



Les Nouvelles du Front

DUDIX CTI

Semaine 35

2 septembre 2025

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



TOP THREAT

Targeted Sector: Government

Top Targeted Countries: USA

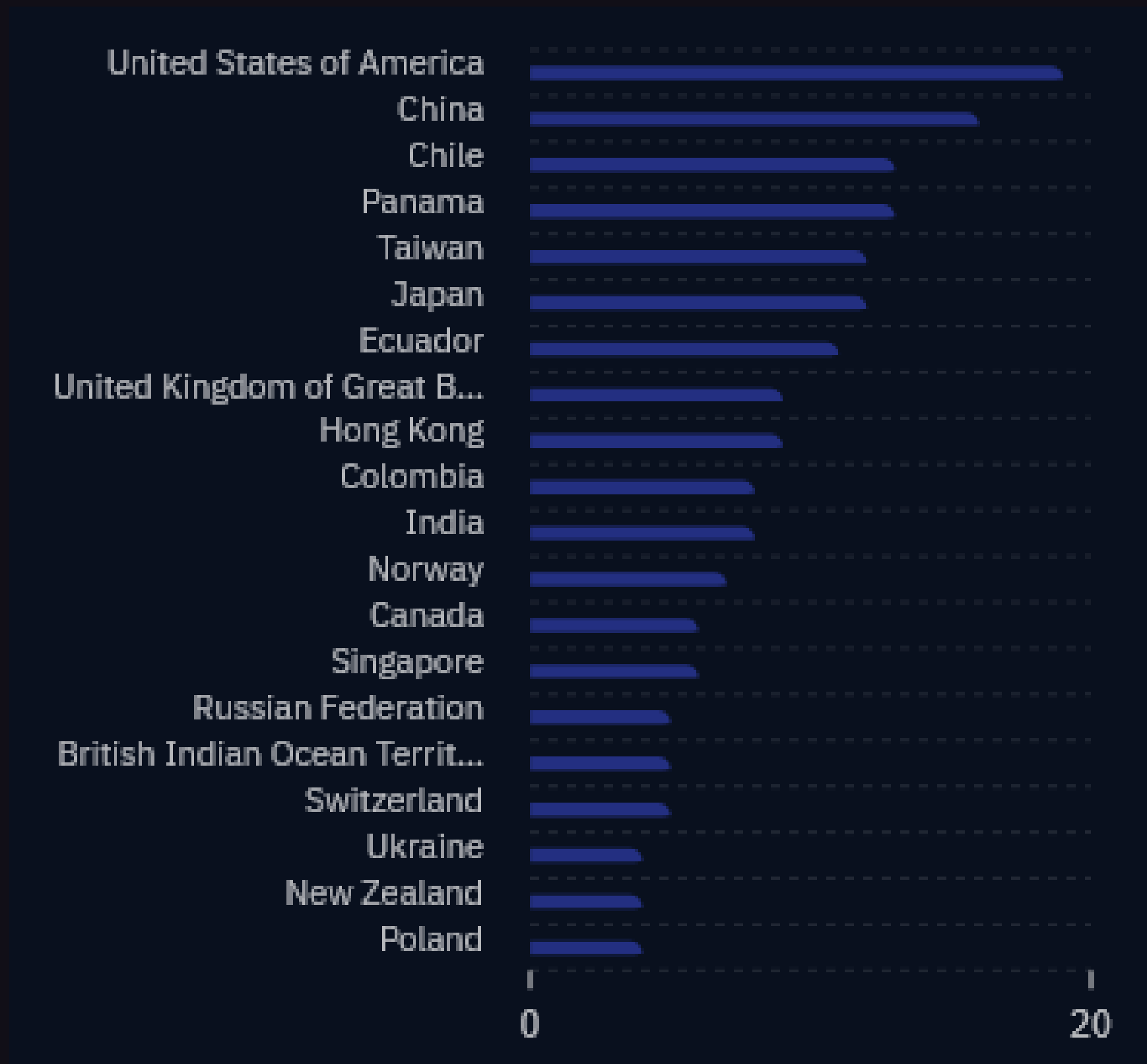
Active Intrusion Set: TAOTH

Active Vuln: CVE-2018-0171

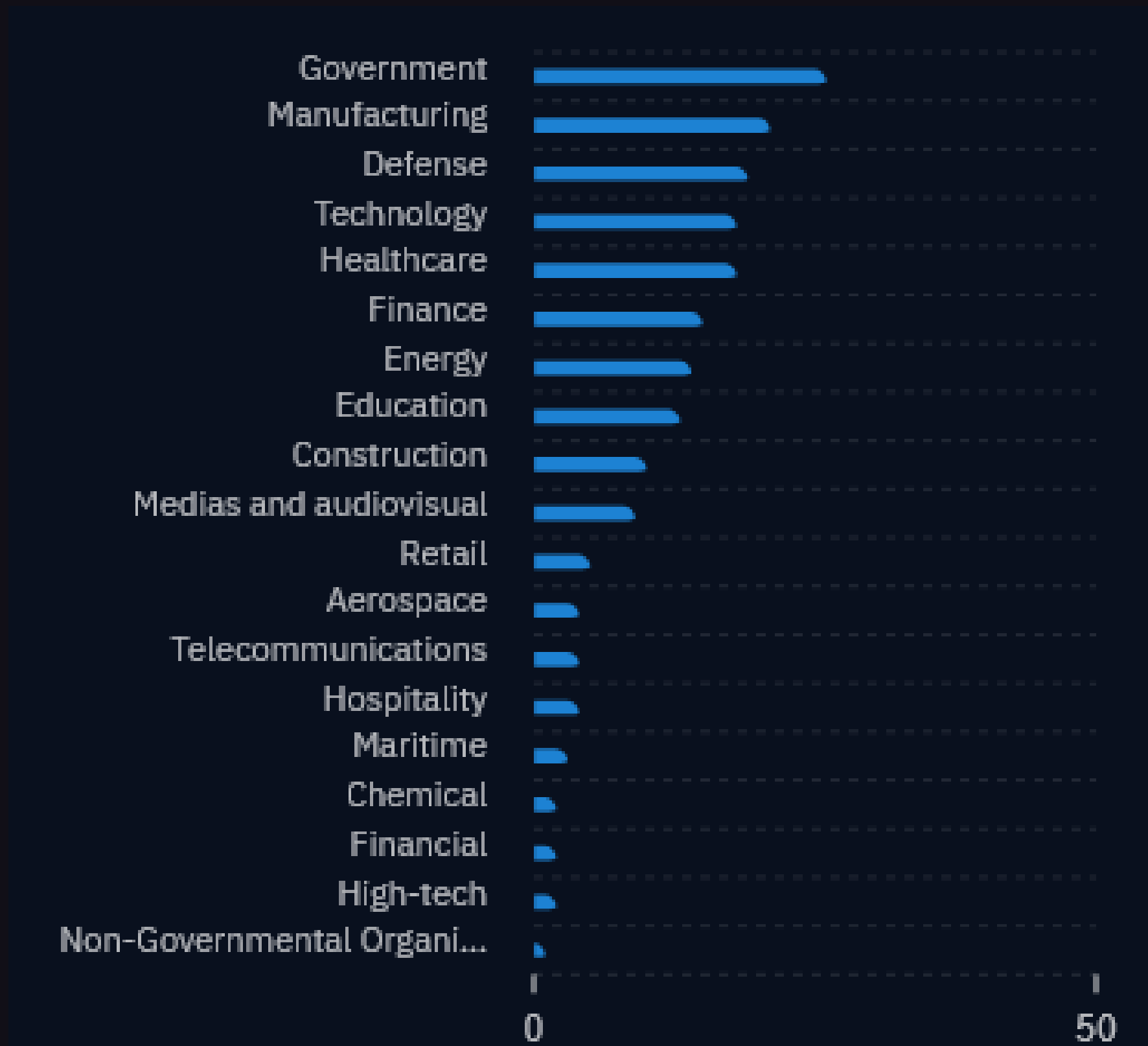
Active TTP: T1566, TA0011

Active Malware: DESFY, ClickFix

Targeted Countries









Top Targeted Sectors



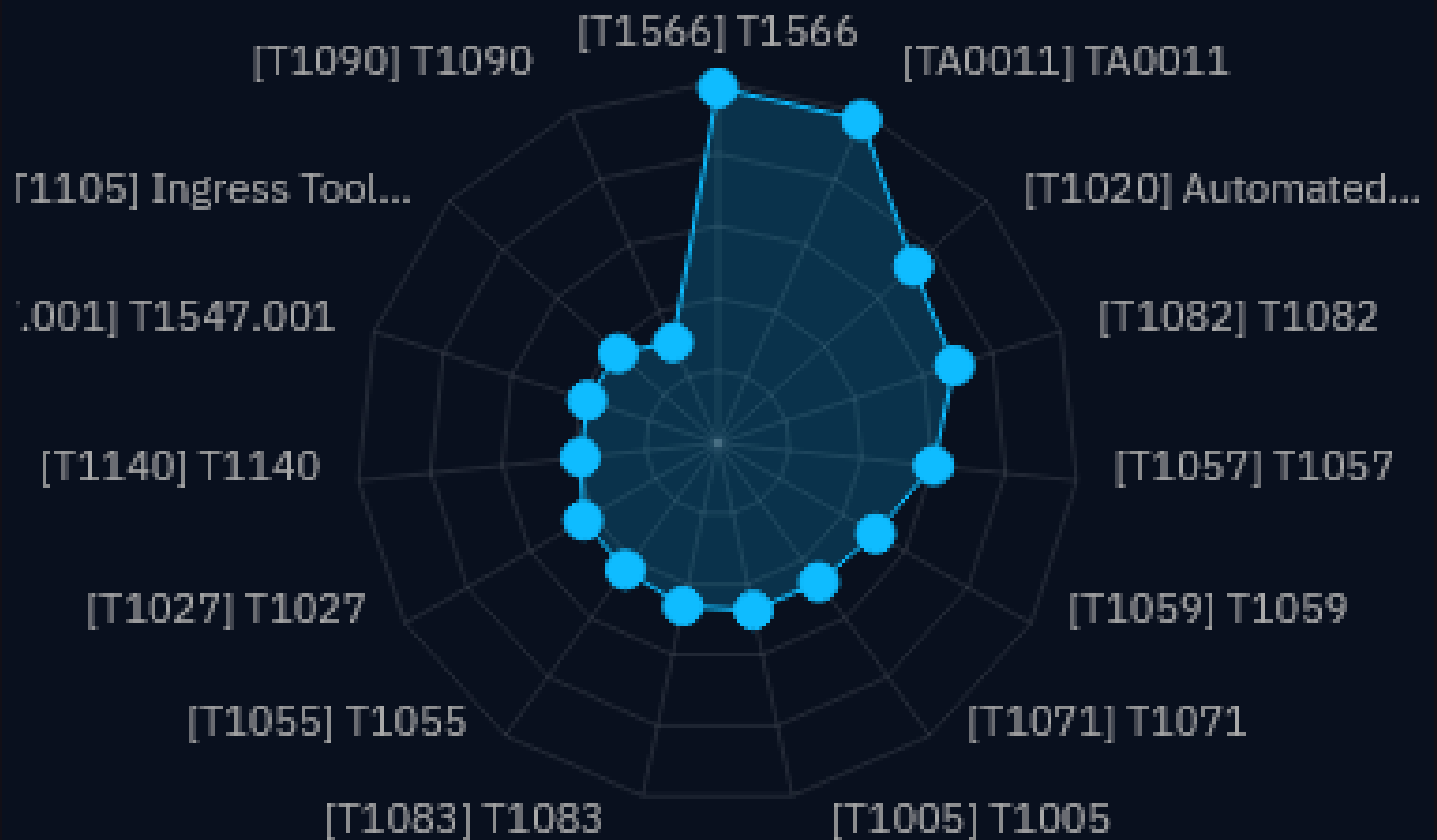
Active Intrusion Sets



Top Active Vulns

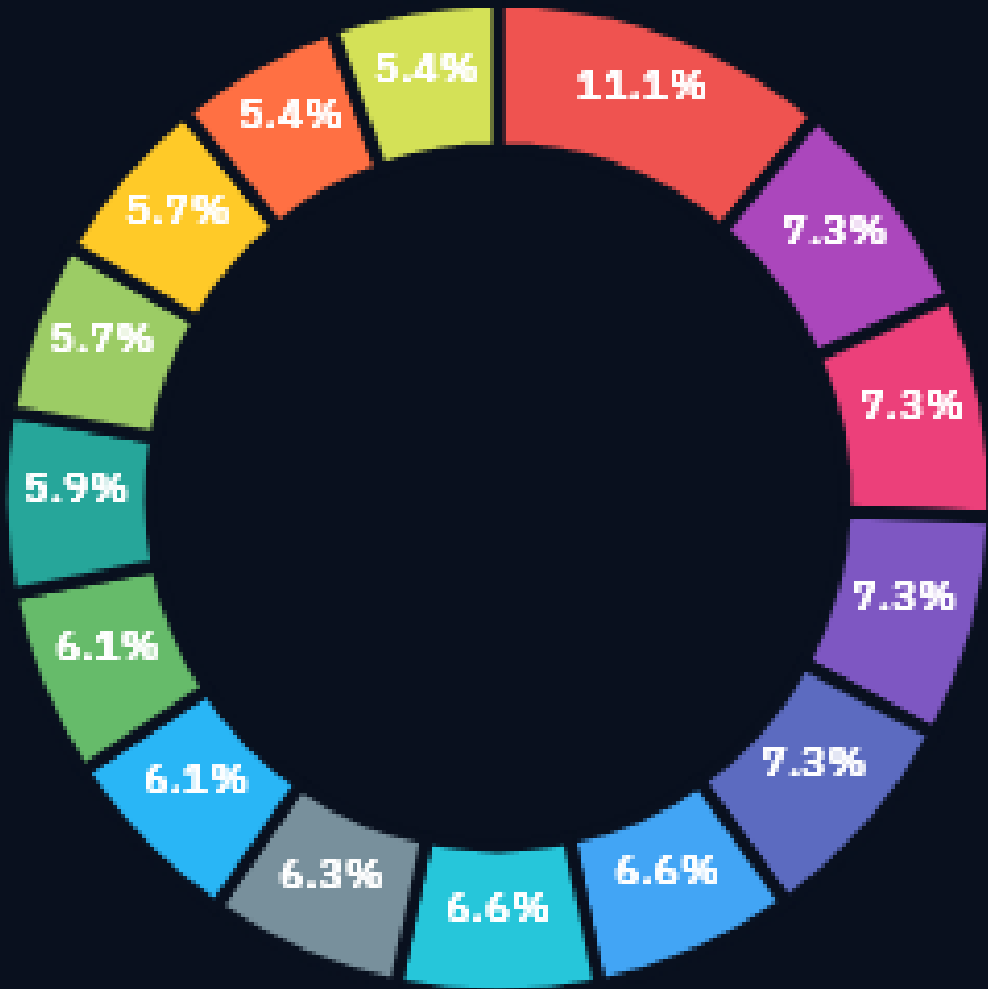
	CVE-2018-0171	32
	CVE-2023-20273	30
	CVE-2023-20198	30
	CVE-2024-3400	21
	CVE-2023-46805	15
	CVE-2024-42009	14

ACTIVE TTPs



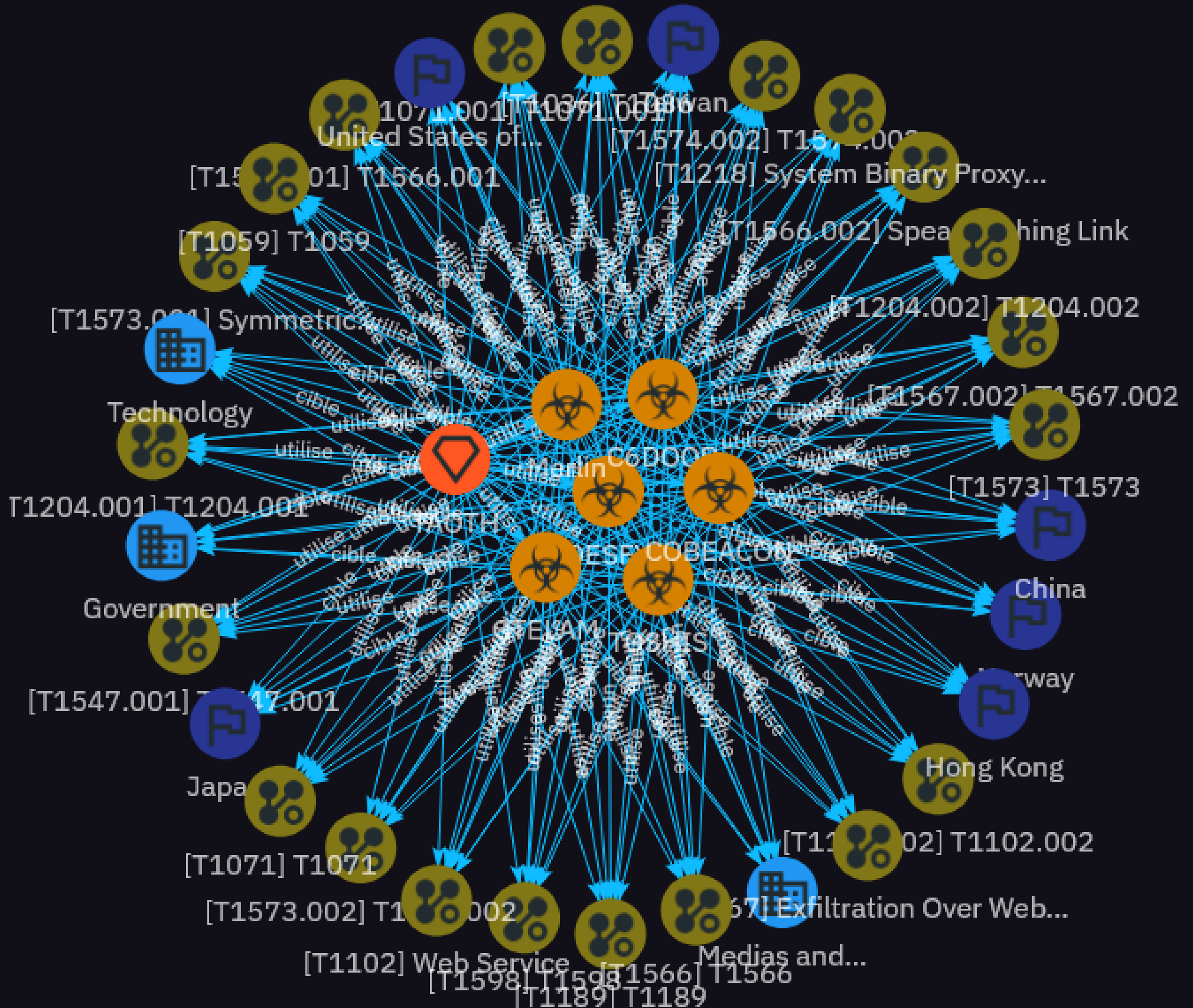
ACTIVE MALWARE

ACTIVE MALWARE



- clickfix
- DESFY
- TOSHIS
- GTELAM
- C6DOOR
- Merlin
- PromptLock
- NightSpire
- UPX
- ConfuserEx
- Underground ransomware
- Babylon RAT
- UpCrypter
- SOGU.SEC
- CANONSTAGER

ACTIVITIE OF THREAT : TAOTH



ACTIVITE OF THREAT : TAOTH

Les opérations principales :

- 1) Mises à jour falsifiées via le logiciel Sogou Zhuyin, déclenchant l'installation de malwares :
 - TOSHIS : chargeur (loader/stager), dérivé de Xiangoop. Il injecte du shellcode dans des exécutables légitimes (ex. SunloginDesktopAgent.exe, SearchIndexer.exe) puis communique avec un serveur C&C pour télécharger des cargos utiles (Cobalt Strike, backdoors).
 - DESFY : spyware récoltant les noms de fichiers depuis Desktop et Program Files pour identifier les cibles de valeur
 - GTELAM : spyware collectant les noms de fichiers (PDF, DOC, XLS, PPT...), puis les exfiltrant via Google Drive en chiffrement AES
 - C6DOOR : backdoor écrite en Go permettant commandes système, captures d'écran, transferts de fichiers, scans, et injection de shellcode. Le code contient des artefacts en chinois simplifié, signifiant un opérateur probablement sinophone.
- 2) Campagne de spear-phishing parallèle en Asie de l'Est (avec quelques cibles en Norvège et aux États-Unis) :
 - Envoi d'e-mails ciblés incluant URL piégées ou documents factices menant à :
 - Des pages OAuth frauduleuses (Google ou Microsoft) demandant des accès gmail.modify, mail.read, mail.send afin de compromettre les boîtes mail.
 - Des pages imitant des services cloud (ex. Tencent Cloud StreamLink), incitant à télécharger des archives ZIP malveillantes contenant TOSHIS.

Attribution et tactiques globales

- Le groupe TAOTH partage des infrastructures C&C, des variantes de malwares, et des tactiques similaires à celles observées dans des attaques précédentes (ex. Cas ITOCHU) — tunnels VS-Code, attaques en chaîne d'approvisionnement via des applications légitimes (YouDao, Sogou).
- Les techniques correspondent aux codes MITRE tels que T1566 (spear-phishing), T1574.002 (hijacking de mises à jour), T1071 (communication C&C), T1547.001 (persistance)

RESUME: TAOTH

La campagne TAOTH, détectée en août 2025, est une opération d'espionnage ciblée exploitant un logiciel obsolète (Sogou Zhuyin) et des tactiques de spear-phishing évoluées.

Elle déploie plusieurs malwares (TOSHIS, DESFY, GTELAM, C6DOOR) à des fins de surveillance, collecte de données et contrôle à distance.

Seules la vigilance, la gestion stricte des logiciels hérités et les mesures proactives de sécurité peuvent en limiter les risques.