WWW.DUDIX-CONSULTING.FR

Les Nouvelles du Front

DUDIX CTI

Semaine 34

25 août 2025

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

TOP THREAT

Targeted Sector : Government

Top Targeted Countries : USA

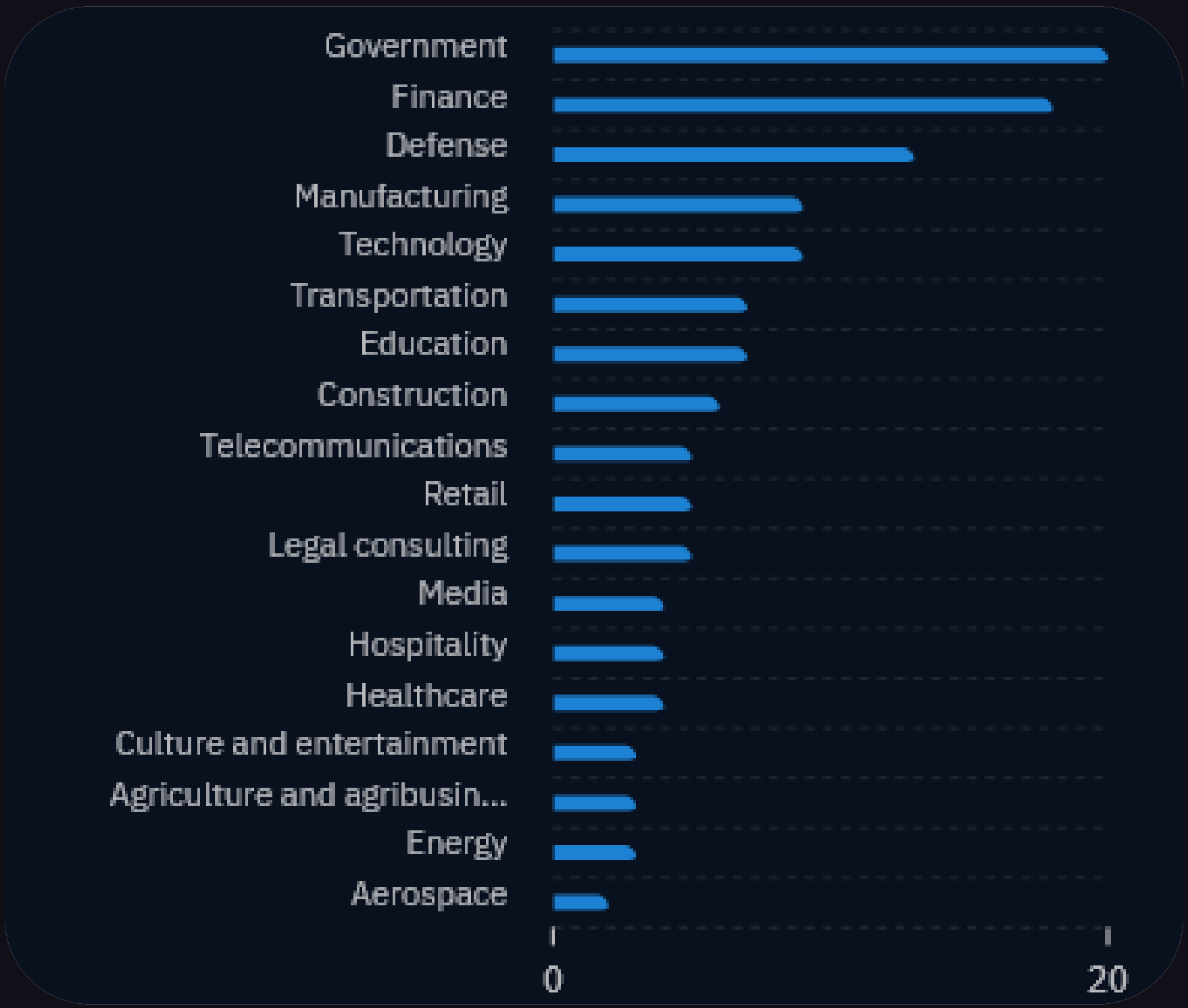
Active Intrusion Set : Candiru (CHANSHOT, DevilsTongue)

Active Vuln : CVE-2018-0171

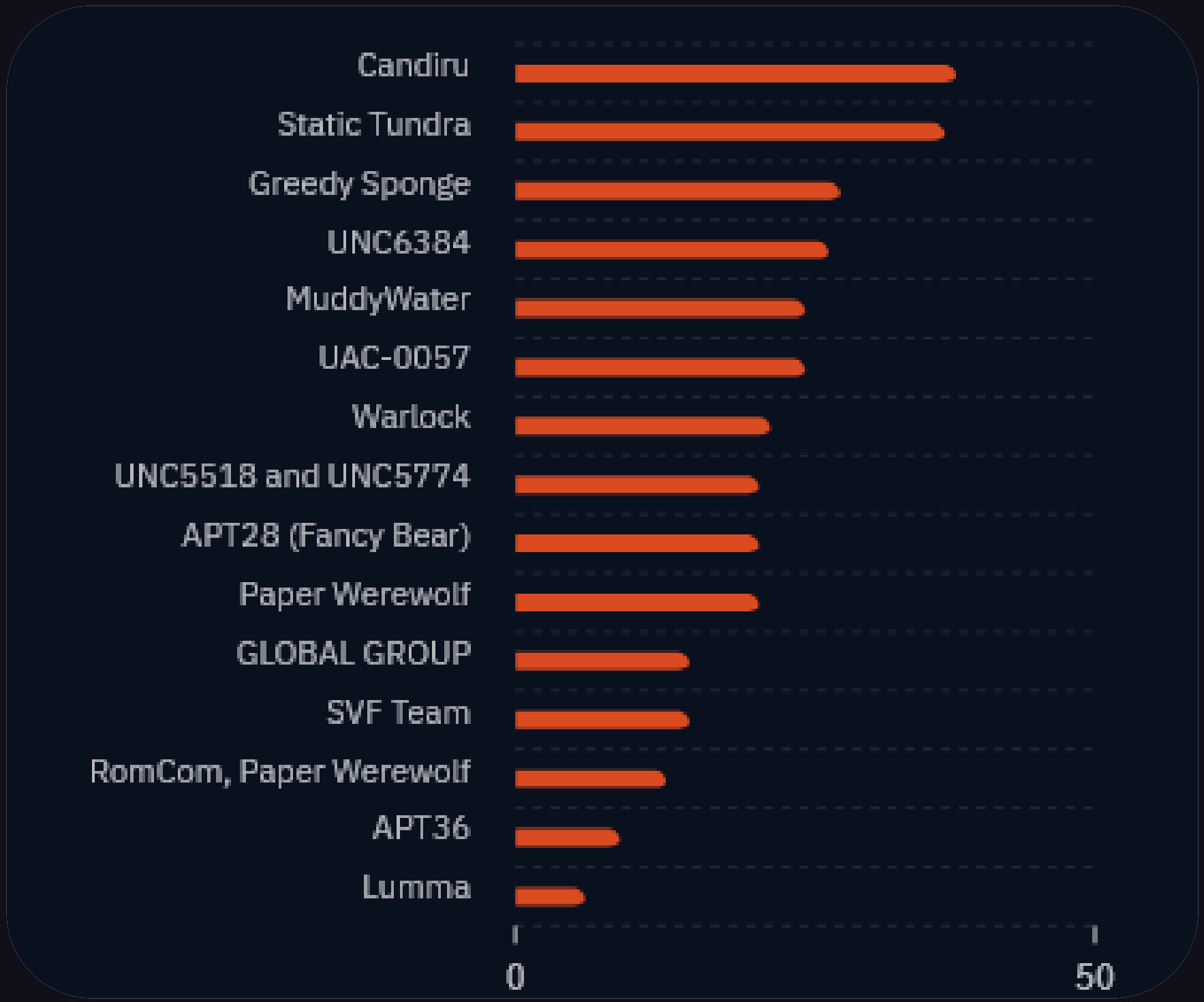
Active TTP : T1020

Active Malware : CHAINSHOT (DevilsTongue, Candiru)

Top Targeted Sectors



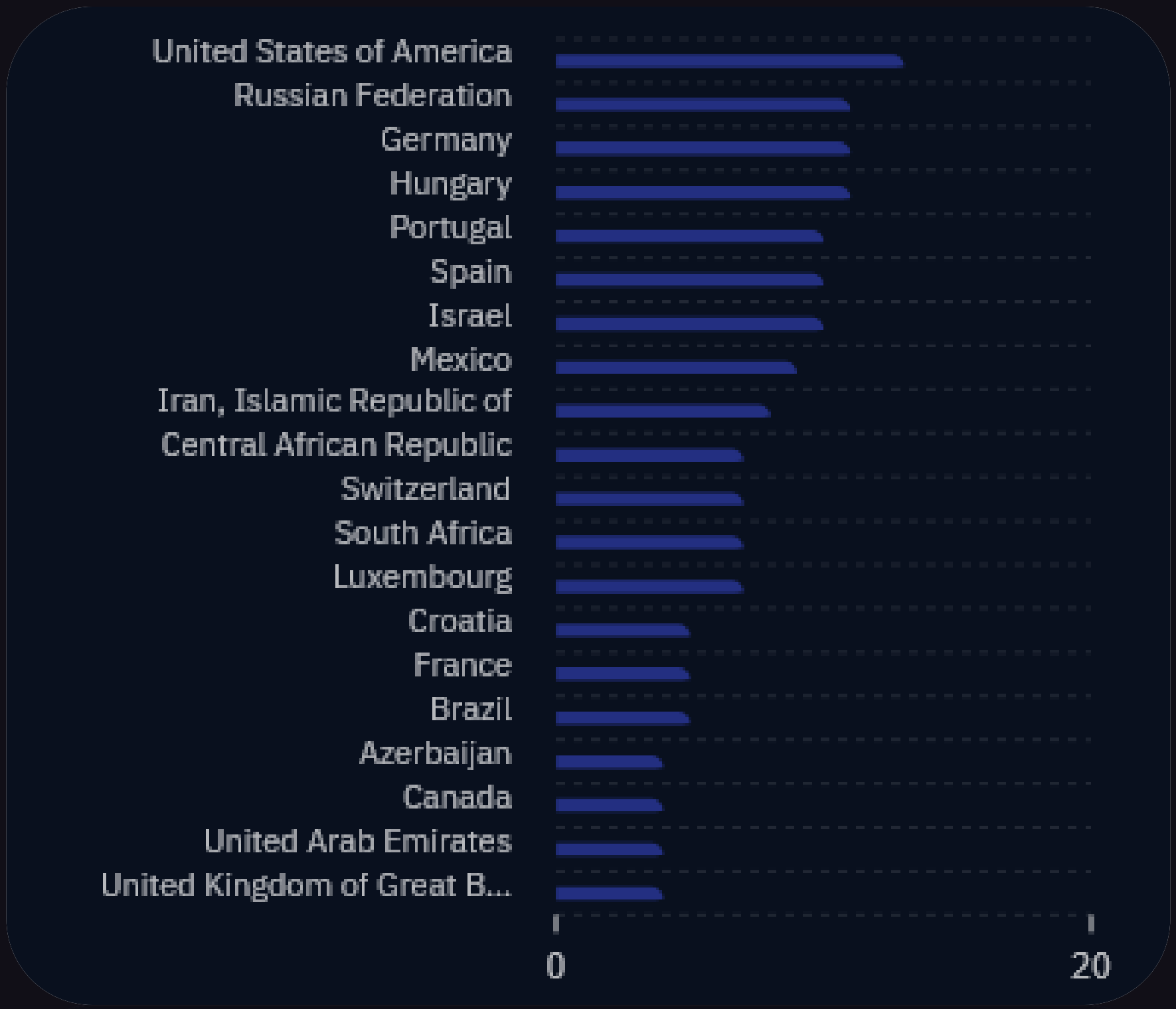
Active Intrusion Sets



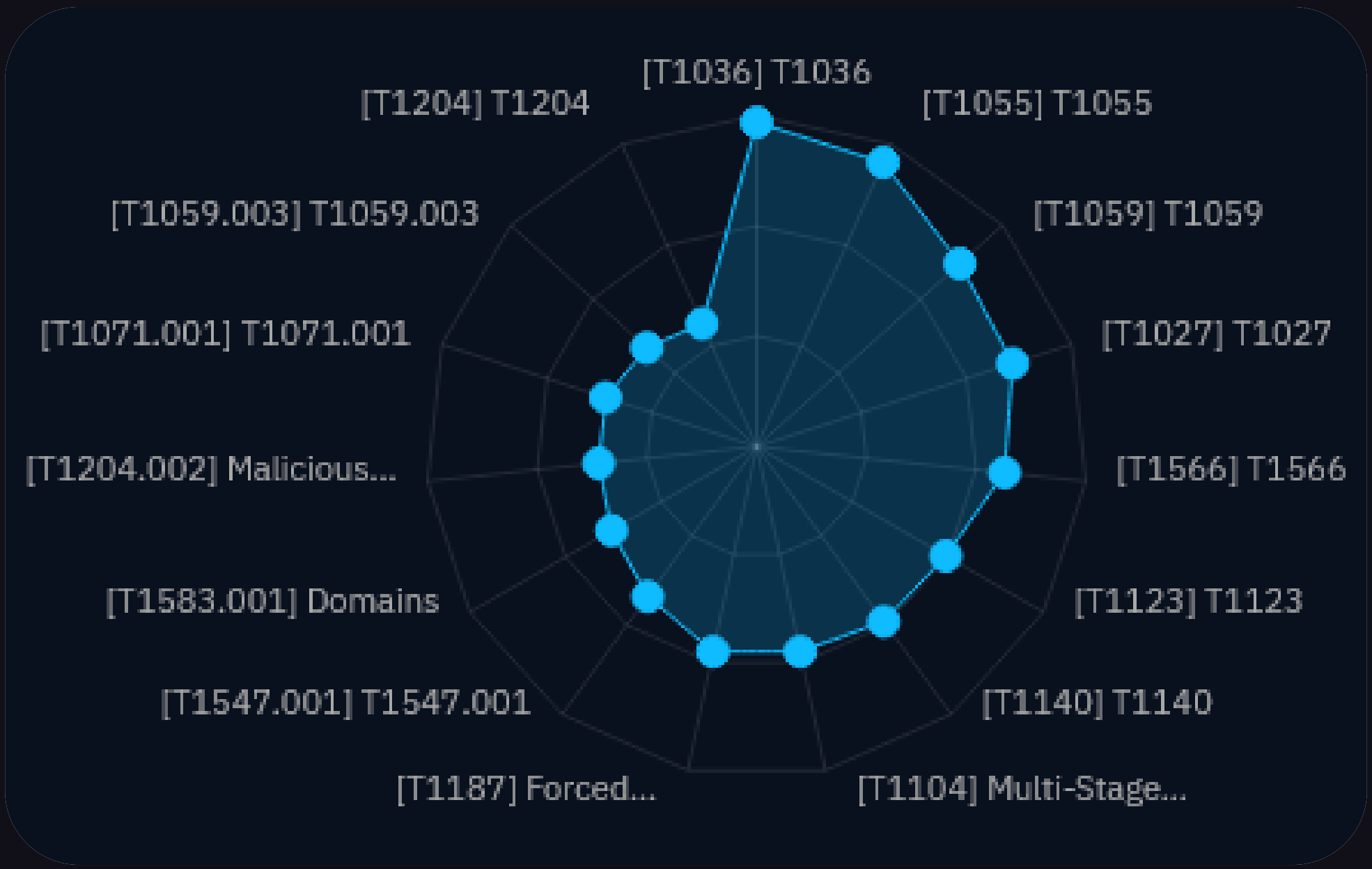
Top Active Vulns

CVE-2018-0171	31
CVE-2025-6218	27
CVE-2021-21166	24
CVE-2021-33742	24
CVE-2021-1844	24
CVE-2021-30551	24
CVE-2025-32433	23

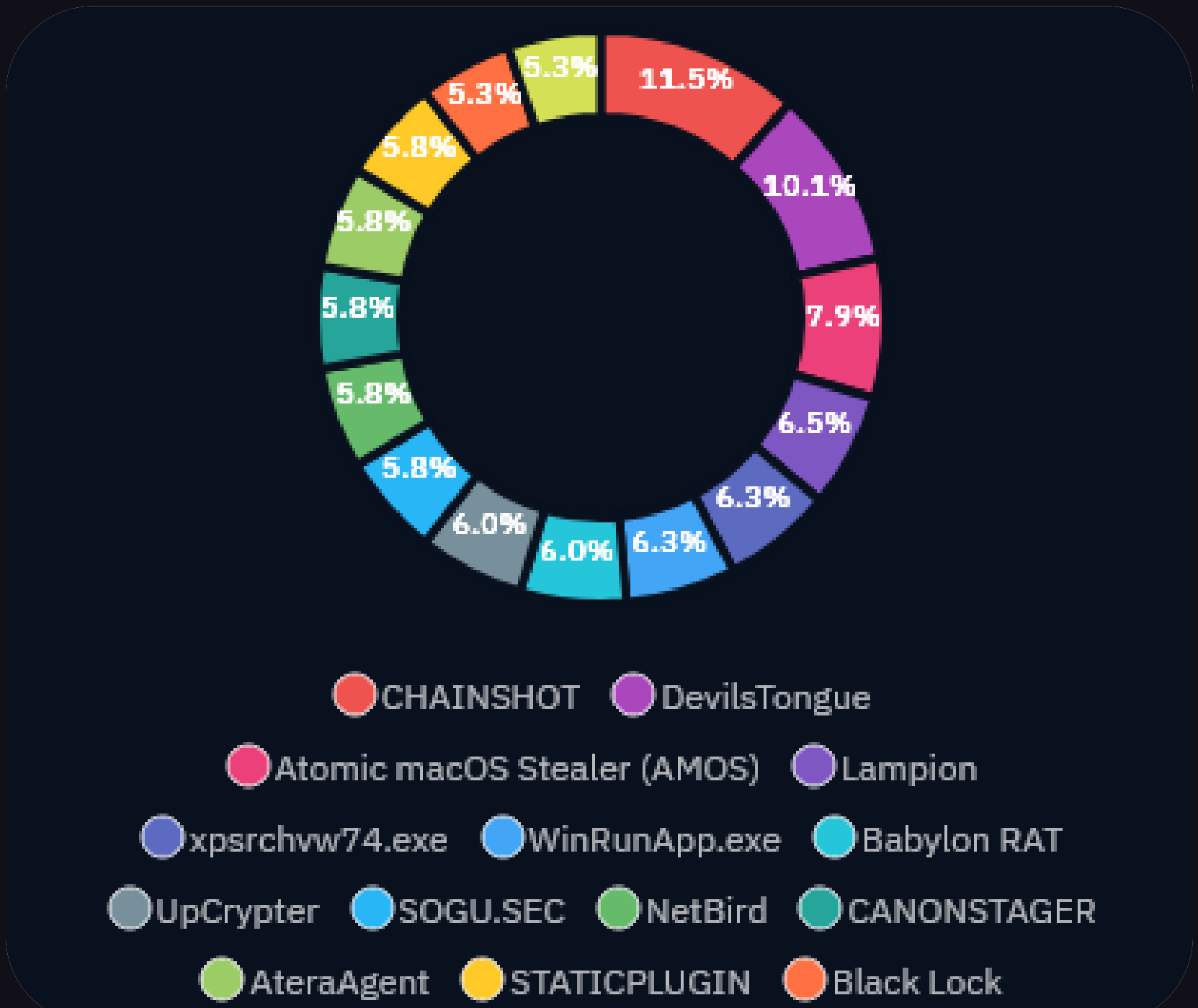
Targeted Countries



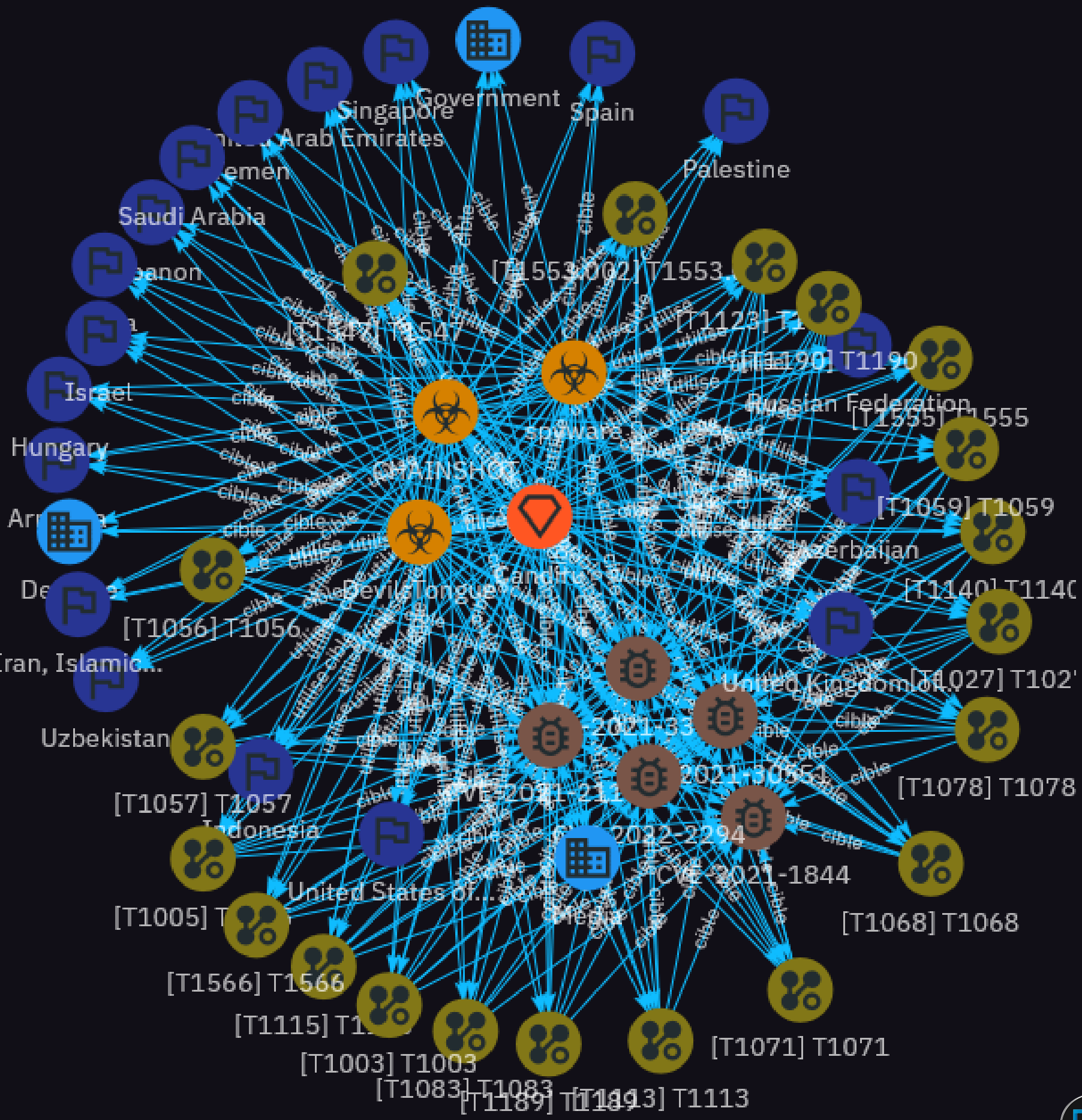
ACTIVE TTPS


[T1036] T1036
[T1204] T1204
[T1055] T1055
[T1059.003] T1059.003
[T1059] T1059
[T1071.001] T1071.001
[T1027] T1027
[T1204.002] Malicious...
[T1566] T1566
[T1583.001] Domains
[T1123] T1123
[T1547.001] T1547.001
[T1140] T1140
[T1187] Forced...
[T1104] Multi-Stage...

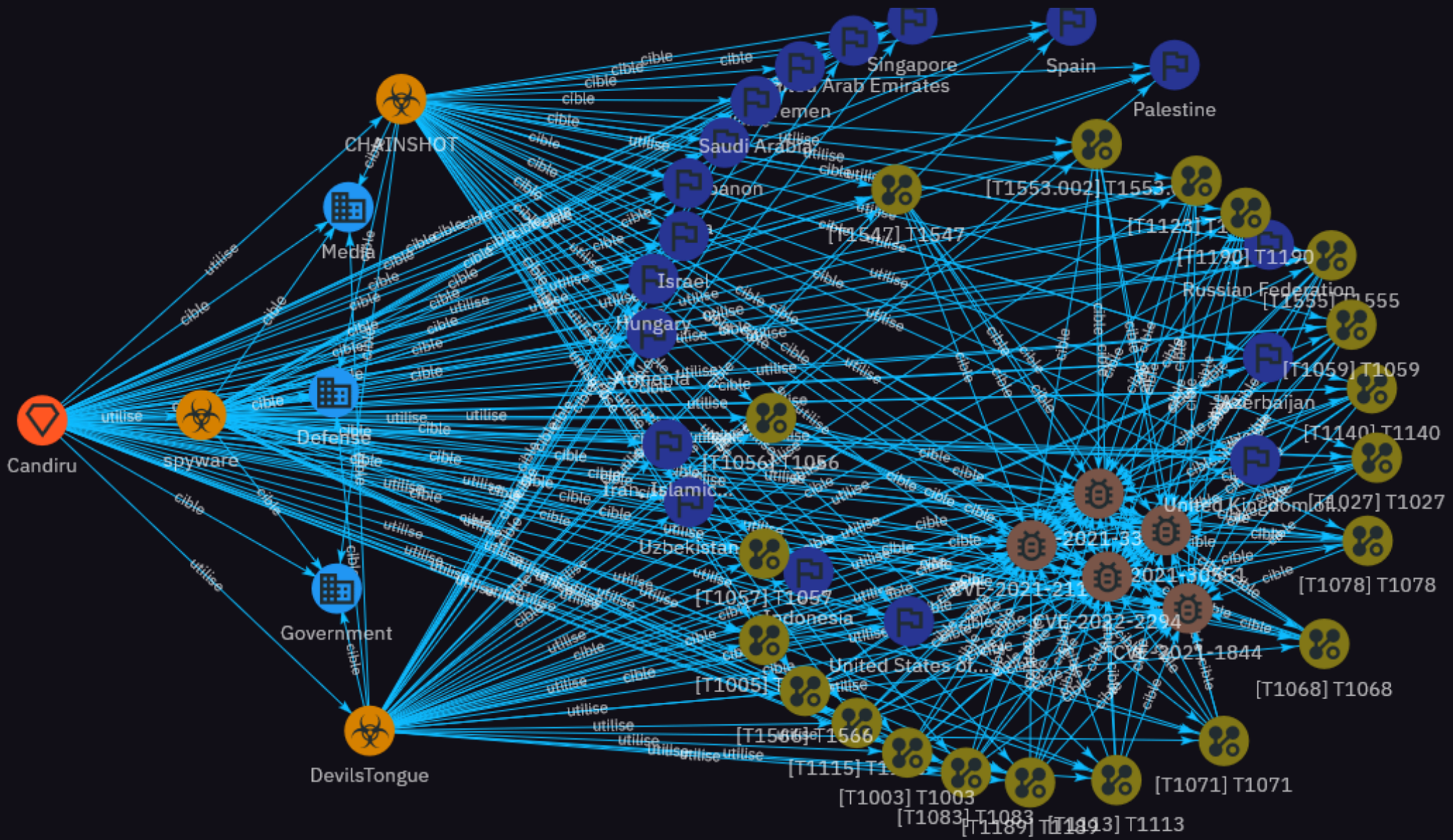
ACTIVE MALWARE



ACTIVITIE OF THREAT : CANDIRU



ACTIVITIE OF THREAT : CANDIRU



ACTIVITIE OF THREAT : CANDIRU

Candiru, société israélienne de « mercenary spyware », vend des capacités d'intrusion clé-en-main à des États pour cibler journalistes, défenseurs des droits, diplomates et opposants. Ses implants- notamment DevilsTongue sur Windows, offrent un contrôle profond des postes et des comptes en ligne.

Cette évolution du spyware Candiru, le DevilsTongue, illustre la montée en puissance des outils d'espionnage numérique, dont la sophistication et l'usage à l'échelle mondiale posent des défis majeurs à la cybersécurité, à la régulation et à l'éthique.

Un arsenal technique et opérationnel hors du commun.

- Modularité et furtivité : DevilsTongue s'infiltre sur Windows, mais aussi sur Android ou iOS grâce à des modules personnalisés. Il utilise des techniques telles que COM hijacking, détournement du registre Windows, drivers noyau et exécution in-memory pour rester invisible et persistant.
- Vecteurs d'infection avancés : phishing ciblé (spearphishing), watering-holes, failles zero-day de navigateurs (notamment Chrome, CVE-2021-21166, CVE-2021-30551, CVE-2022-2294), et programme publicitaire malicieux (capacité Sherlock) permettant même des attaques cross-plateformes via des publicités ciblées.
- Activités post-intrusion : extraction de messages chiffrés (Signal, WhatsApp, Viber), vol de credentials dans LSASS ou navigateurs, accès à la caméra et au micro, capture de cookies et usurpation de sessions web (Gmail, Facebook), upload de fichiers et accés total à la ligne de commande via shell distant.

Modèle économique et géopolitique

- Vente exclusive à des gouvernements : Candiru ne vend qu'à des États ou agences, via des contrats valorisés plusieurs millions d'euros, structurés selon le nombre de cibles surveillées, les modules activés et les territoires concernés. Exemple : 16 M€ pour surveiller 10 terminaux, avec des extensions à prix fort selon les besoins.
- Cloisonnement géographique partiellement respecté : Officiellement, Candiru interdit l'usage dans certains pays (USA, Russie, Chine, Israël, Iran), mais des traces d'utilisation hors cadre existent, preuve du risque de dissémination.

ACTIVITIE OF THREAT : CANDIRU

Résilience face à la régulation et prolifération technique

- Infrastructure mondiale robuste : plusieurs clusters opérationnels actifs en 2025 ont été repérés (Hongrie, Arabie Saoudite, Indonésie, Azerbaïdjan), certains utilisant des couches intermédiaires et le réseau Tor pour l'obfuscation et la redondance, malgré des sanctions internationales et tentatives d'interdiction.
- Rôle de la société civile et des chercheurs : Citizen Lab, Microsoft, Recorded Future et des ONG ont permis d'identifier et d'enrayer des campagnes, mais la réponse réglementaire internationale reste fragmentée alors que la menace, elle, ne cesse de s'étendre.

La menace Candiru change la donne

- Risque systémique pour les droits fondamentaux : ciblage de journalistes, dissidents, élus et avocats, menace sur la confidentialité, la protection des données et l'intégrité démocratique.
- Pression sur les lois et standards : de plus en plus d'États et d'ONG appellent à une gouvernance internationale des armes numériques, face à l'agilité technique et l'opacité des acteurs privés du secteur.
- Impératif pour les RSSI et DSI : élever la sécurité des terminaux, sensibiliser les VIP, et surveiller activement leur exposition numérique n'est plus optionnel. La chaîne d'approvisionnement logicielle et les points d'accès publicitaires sont de nouveaux fronts à protéger.

Candiru symbolise la course technologique entre cyber-offensive privée et sécurité défensive. Sa maîtrise n'est pas seulement un enjeu technique, mais un défi multidimensionnel pour la souveraineté, la confiance numérique et les libertés fondamentales.