DUDIX CTI

Les Nouvelles du Front

S37

15 septembre 2025

Basé sur un cluster OpenCTI enrichi en temps réel, auto-hébergé et affuté chaque jour

www.dudix-consulting.fr

TOP THREAT

Targeted Sector: Government

Top Targeted Countries: India

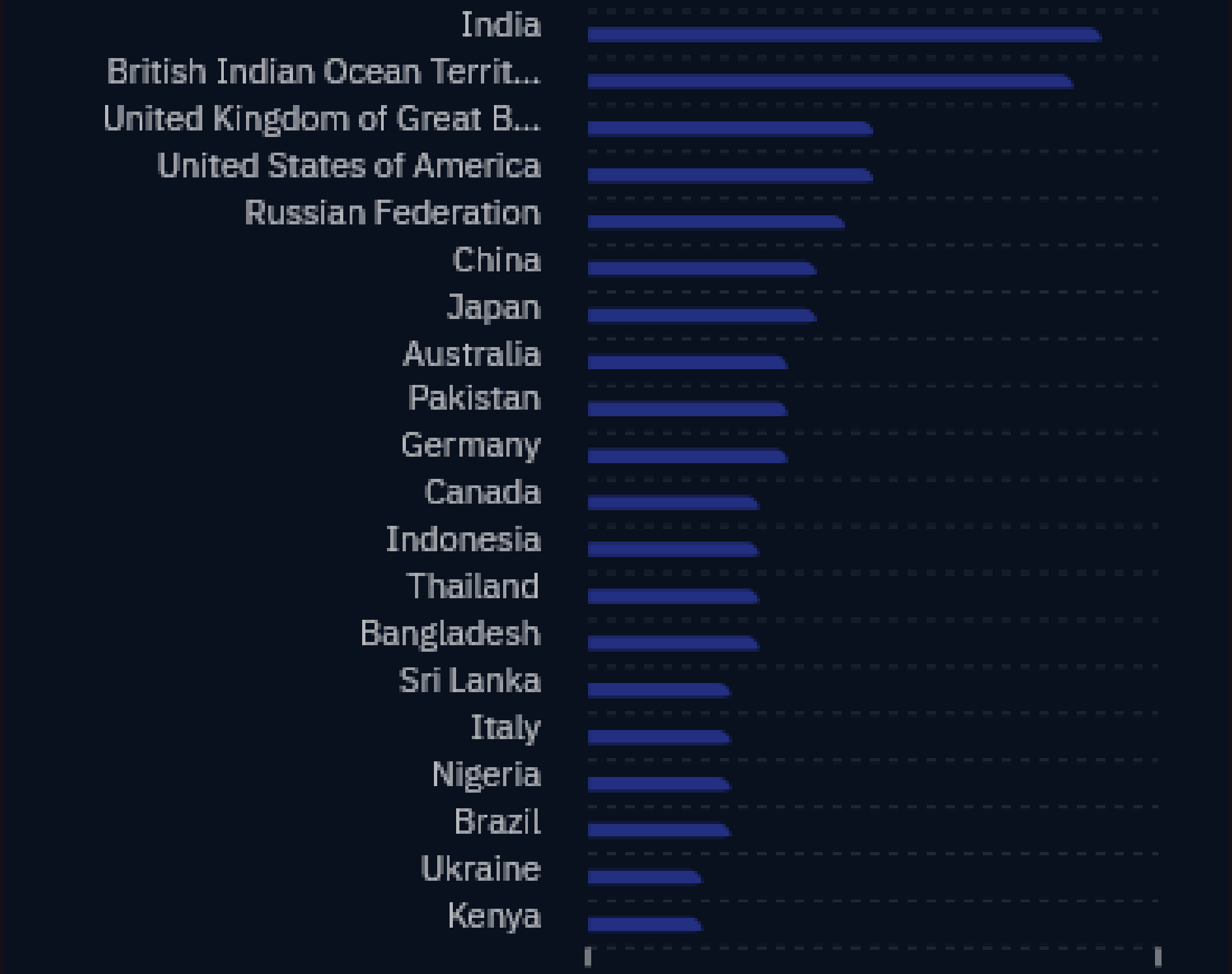
Active Intrusion Set: EvilAI

Active Vuln: CVE-2025-20265

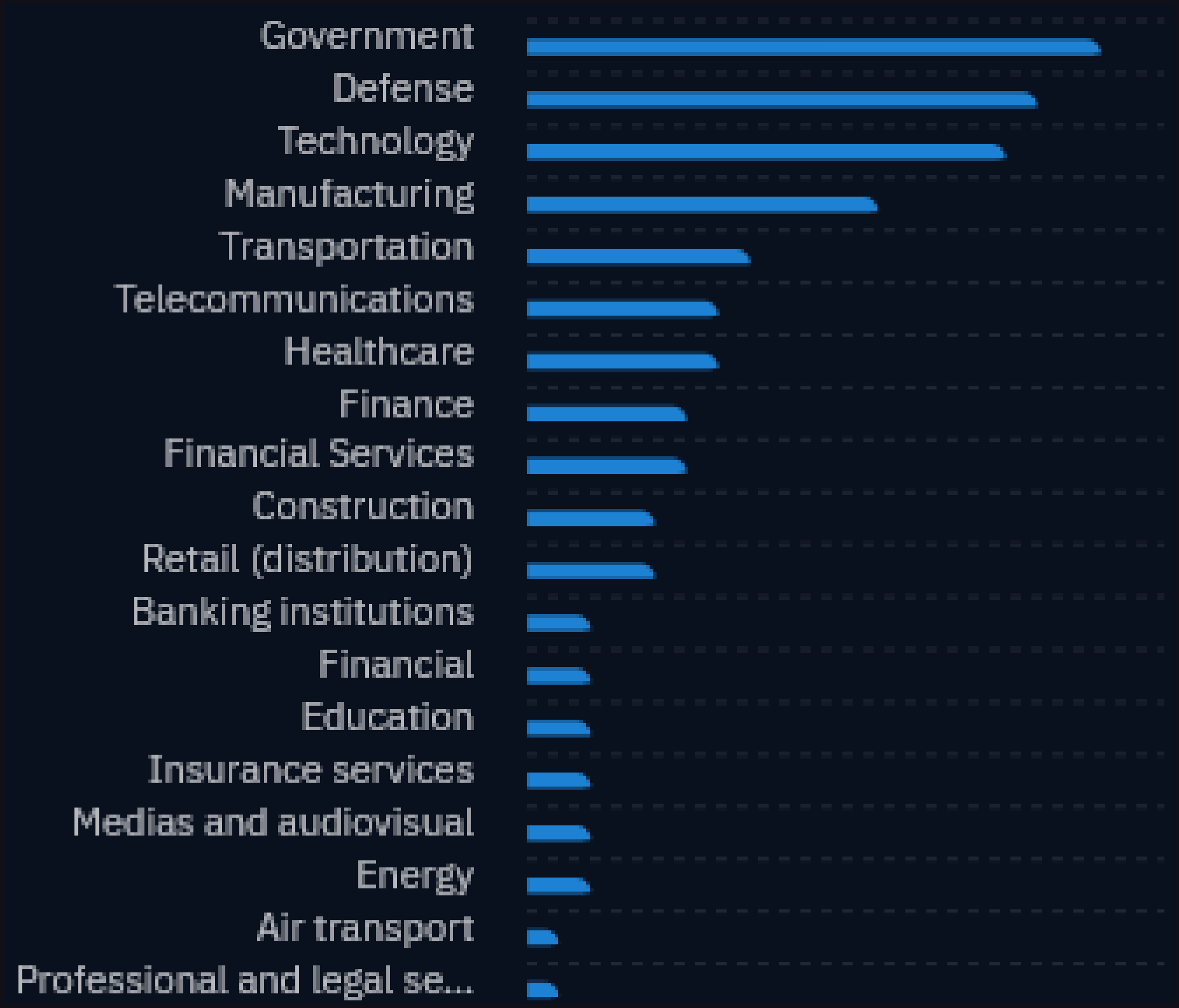
Active TTP: T1027

Active Malware: banking trojan

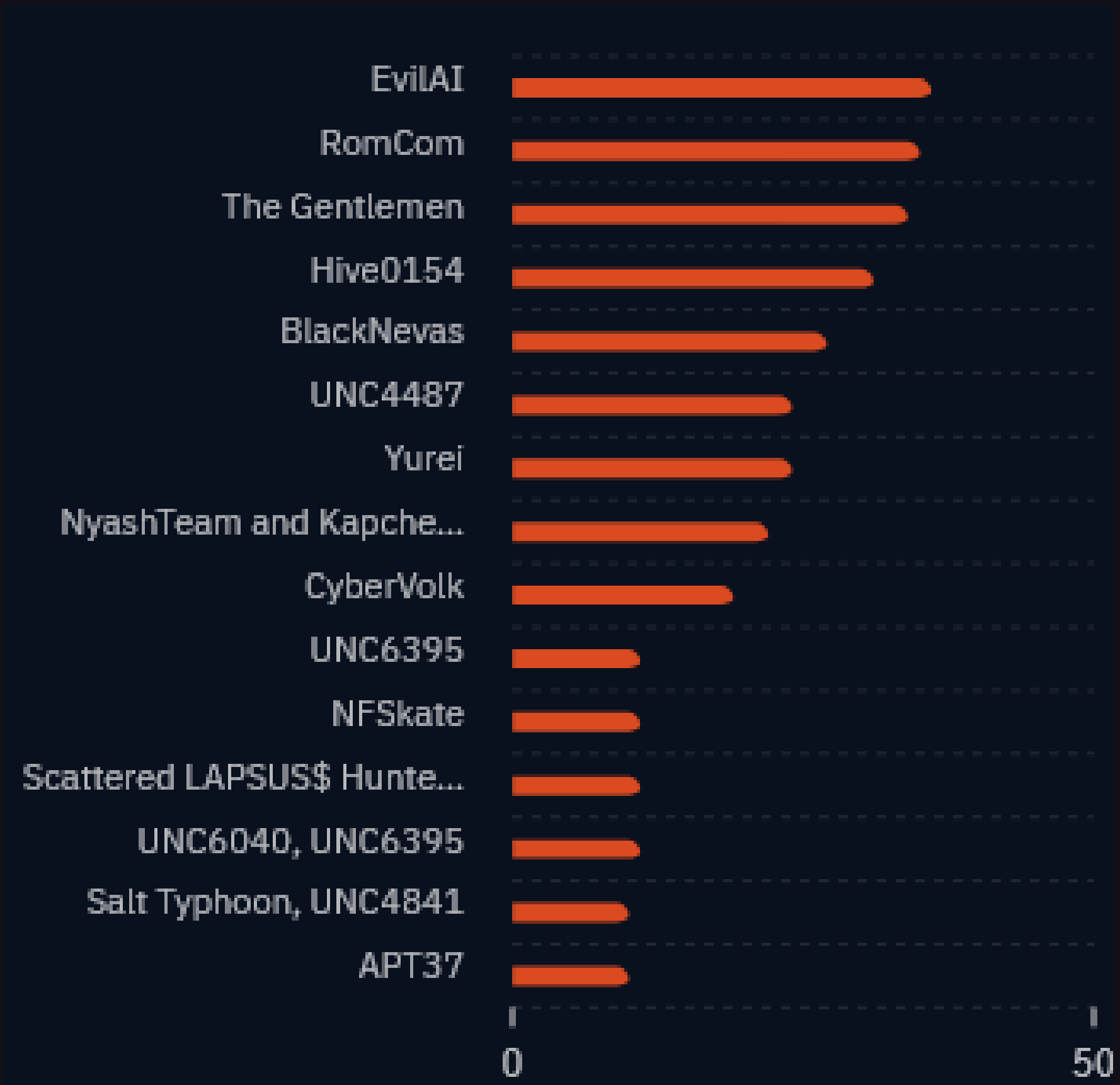
Targeted Countries



Top Targeted Sectors



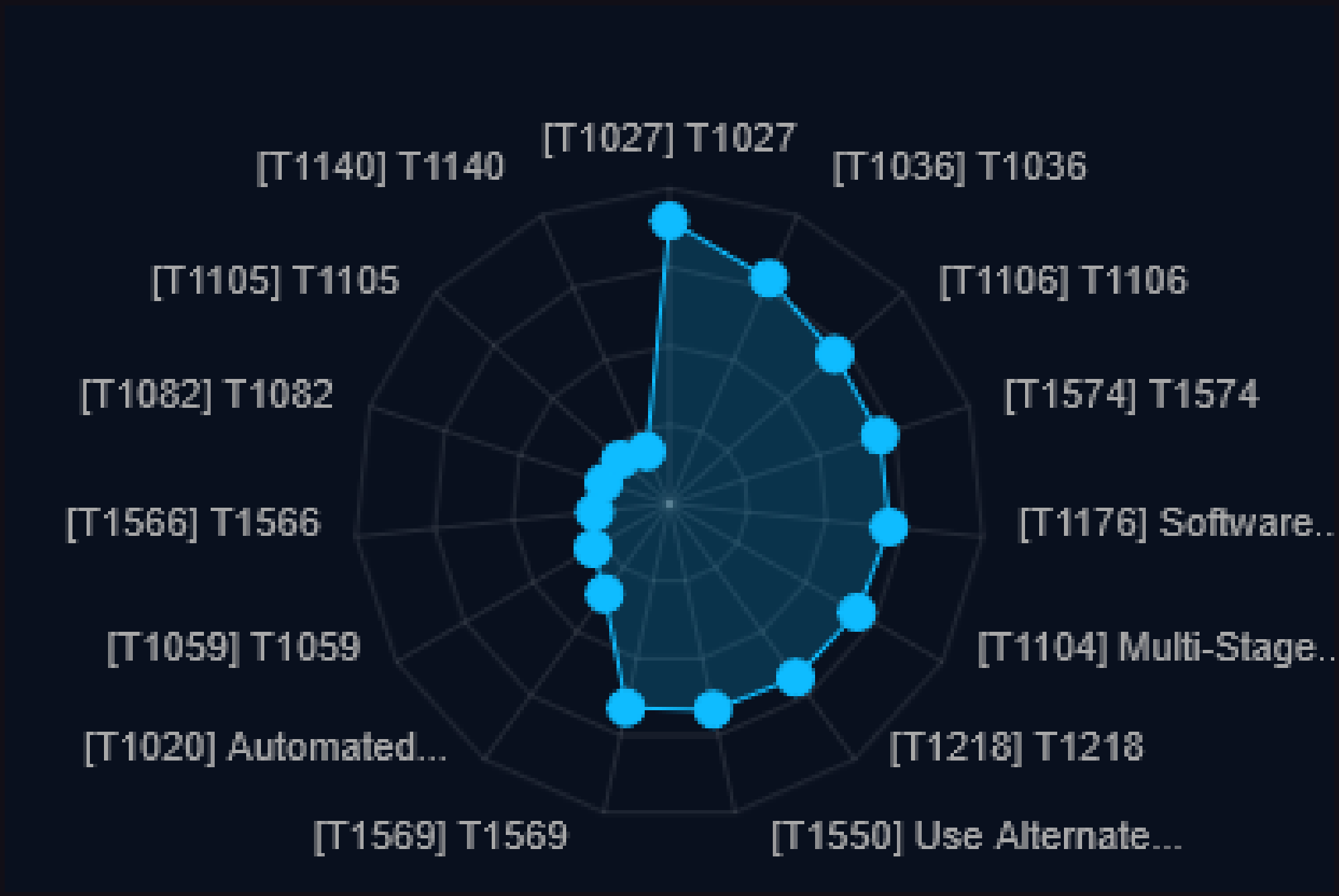
Active Intrusion Sets



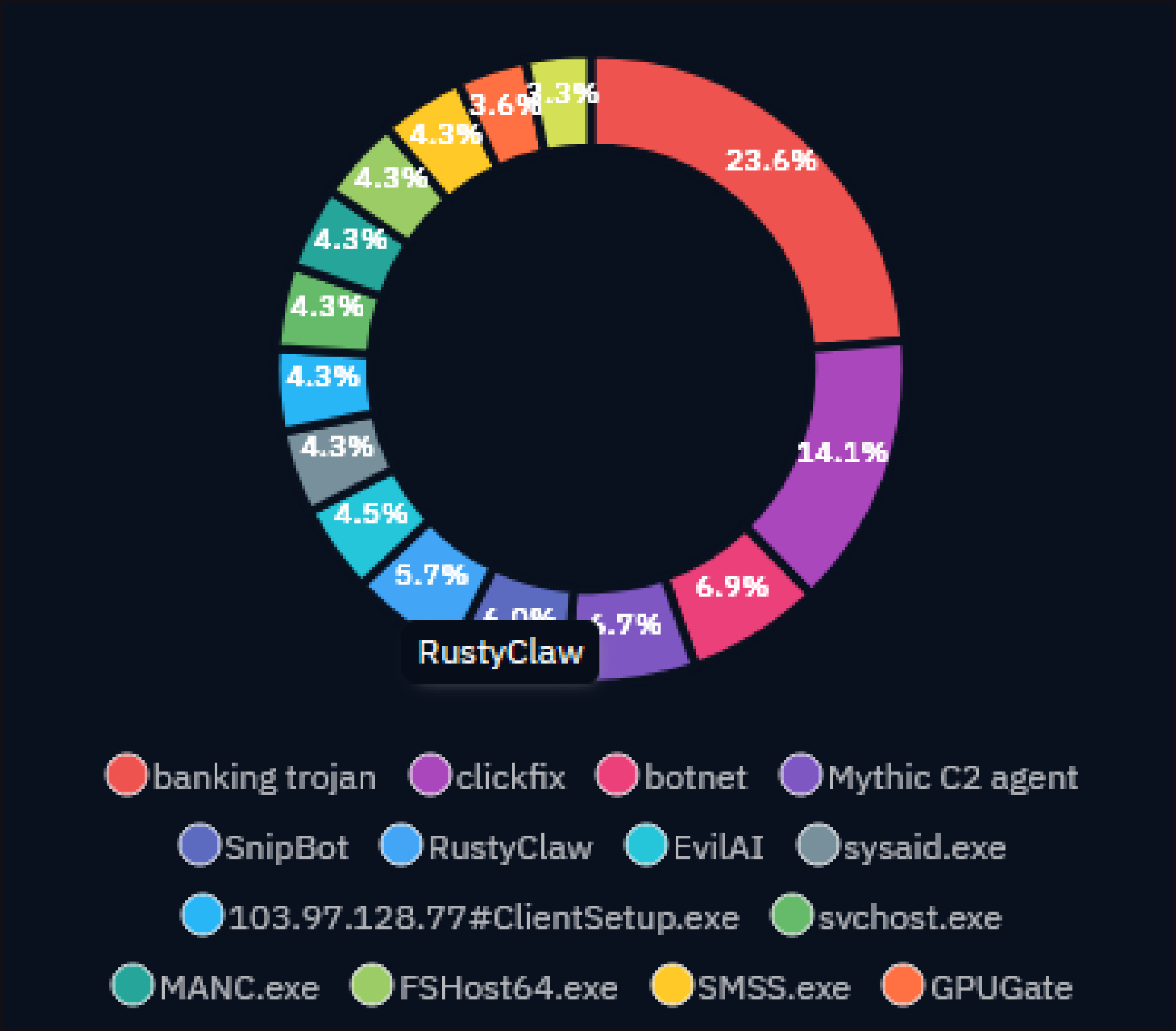
Top Active Vulns

CVE-2025-20265	56
CVE-2025-7775	43
CVE-2025-25256	37
CVE-2025-43300	20
CVE-2020-14993	20
CVE-2025-7776	20
CVE-2025-20281	20

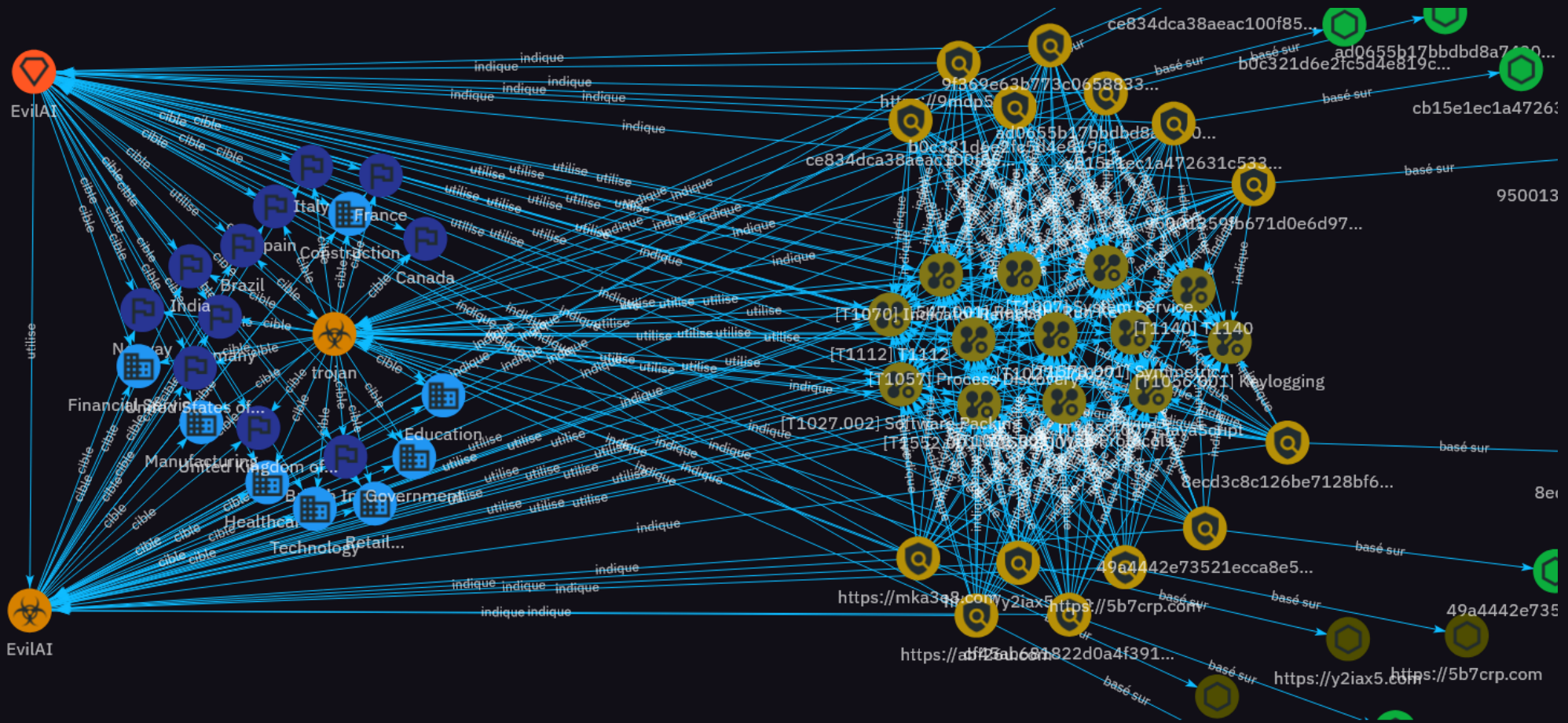
ACTIVE TTPS


[T1027] T1027
[T1140] T1140
[T1036] T1036
[T1105] T1105
[T1106] T1106
[T1082] T1082
[T1574] T1574
[T1566] T1566
[T1176] Software..
[T1059] T1059
[T1104] Multi-Stage..
[T1020] Automated...
[T1218] T1218
[T1569] T1569
[T1550] Use Alternate...

ACTIVE MALWARE



ACTIVITIE OF THREAT : EvilAI



Une nouvelle campagne de malware appelée EvilAI se propage à l'échelle mondiale en se faisant passer pour des outils de productivité légitimes optimisés par l'IA.

Ce malware utilise du code généré par l'IA et des interfaces professionnelles pour échapper à la détection et cible des organisations de secteurs tels que l'industrie manufacturière, le secteur public et la santé. Il exploite Node.js pour exécuter du JavaScript malveillant, établit une persistance via des tâches planifiées et des modifications de registre, et communique avec des serveurs de commande et de contrôle via des canaux chiffrés.

EvilAI répertorie les logiciels installés, interrompt les processus du navigateur et duplique les données d'identification. Il utilise des techniques sophistiquées d'obfuscation et d'anti-analyse pour empêcher la rétro-ingénierie. Le malware agit comme un vecteur d'accès initial, déployant potentiellement des charges utiles supplémentaires. Cette campagne met en évidence la manière dont l'IA est instrumentalisée pour créer des menaces de malwares de plus en plus furtives et adaptatives.

ANNEXE

KILL CHAIN GLOBALE

defense-evasion

T1027 - T1027
Aucune description de cet usage
TLP:CL... Aucun

T1027.002 - Software Packing
Aucune description de cet usage
TLP:CL... Aucun

T1070 - Indicator Removal
Aucune description de cet usage
TLP:CL... Aucun

T1112 - T1112
Aucune description de cet usage
TLP:CL... Aucun

T1140 - T1140
Aucune description de cet usage
TLP:CL... Aucun

command-and-control

T1071.001 - Web Protocols
Aucune description de cet usage
TLP:CL... Aucun

T1573.001 - Symmetric Cryptography
Aucune description de cet usage
TLP:CL... Aucun

discovery

T1057 - Process Discovery
Aucune description de cet usage
TLP:CL... Aucun

T1007 - System Service Discovery
Aucune description de cet usage
TLP:CL... Aucun

persistence

T1547.001 - Registry Run Keys / Startup Folder
Aucune description de cet usage
TLP:CL... Aucun

credential-access

T1552.001 - T1552.001
Aucune description de cet usage
TLP:CL... Aucun

execution

T1059.007 - JavaScript
Aucune description de cet usage
TLP:CL... Aucun

collection

T1056.001 - Keylogging
Aucune description de cet usage
TLP:CL... Aucun

inconnu

EvilAI
Aucune description de cet usage
TLP:CL... Aucun

trojan
Aucune description de cet usage
TLP:CL... Aucun