WWW.DUDIX-CONSULTING.FR

Les Nouvelles du Front

DUDIX CTI

Semaine 29

21 Juillet 2025

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

TOP THREAT

Targeted Sector: Finance, Govenrnment

Top Targeted Countries: USA, RUS, UKR

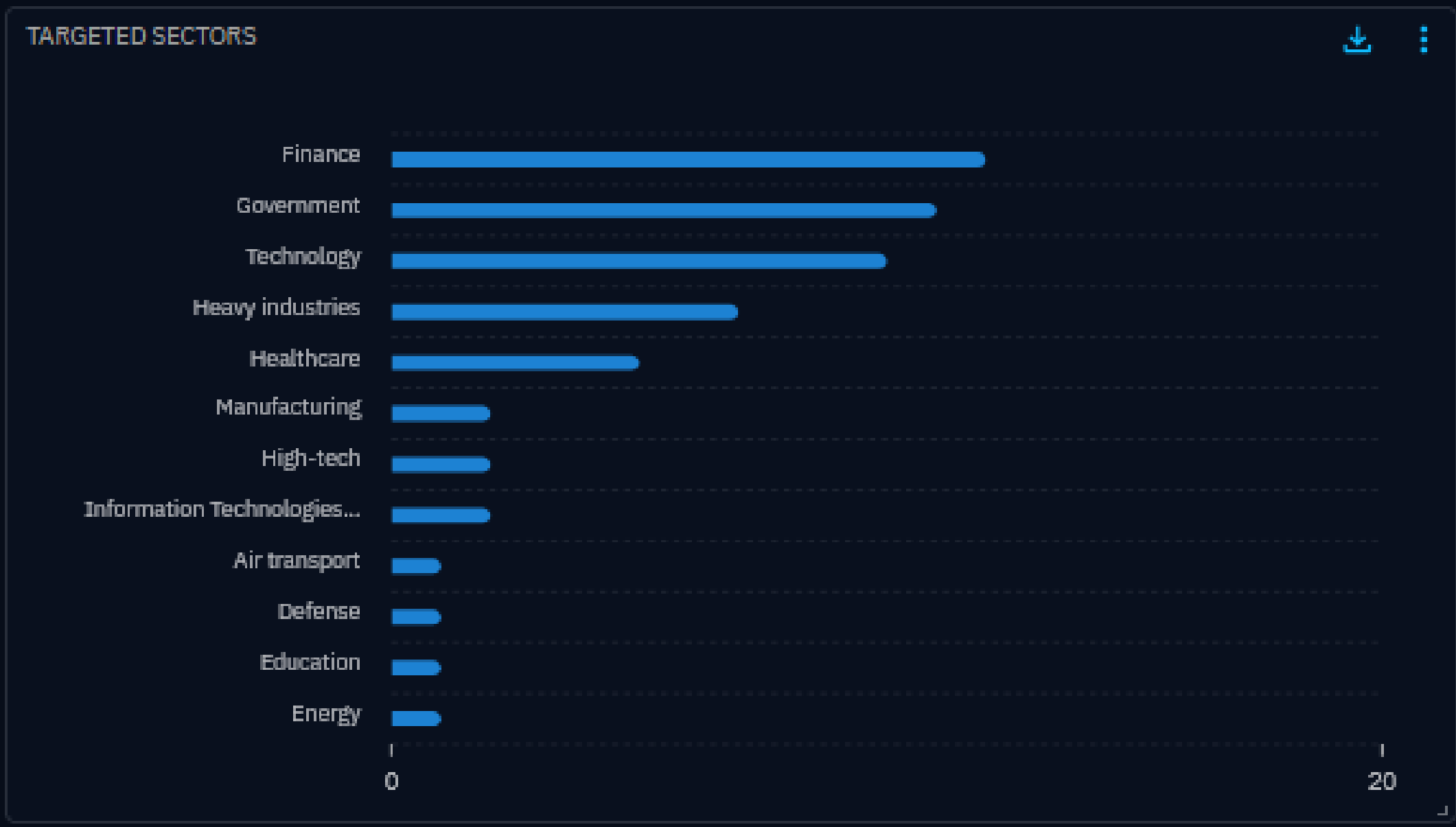
Active Intrusion Set: UNG0002

Active Vuln: CVE-2021-20038

Active TTP: T1027

Active Malware: OVERSTEP (UNC6148)

Top Targeted Sectors



Active Intrusion Sets

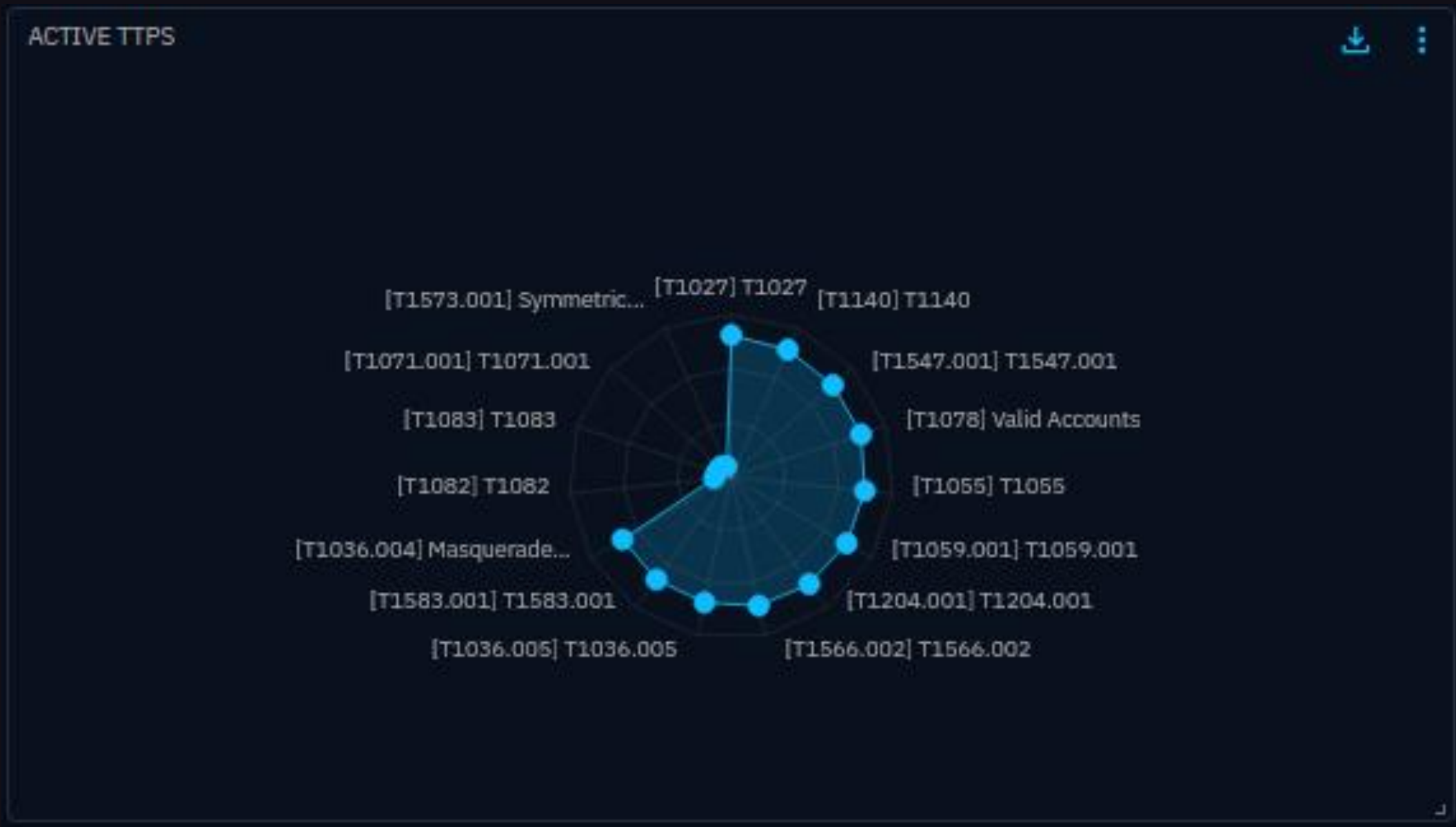
Top Active Vulns

ACTIVE VULNERABILITIES

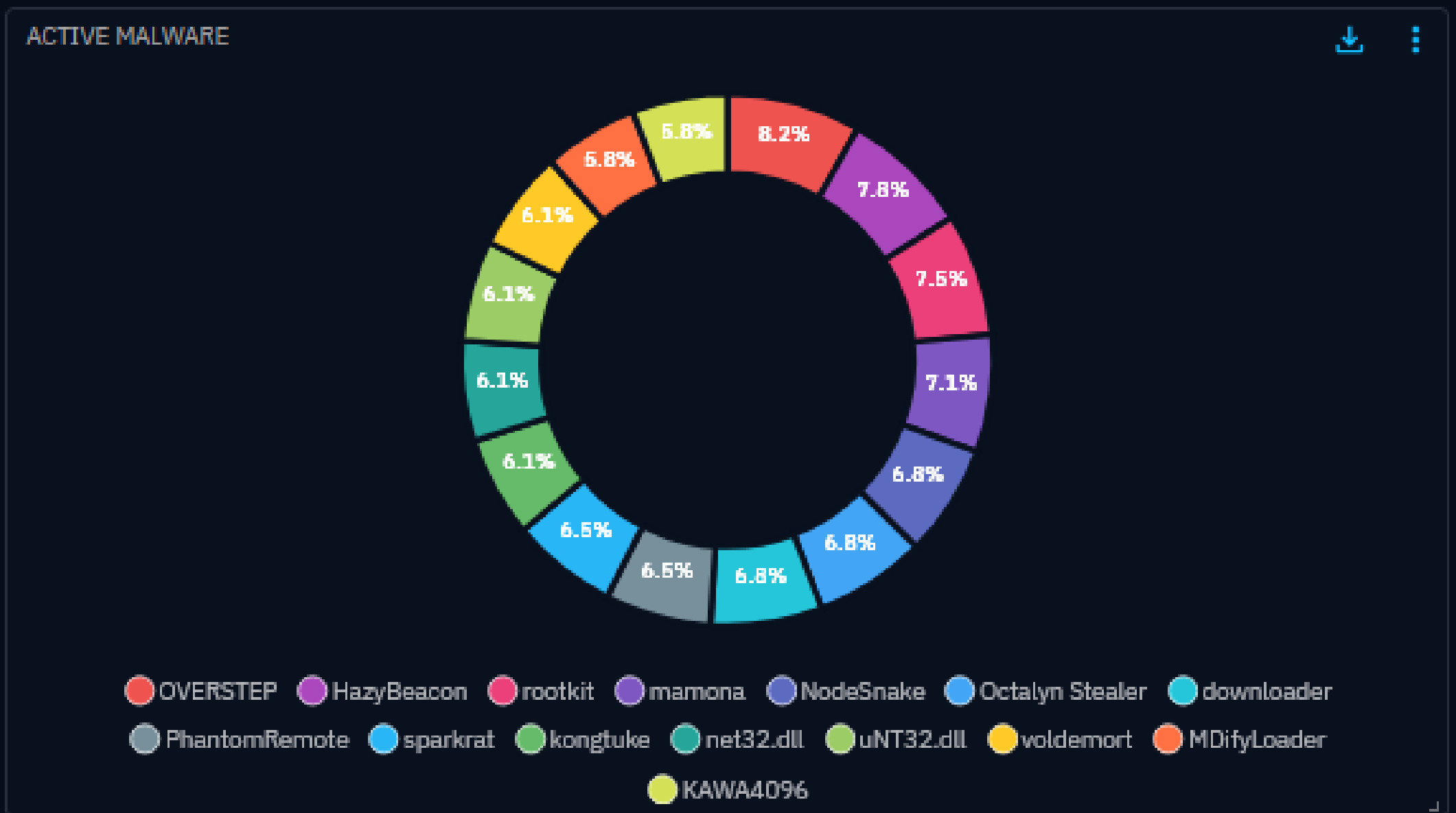
CVE-2021-20038	19
CVE-2021-20039	19
CVE-2024-38475	19
CVE-2025-32819	19
CVE-2021-20035	19
CVE-2023-44221	19
CVE-2024-3721	13

Targeted Countries

ACTIVE TTPS

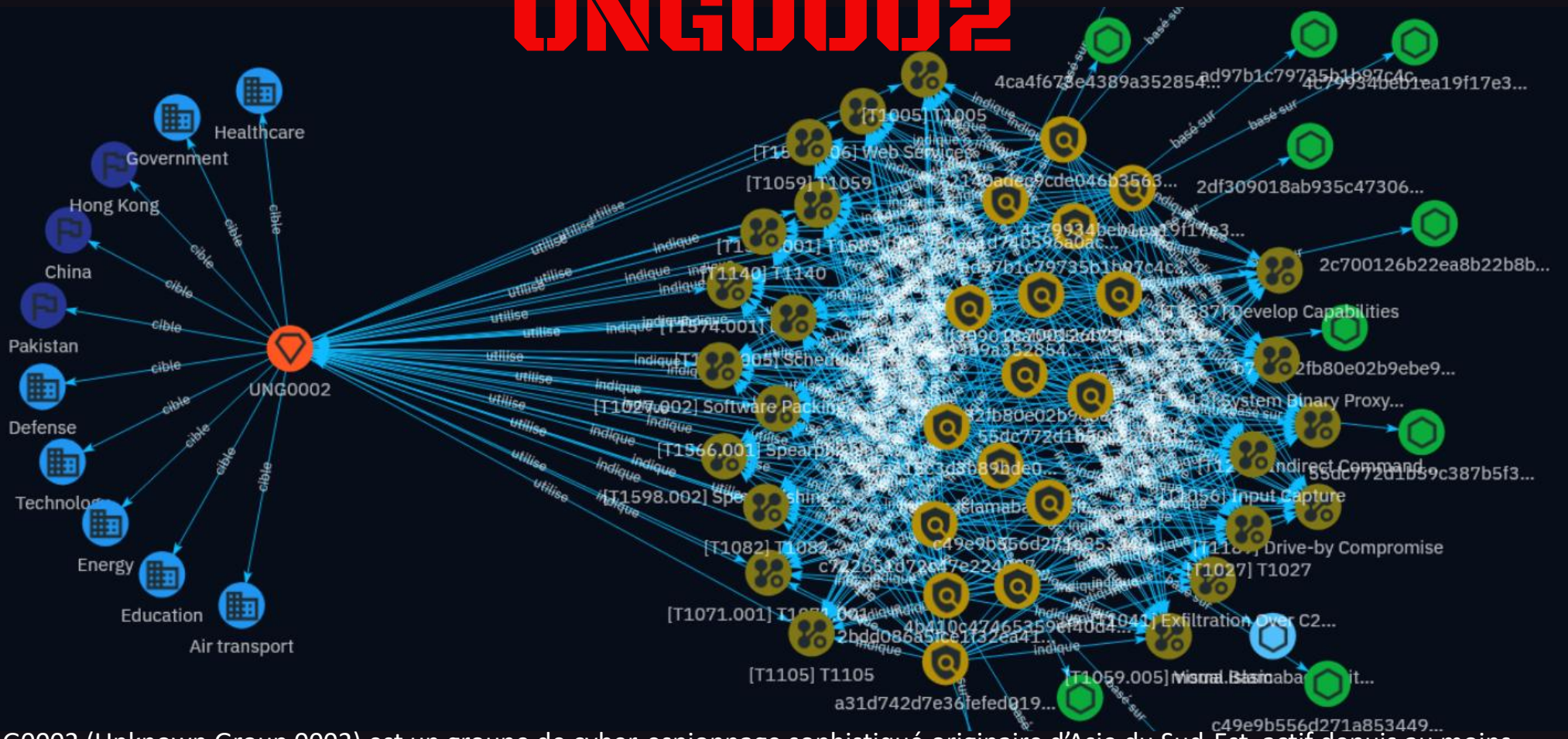

ACTIVE TTPS
[T1573.001] Symmetric...
[T1027] T1027
[T1140] T1140
[T1071.001] T1071.001
[T1547.001] T1547.001
[T1083] T1083
[T1078] Valid Accounts
[T1082] T1082
[T1055] T1055
[T1036.004] Masquerade...
[T1059.001] T1059.001
[T1583.001] T1583.001
[T1204.001] T1204.001
[T1036.005] T1036.005
[T1566.002] T1566.002

ACTIVE MALWARE



ACTIVITIE OF THREAT :

UNG0002



UNG0002 (Unknown Group 0002) est un groupe de cyber-espionnage sophistiqué originaire d'Asie du Sud-Est, actif depuis au moins mai 2024. Ce collectif cible prioritairement des secteurs stratégiques en Chine, à Hong Kong et au Pakistan, tels que la défense, l'aéronautique, l'énergie, la cybersécurité, l'enseignement supérieur, le médical, le jeu vidéo et le développement logiciel.

Tactiques et techniques:
Livraison initiale - Campagnes de spear-phishing contenant des fichiers LNK (shortcuts Windows) et documents faussement professionnels (CV, offres d'emploi, etc.).

Infection multistade - Utilisation en chaîne de scripts VBScript, batch, et PowerShell pour déployer des implants personnalisés.

Social engineering avancé - Emploi du « ClickFix », une fausse page CAPTCHA incitant la victime à lancer des scripts malicieux déguisés, souvent sur des sites imitant des ministères ou organisations officielles.

Décoy documents réalistes - Faux profils très crédibles (ex : designers UI de jeux vidéo, étudiants d'écoles prestigieuses) pour augmenter le taux d'ouverture des pièges.

Sideloading de DLL - Détournement d'applications légitimes (Node-Webkit, Rasphone) pour exécuter discrètement les implants, contournant outils EDR.