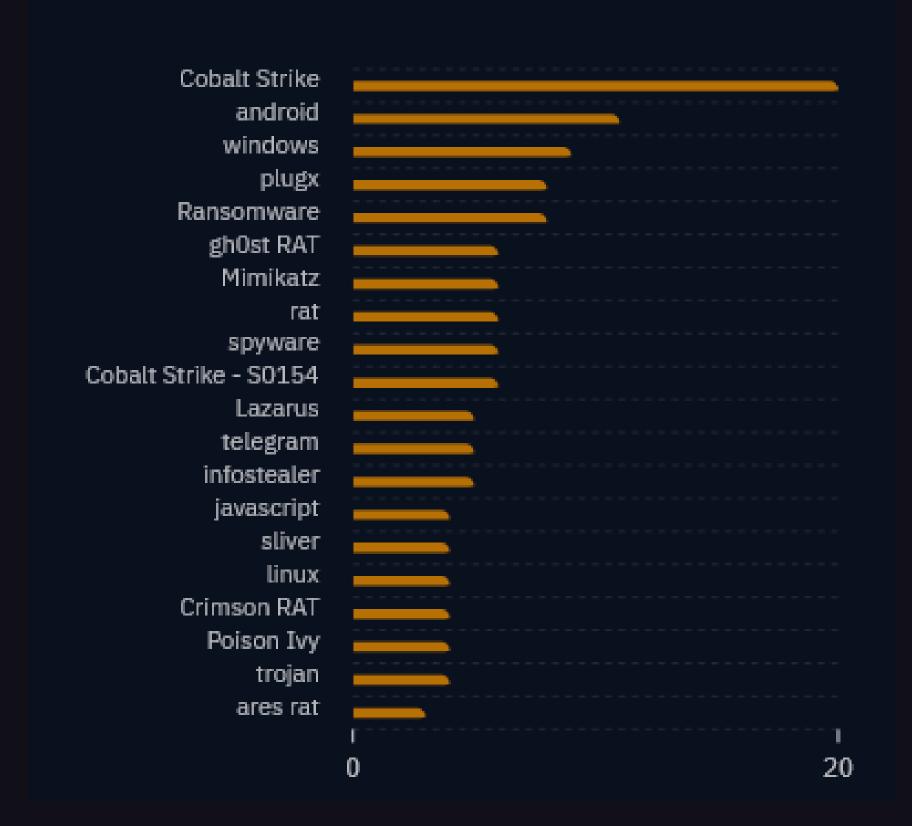


Top malware

TOP 20 MALWARE USED BY THREATS TARGETING DEFENSE







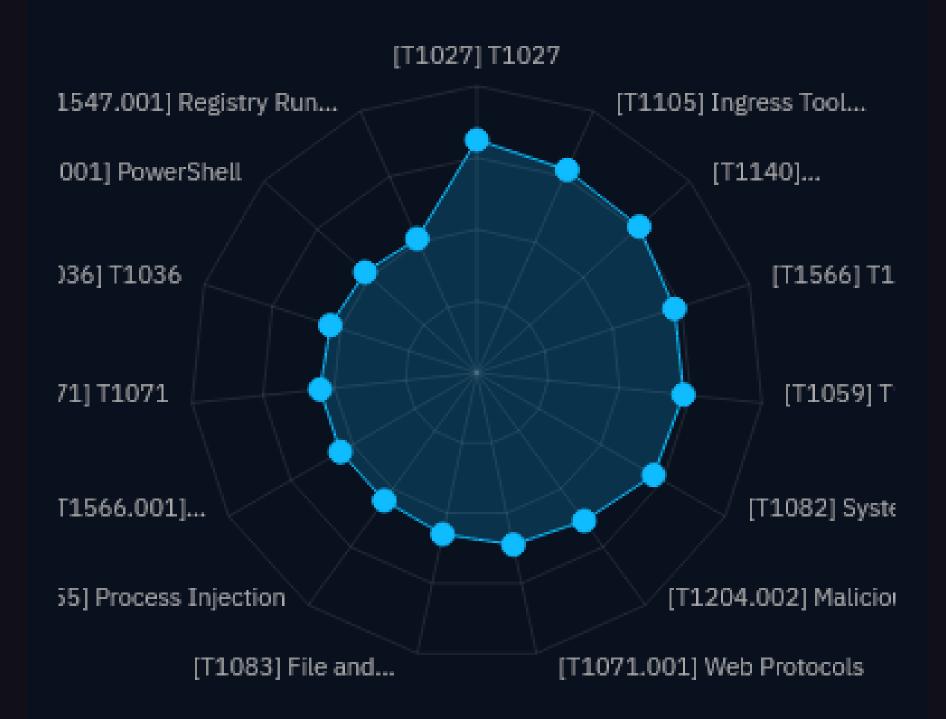


Top TTPS

TOP TECHNIQUES USED BY THREATS TARGETING DEFENSE







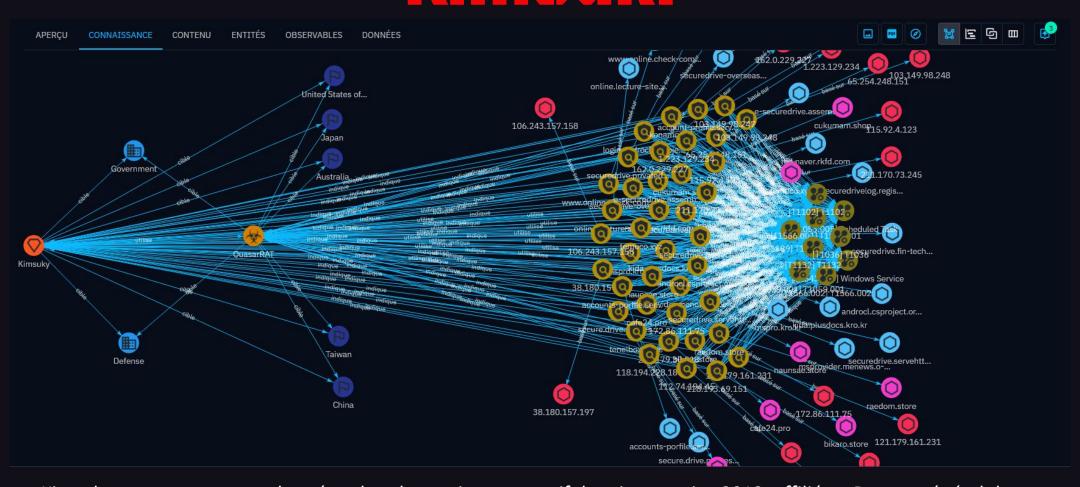


Top vulnerabilities

TOP VULNERABILITIES TARGETED BY THREATS TARGETING DEFENSE		
Ð	CVE-2023-42793	5
Ð	CVE-2024-21887	4
Ð	CVE-2017-11882	4
Ð	CVE-2021-44228	4
Ð	CVE-2023-38831	4
Ð	CVE-2021-34473	3
₫	CVE-2023-23397	3



ACTIVITIE OF THREAT: Kimsuki



Kimsuky est un groupe nord-coréen de cyberespionnage actif depuis au moins 2012, affilié au Bureau général de reconnaissance, le service de renseignement extérieur de la Corée du Nord.

Il cible principalement des gouvernements, centres de recherche, médias et institutions liés à la politique étrangère, la sécurité nationale et les programmes nucléaires, principalement en Corée du Sud, mais aussi aux États-Unis, en Europe et au Japon.

Kimsuky utilise des techniques sophistiquées comme le spear-phishing, l'envoi d'emails ciblés avec pièces jointes ou liens malveillants, l'exploitation de failles zero-day, et déploie des malwares personnalisés pour voler des informations stratégiques et maintenir un accès furtif. Ce groupe participe aussi au vol de cryptomonnaies pour financer ses opérations.

Il est reconnu comme une menace persistante d'État (APT), marquée par une grande discrétion et une longue persistance dans les réseaux ciblés, avec des campagnes d'espionnage visant à soutenir les ambitions stratégiques et nucléaires de la Corée du Nord



Au troisième trimestre 2025, plusieurs catégories d'entités françaises du secteur de la défense sont particulièrement visées par les attaques cyber, les ingérences et le sabotage.

Les grandes entreprises de défense et les maîtres d'œuvre (Naval Group, Thalès, Safran, Dassault...) sont régulièrement la cible d'attaques sophistiquées. Par exemple, Naval Group a récemment subi une fuite massive de données, avec le vol d'1 téraoctet de documents, comprenant des informations sur ses frégates et des codes sources sensibles. Des groupes hackers prorusses comme NoName057 ont aussi orchestré des attaques de type déni de service à répétition depuis 2022.

Les PME et sous-traitants de la Base Industrielle et Technologique de la Défense (BITD) sont de loin les cibles les plus vulnérables et les plus fréquemment attaquées. Plus de 60 % des cyberattaques de 2025 concernent des PME du secteur, qui subissent aussi des attaques physiques (intrusions, sabotage, vols de données). Ces petites structures, souvent moins protégées, jouent un rôle clé dans la chaîne d'approvisionnement du secteur mais manquent fréquemment de moyens dédiés à la cybersécurité.

Les entités gouvernementales et organismes publics liés à la défense ne sont pas épargnés, notamment par des campagnes d'espionnage pilotées par des groupes étrangers, parfois attribuées à des acteurs comme APT 28 (proches de la Russie).

Les sites industriels stratégiques et sensibles subissent aussi des attaques physiques : destruction de matériel, sabotage sur les chaînes de production, survols par drones, etc., avec une hausse sensible du nombre de ces incidents depuis 2022.

Tous les maillons de la chaîne, y compris les prestataires IT et cabinets d'ingénierie travaillant dans la défense sont visés, car ils peuvent servir de porte d'entrée vers des systèmes critiques.

En résumé, les entreprises françaises, grandes ou petites, associées de près ou de loin à la BITD, sont désormais des cibles privilégiées pour les États hostiles, les groupes cybercriminels et les acteurs de l'ingérence économique, qui profitent des failles de sécurité (physiques ou numériques) dans un contexte de tensions internationales accrues. Les PME sont toutefois les plus exposées, représentent désormais la majorité des victimes recensées en France dans le secteur de la défense.

