WWW.DUDIX-CONSULTING.FR

Les Nouvelles du Front

DUDIX CTI

Semaine 31

04 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, UKR

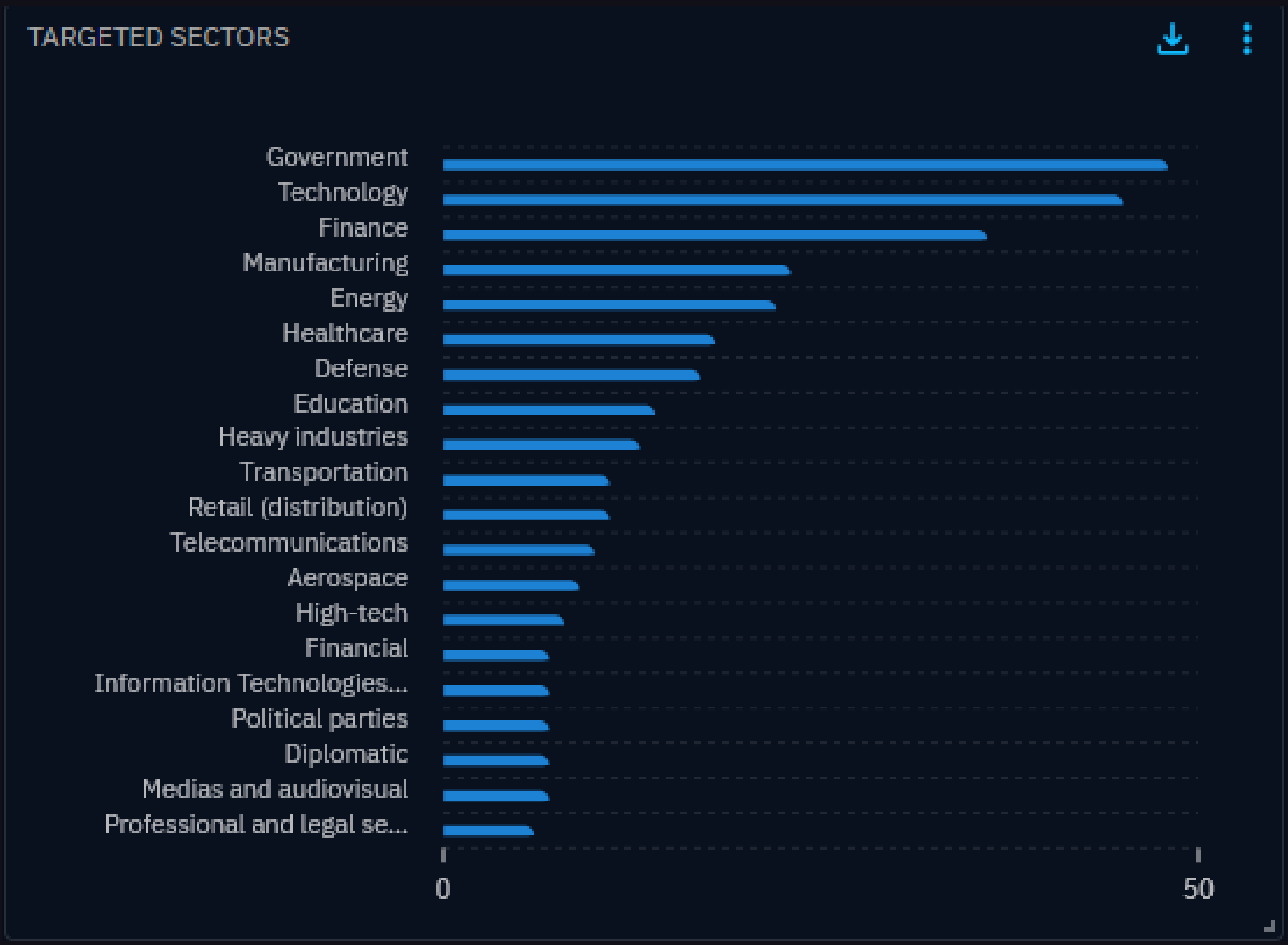
Active Intrusion Set: Linen Typhoon, Violet Typhoon, Storm-2603

Active Vuln: CVE-2025-53770

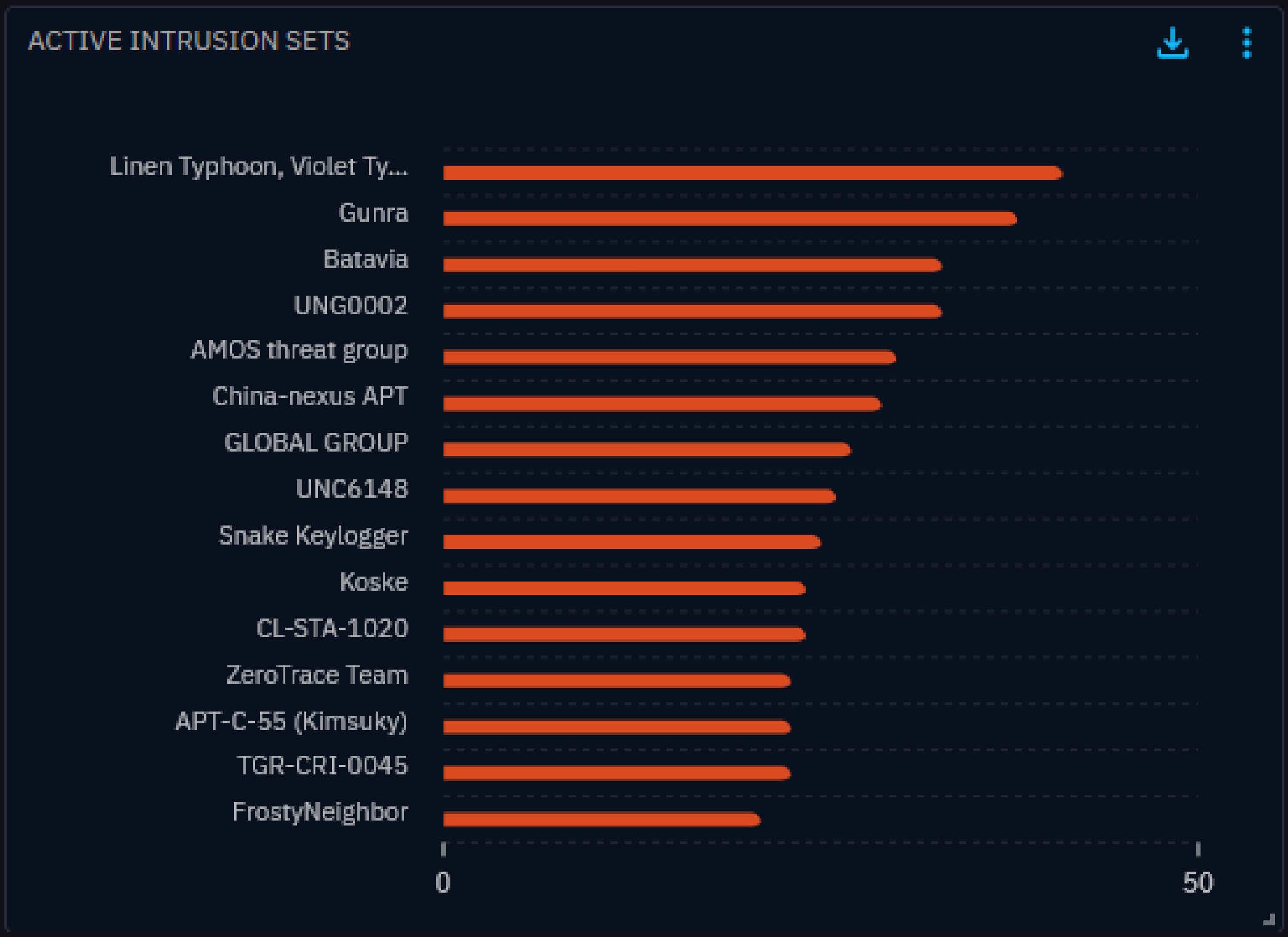
Active TTP: T1027

Active Malware: botnet

Top Targeted Sectors



Active Intrusion Sets

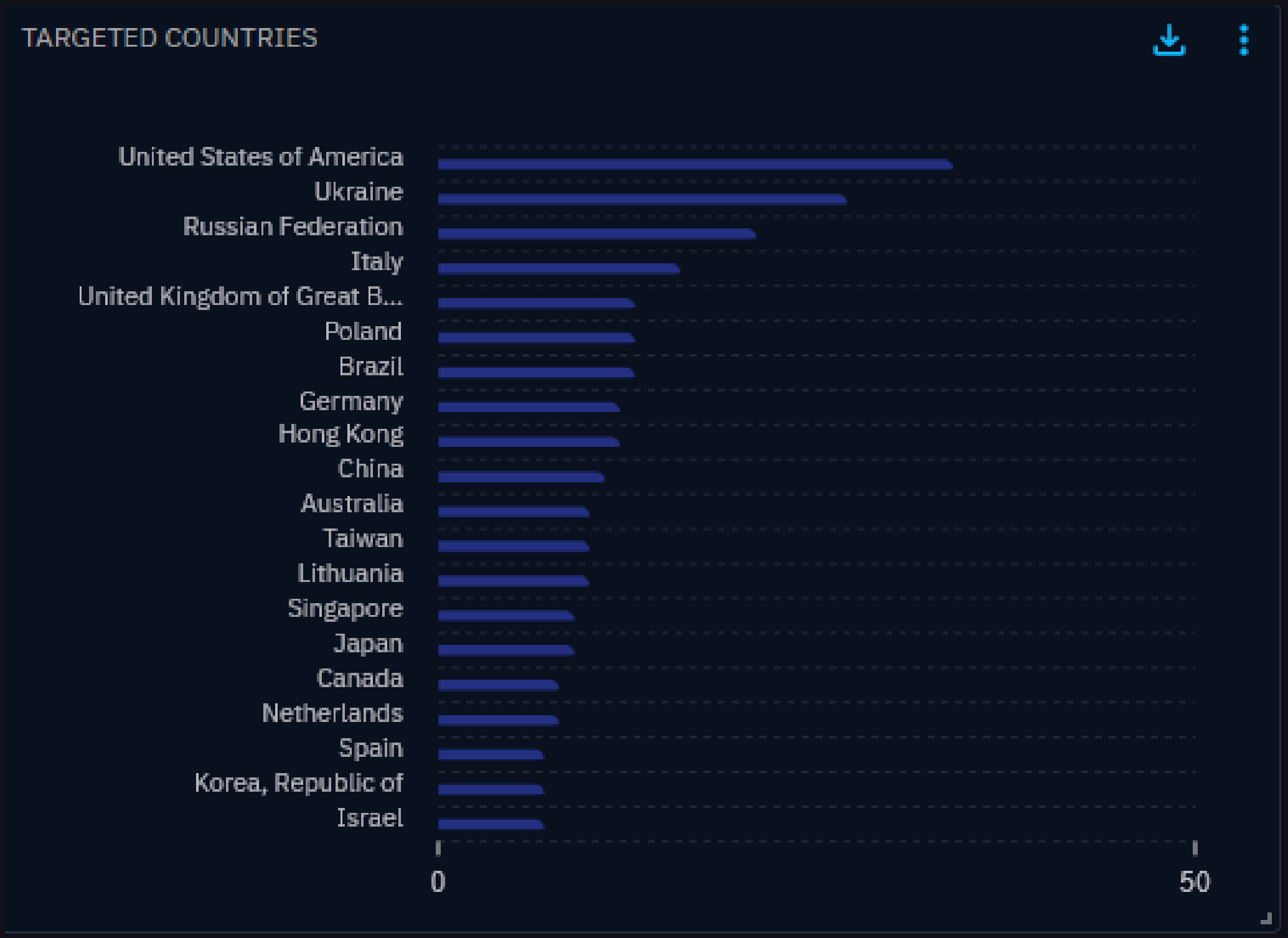


Top Active Vulns

ACTIVE VULNERABILITIES

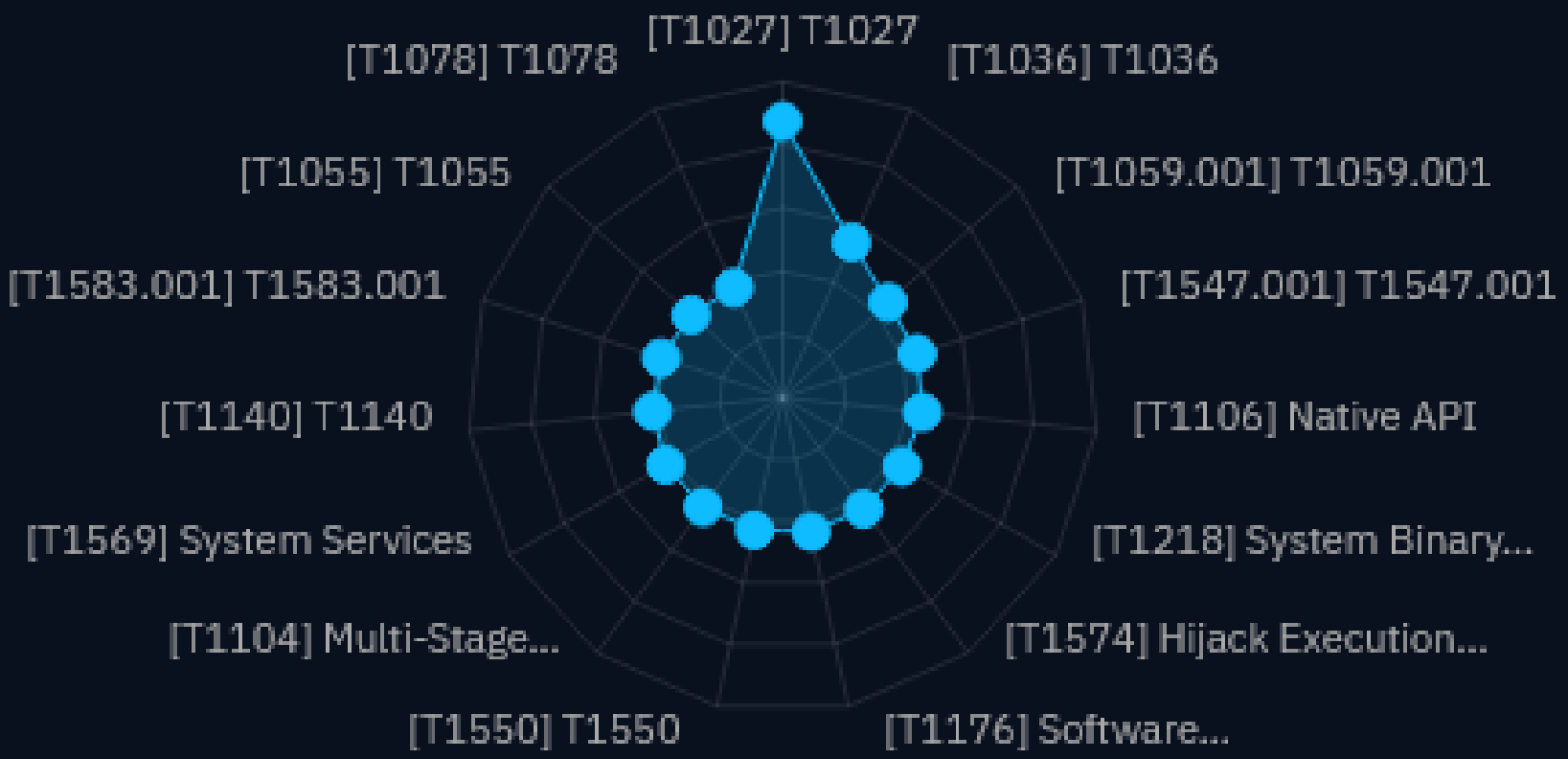
CVE-2025-53770	95
CVE-2025-53771	69
CVE-2025-49706	68
CVE-2025-49704	68
CVE-2024-3721	25
CVE-2025-20337	23
CVE-2025-4632	22

Targeted Countries

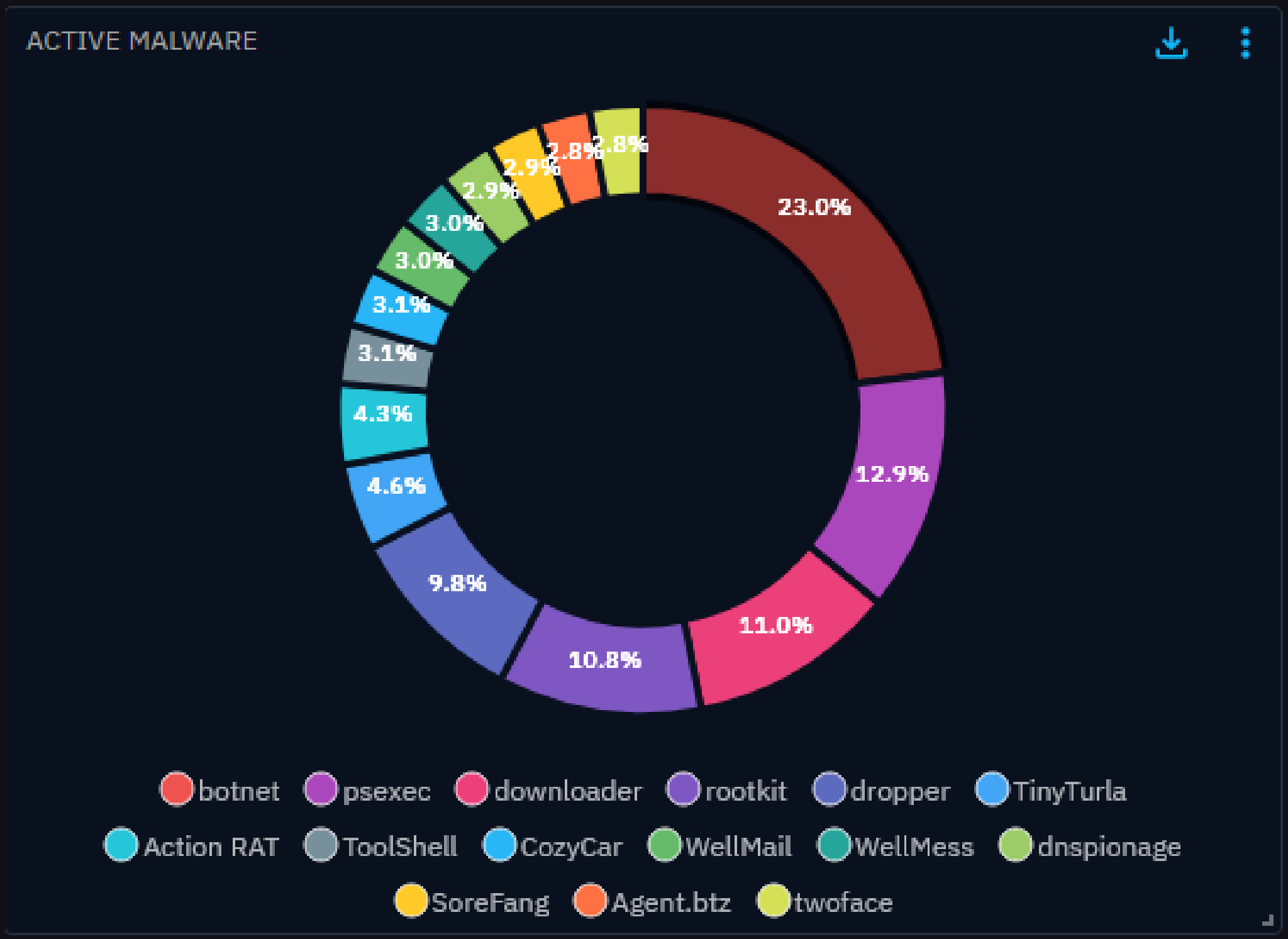


ACTIVE TTPS

ACTIVE TTPS

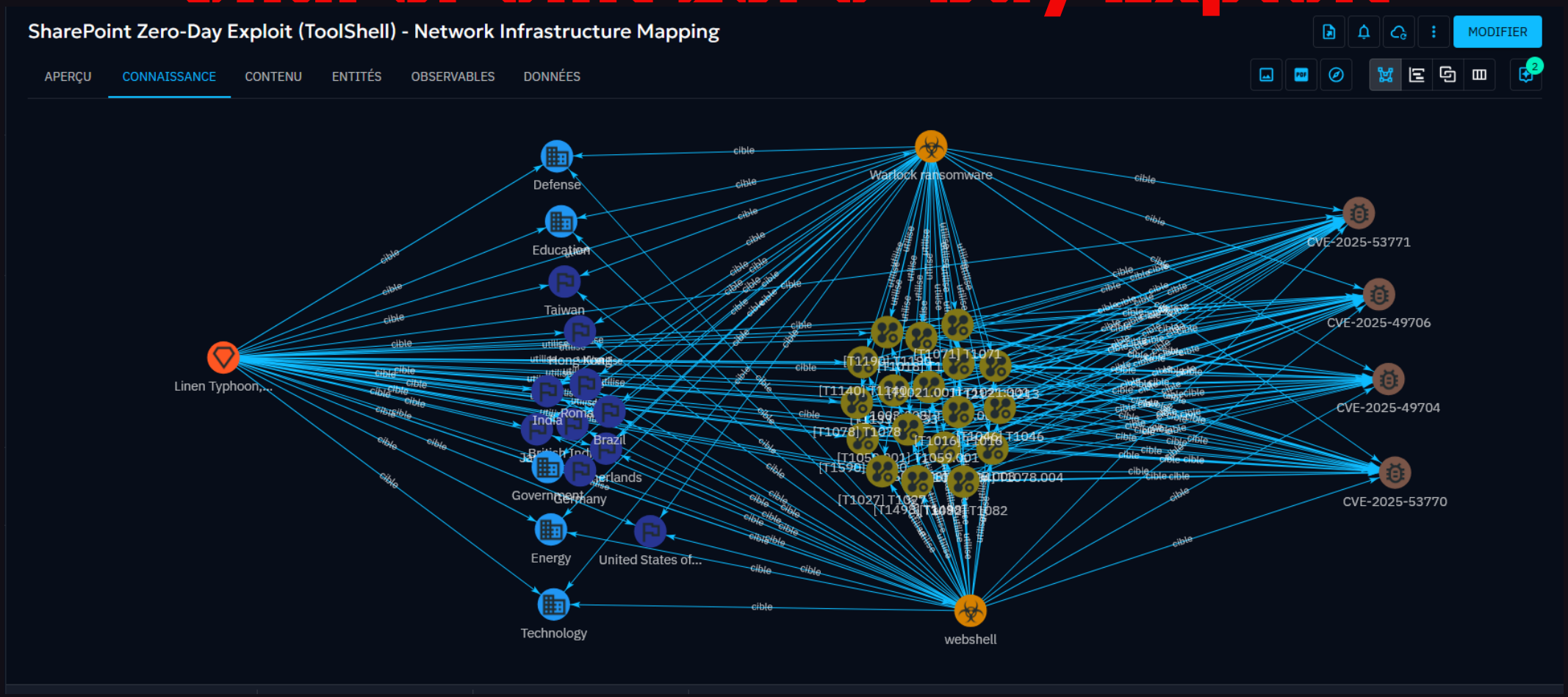


ACTIVE MALWARE



ACTIVITIE OF THREAT :

SharePoint Zero-Day Exploit



Les cybercriminels chinois exploitent des vulnérabilités zero-day dans les serveurs SharePoint, connues sous le nom de ToolShell, affectant près de 150 organisations dans le monde.

Ces attaques, attribuées à des groupes comme Linen Typhoon et Violet Typhoon, ont débuté dès le 17 juillet 2025 et ont ciblé des agences gouvernementales, des infrastructures critiques, des universités et des entreprises privées. L'exploitation impliquait l'enchaînement de plusieurs vulnérabilités et le déploiement d'outils de reconnaissance.

Les attaquants ont utilisé une infrastructure réseau diversifiée, notamment des services cloud et des VPN répartis dans plusieurs pays, pour masquer leur origine.

Cette campagne met en lumière les tactiques sophistiquées employées par les acteurs chinois pour exploiter les infrastructures mondiales de télécommunications et de cloud à des fins de cyber espionnage.

ACTIVITIE OF THREAT :

SharePoint Zero-Day Exploit

En effet, depuis mi-juillet 2025, une vulnérabilité critique non corrigée (« zero-day » CVE-2025-53770 et CVE-2025-53771) touche les serveurs SharePoint « On-Premise ». Plus de 100 organisations à travers le monde (administrations, hôpitaux, universités, fournisseurs d'énergie…) ont déjà été compromises.

L'attaque exploite une faille de désérialisation des données dans la gestion des requêtes ASP.NET, permettant à un attaquant non authentifié d'exécuter du code à distance et de voler des clés MachineKey. Cela ouvre la porte à une persistance invisible sur le serveur, même après application des premiers correctifs.

Points clefs :

-Seuls les serveurs sur site (2016, 2019, SE) sont affectés, le cloud (SharePoint Online) n'est pas concerné.

-Les attaquants peuvent injecter des webshells, exfiltrer des données ou lancer des ransomwares.

-Les secteurs critiques comme la santé, la finance, l'énergie et les services publics sont ciblés massivement.

-Microsoft et les CERT recommandent d'appliquer immédiatement tous les correctifs disponibles, de changer impérativement les clés cryptographiques (MachineKey), d'activer AMSI + antivirus et d'assurer une surveillance constante de l'environnement.

Cette attaque démontre — une fois de plus — la nécessité d'une vigilance cyber accrue, d'une politique de patching rapide et d'un monitoring continu de ses SI.