WWW.DUDIX-CONSULTING.FR

DUDIX Consulting

Les Nouvelles du Front

DUDIX CTI

Secteur stratégique:

Gouvernement

26 Juillet 2025

HORS SERIE

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

TOP THREAT

Top targeted country: USA

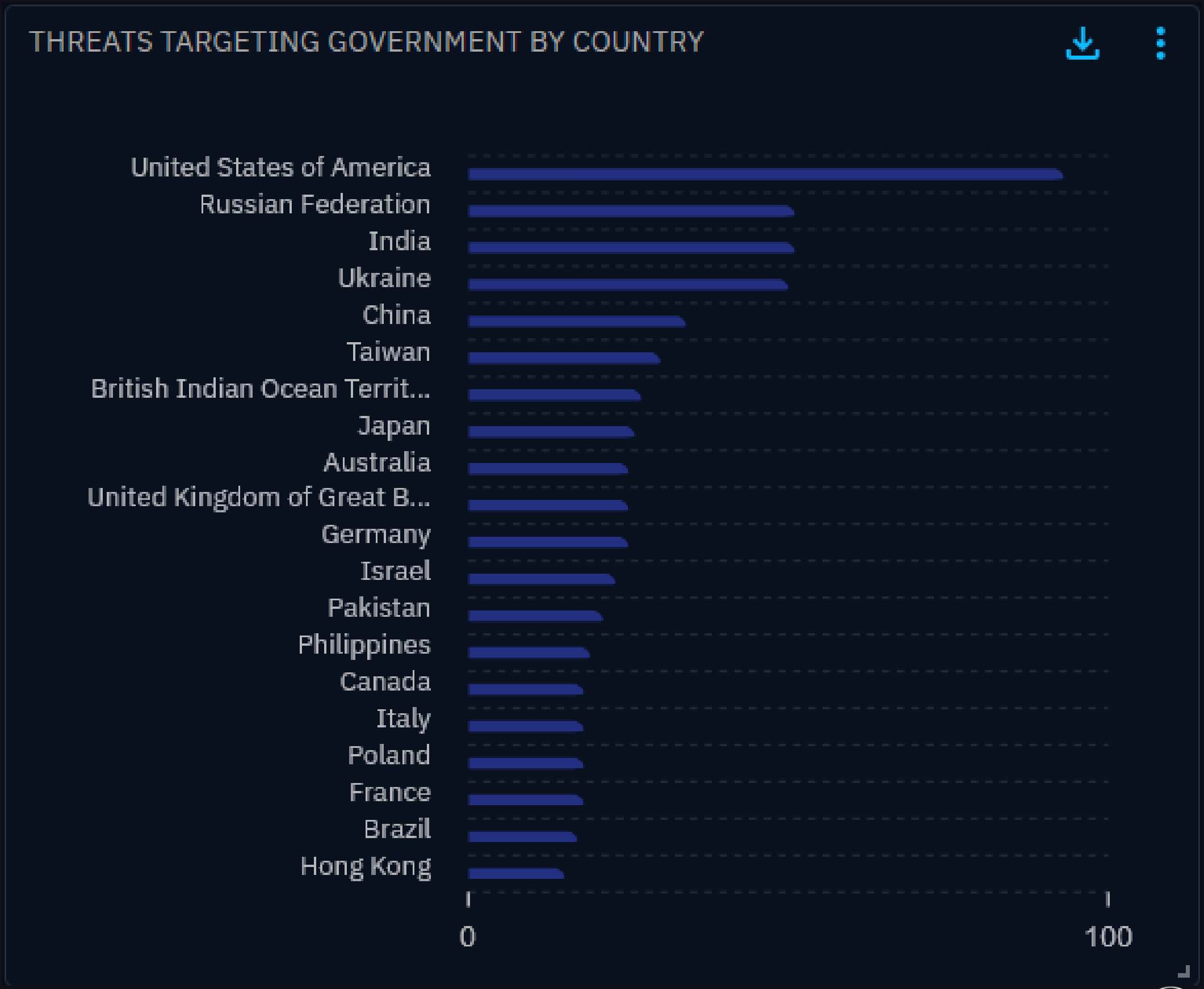
Top threat: RedGolf

Top malware: Cobalt Strike

Active vuln: CVE-2021-44228

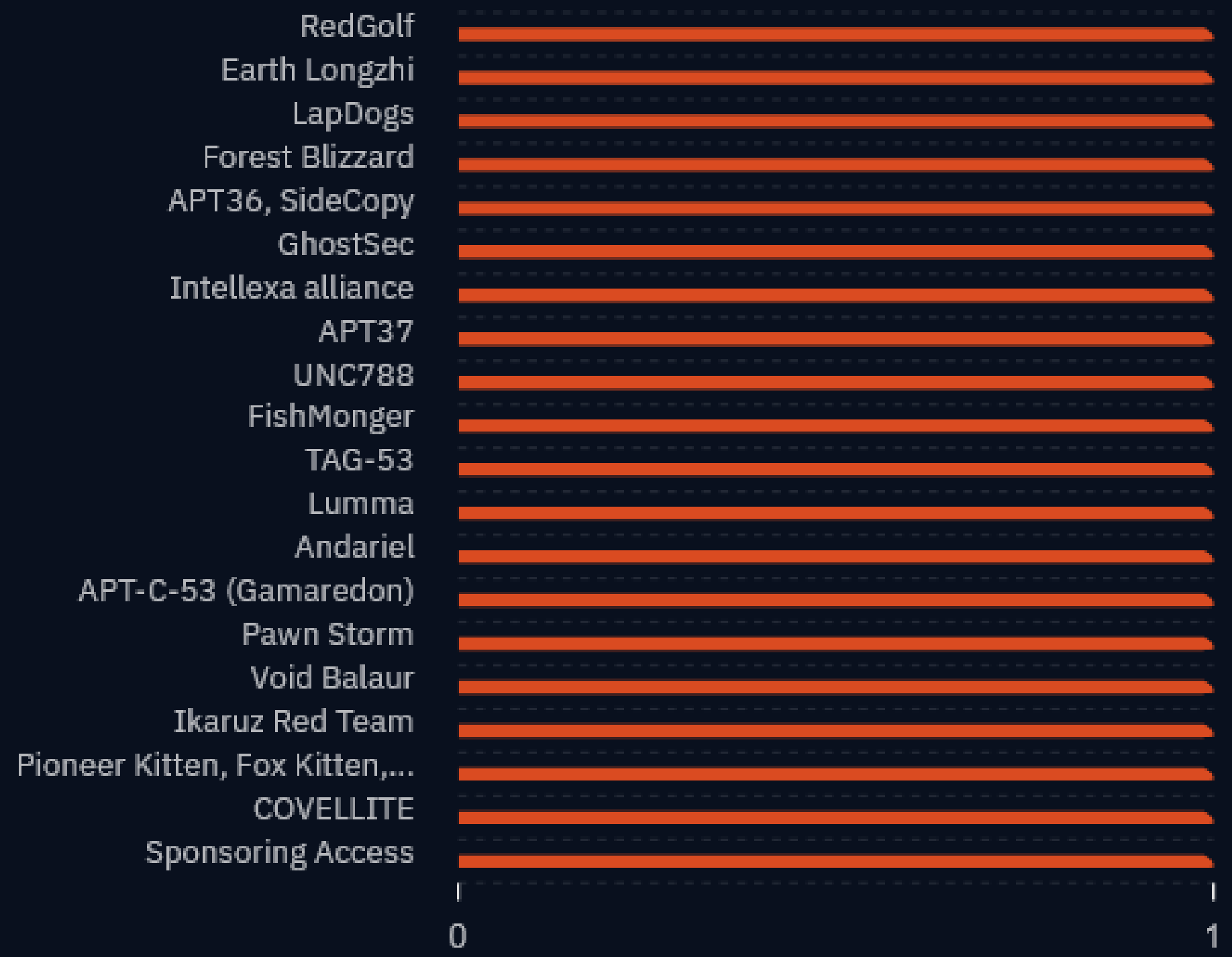
Active TTP: T1027, T1140, T1556

Top targeted country



Top threats

TOP 20 THREATS TARGETING GOVERNMENT

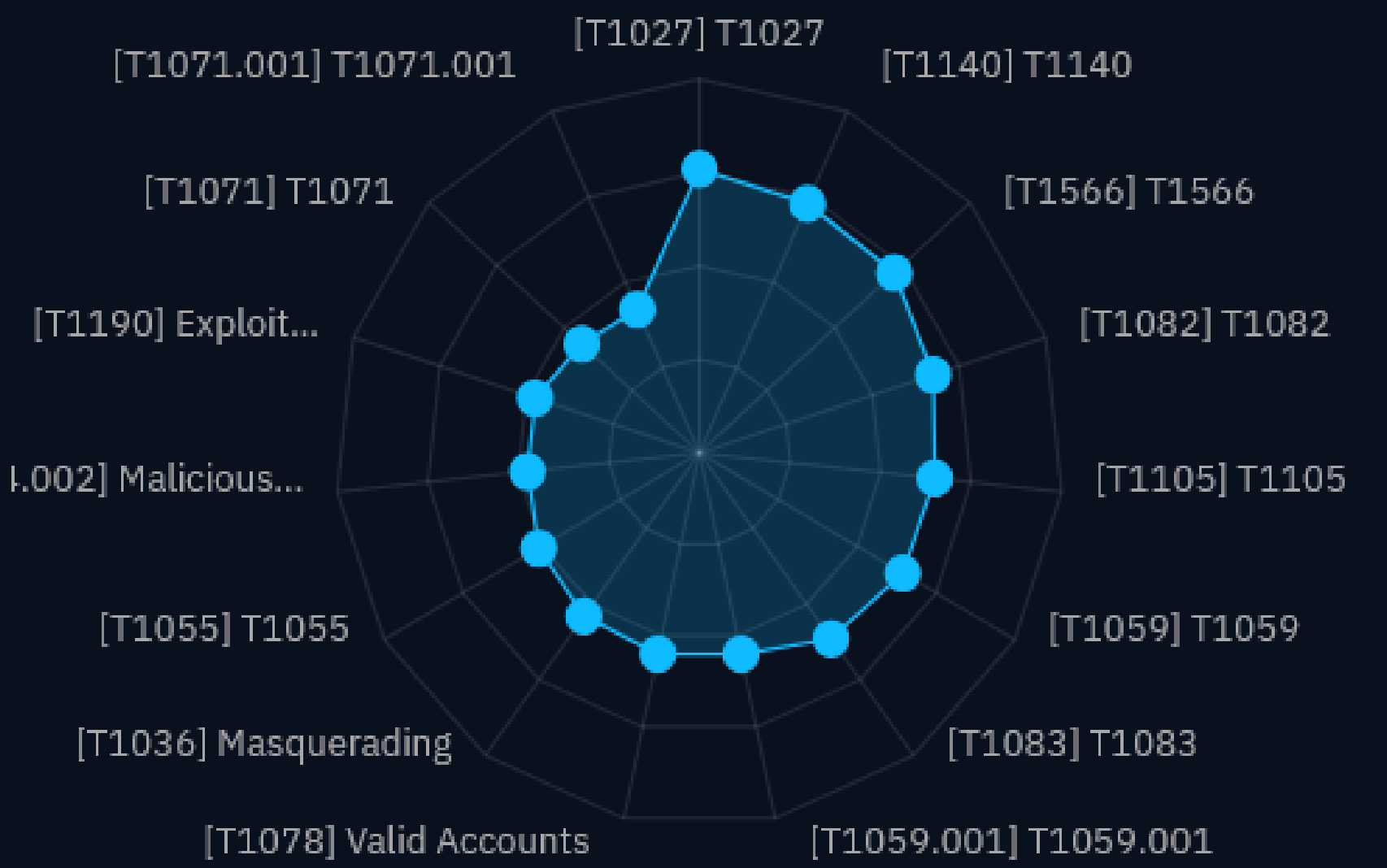


Top malware

TOP 20 MALWARE USED BY THREATS TARGETING GOVERNMENT

Top TTPS

TOP TECHNIQUES USED BY THREATS TARGETING GOVERNMENT



Top vulnerabilities

TOP VULNERABILITIES TARGETED BY THREATS TARGETING GOVERNMENT

CVE-2021-44228	10
CVE-2017-11882	8
CVE-2023-38831	8
CVE-2024-21887	6
CVE-2023-48788	6
CVE-2023-46805	5
CVE-2020-1472	5

Résumé

Au troisième trimestre 2025, le secteur gouvernemental fait face à plusieurs nouvelles tendances majeures en matière de cybermenaces.

Exploitation de vulnérabilités critiques et attaques de masse sur l'infrastructure IT.

Des failles comme CitrixBleed 2 (CVE-2025-5777) ont été activement exploitées, permettant le vol de jetons de session et le contournement de l'authentification multifacteur. Ces attaques visent les équipements critiques exposés sur internet, avec des millions de tentatives observées depuis le printemps.

Prolifération des ransomwares sophistiqués et double extorsion.

Les opérateurs de ransomware concentrent leurs attaques sur les institutions publiques via des tactiques comme la double extorsion (vol de données avant chiffrement), entrainant de sévères interruptions de services gouvernementaux.

Offensives d'APT (Advanced Persistent Threat) sponsorisées par des États.

Les groupes liés à la Chine, la Russie ou l'Iran accentuent le cyberespionnage et cherchent à infiltrer durablement les réseaux gouvernementaux pour le renseignement et la perturbation de processus décisionnels via des campagnes ciblant spécifiquement la diplomatie, les alliances stratégiques et les personnalités politiques sensibles.

Phishing avancé, attaques par ingénierie sociale et IA générative.

L'utilisation de l'IA permet aux acteurs malveillants de lancer des campagnes de phishing (mails, deepfakes, voice phishing/vishing), usurpant de faux portails officiels ou générant des contenus personnalisés pour tromper les agents publics. On observe également une intensification des attaques par "Browser-in-the-Browser".

Menaces liées à l'intelligence artificielle et à la synthèse de l'identité.

Les risques de fraude à l'identité, de clonage vocal et de création de fausses identités numériques (synthetic identity fraud) se multiplient, facilitant l'usurpation d'agents et la compromission des processus critiques.

Risques sur la chaîne d'approvisionnement et dépendance aux technologies tierces.

Des attaques indirectes via des prestataires ou de nouveaux logiciels gouvernementaux exposent les administrations à des brèches entraînant la fuite de données sensibles ou l'installation de portes dérobées.

Multiplication des familles de malware et groupes de menace.

En 2025, le nombre de nouvelles familles de malwares et de groupes d'attaquants organisés a encore augmenté, obligeant les agences à investir dans la veille et l'intelligence de sécurité pour rester à jour face à la diversité des outils utilisés contre les administrations.

Les administrations réagissent principalement par la mise en œuvre de l'architecture zero trust, le renforcement de la surveillance des terminaux, l'accélération de la gestion des correctifs, la formation accrue des agents, et un recours croissant à l'intelligence artificielle défensive pour anticiper et contrer ces menaces évolutives.