



DUDIX CTI

Les Nouvelles du Front

S36

9 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: Education

Top Targeted Countries: Canada

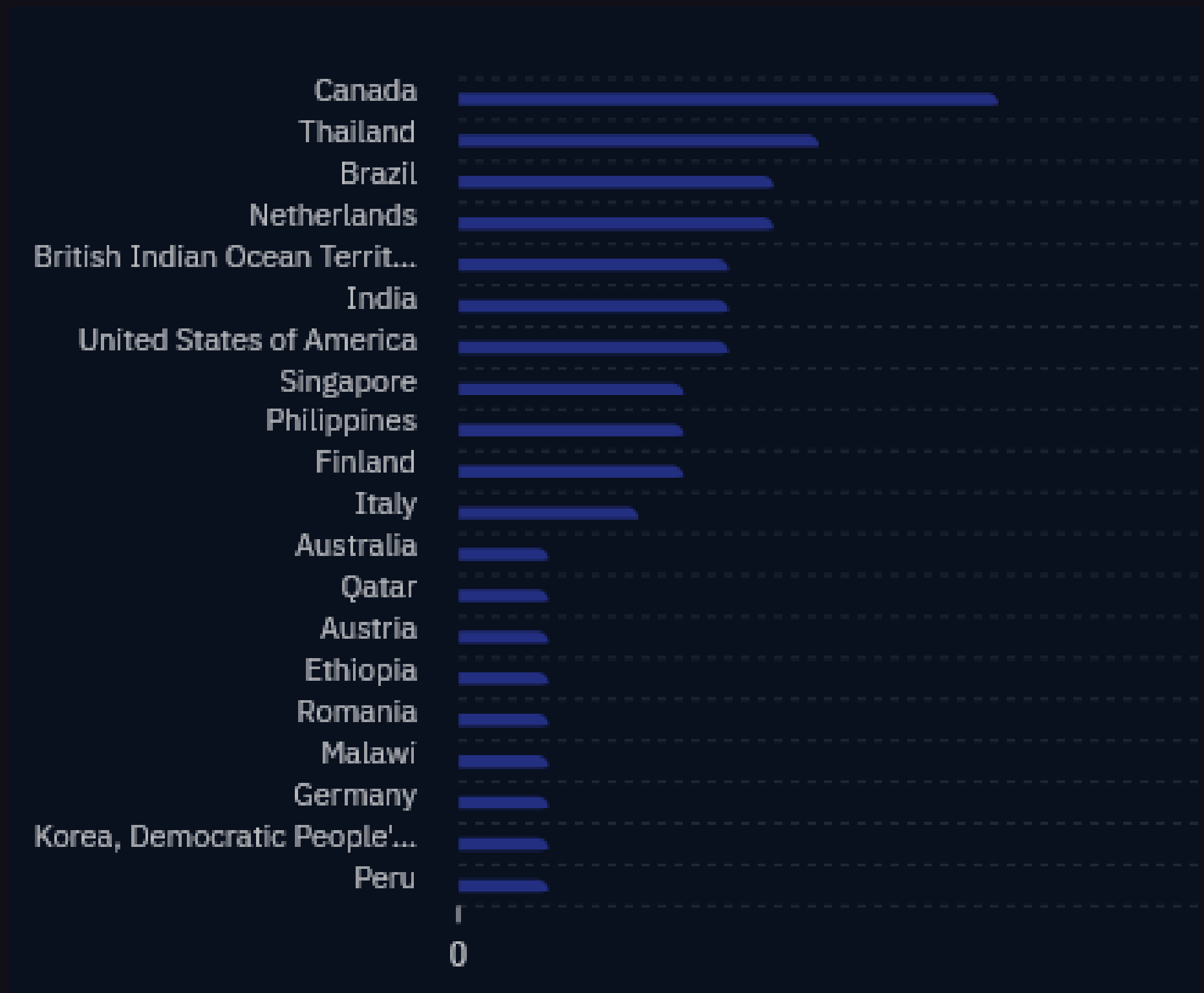
Active Intrusion Set: Homeland Justice

Active Vuln: CVE-2025-53690

Active TTP: T1589, T1584

Active Malware: SysProcUpdate

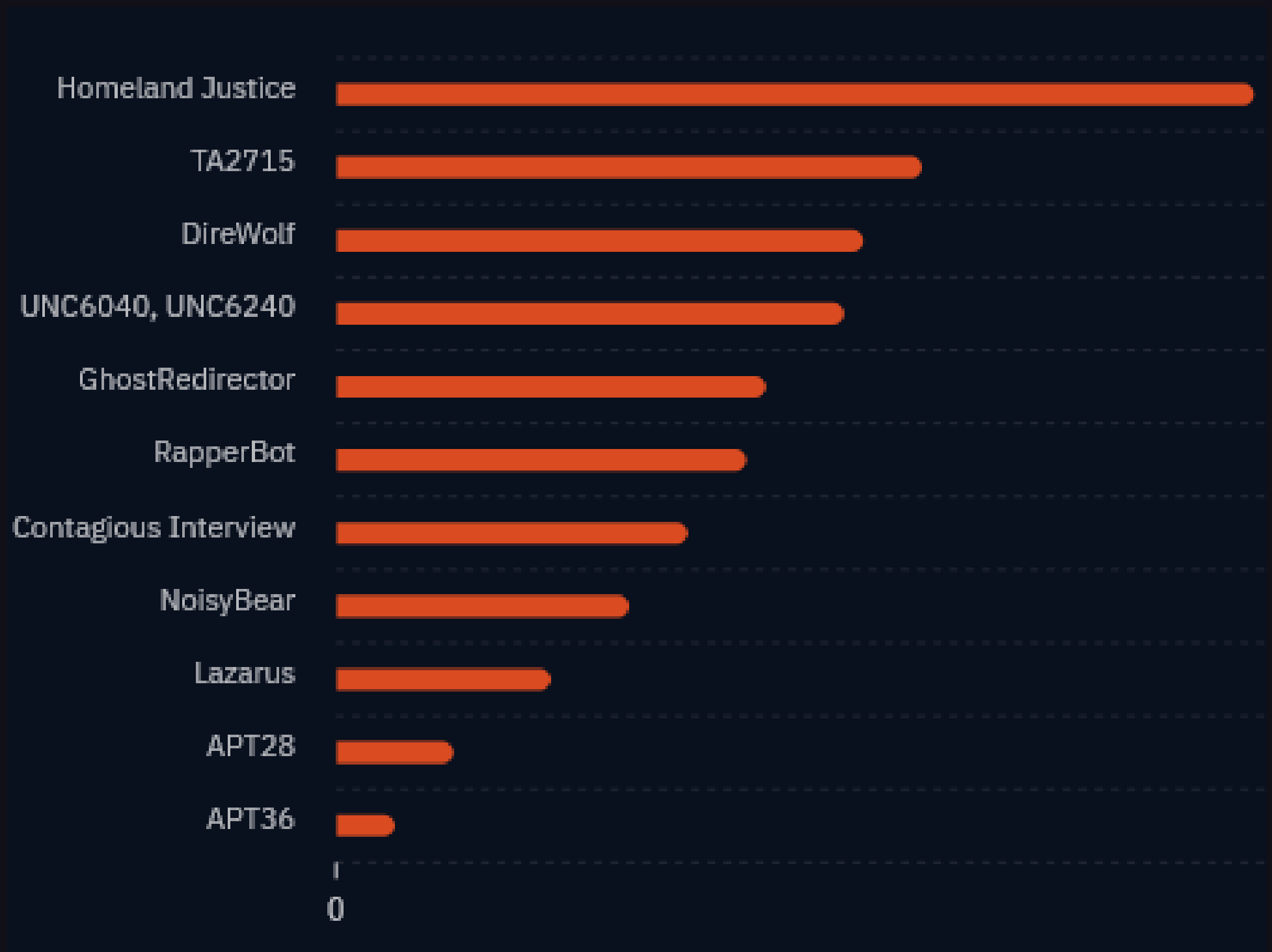
Targeted Countries






Top Targeted Sectors



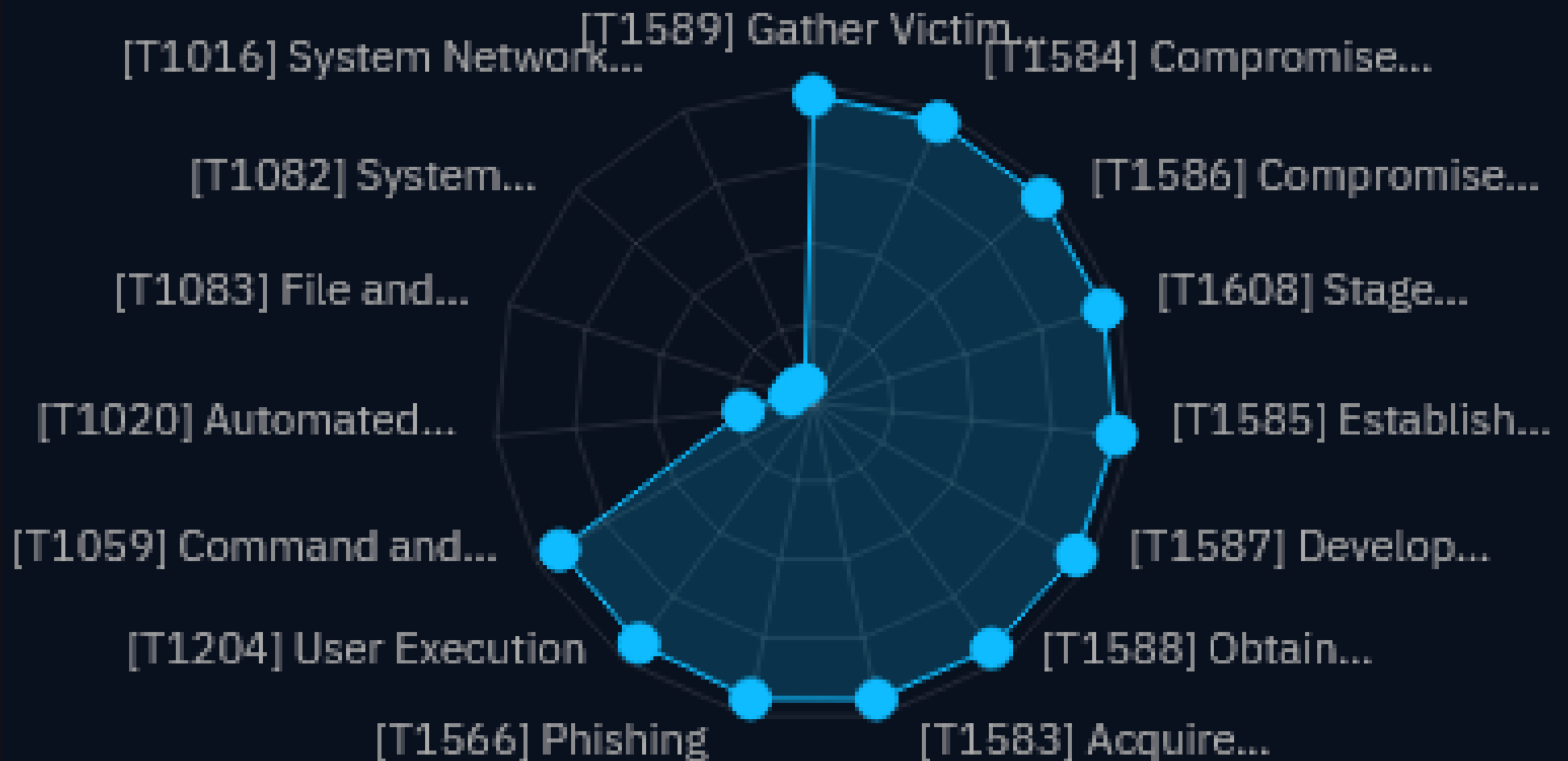
Active Intrusion Sets



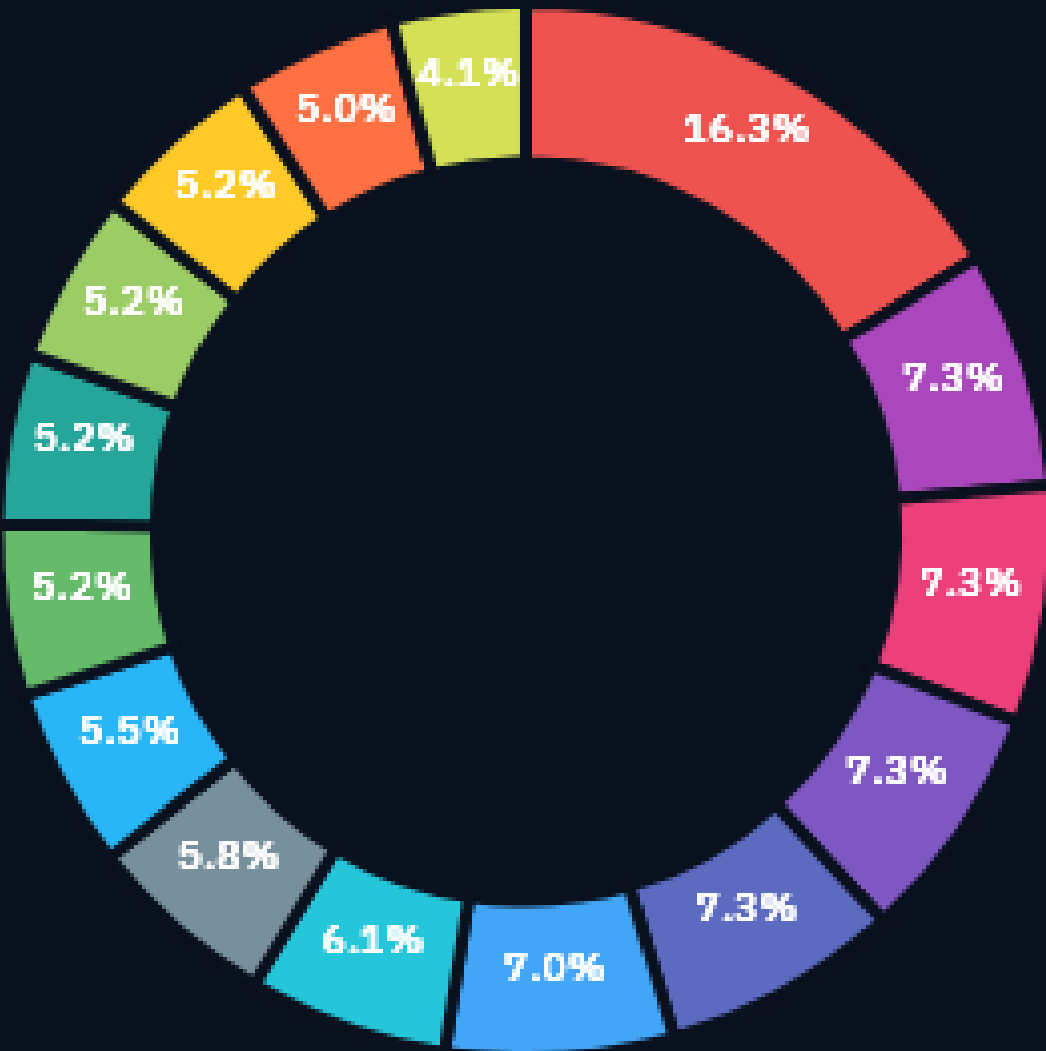
Top Active Vulns

	CVE-2025-53690	21
	CVE-2025-55177	11
	CVE-2023-42793	9

ACTIVE TTPS

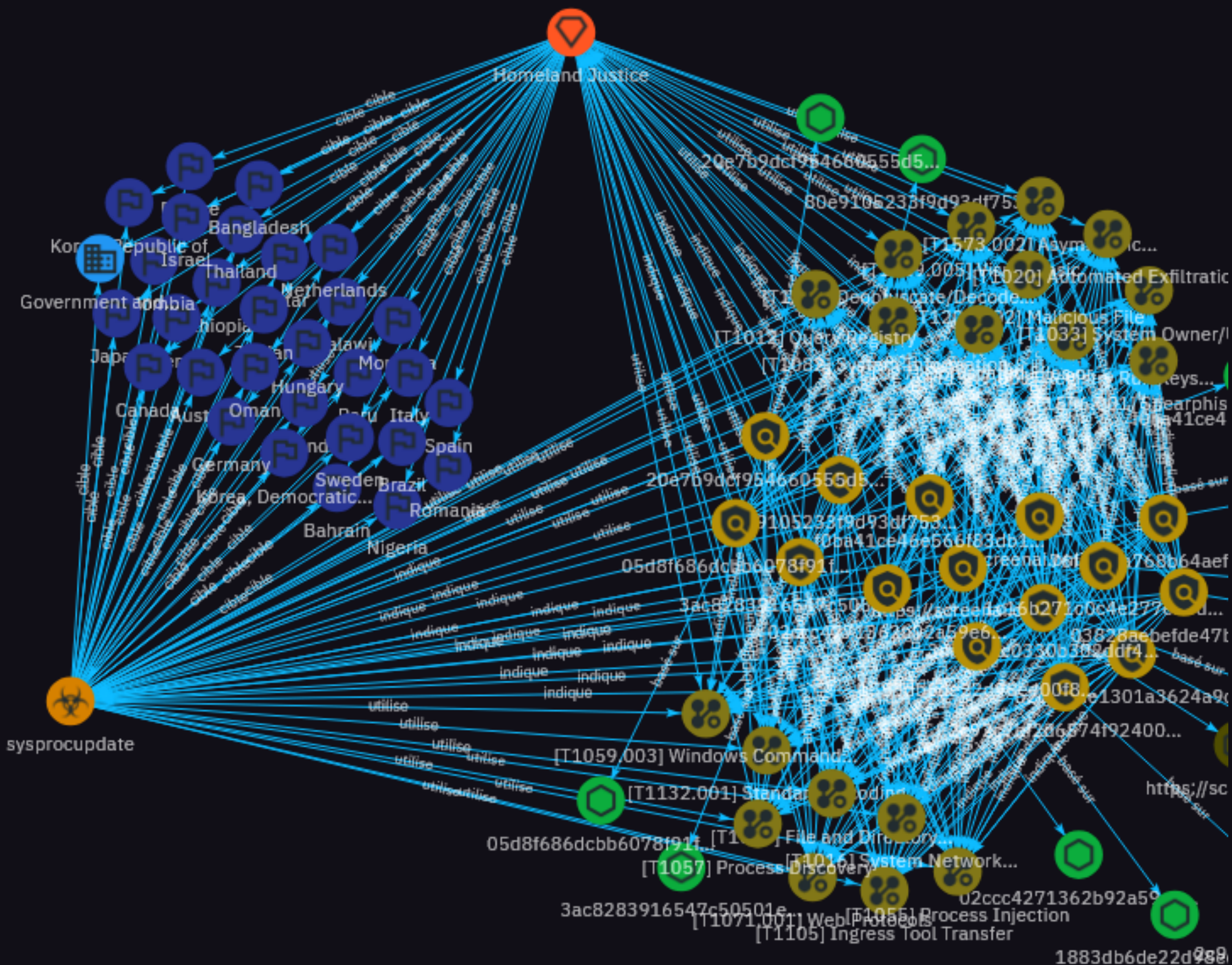


ACTIVE MALWARE

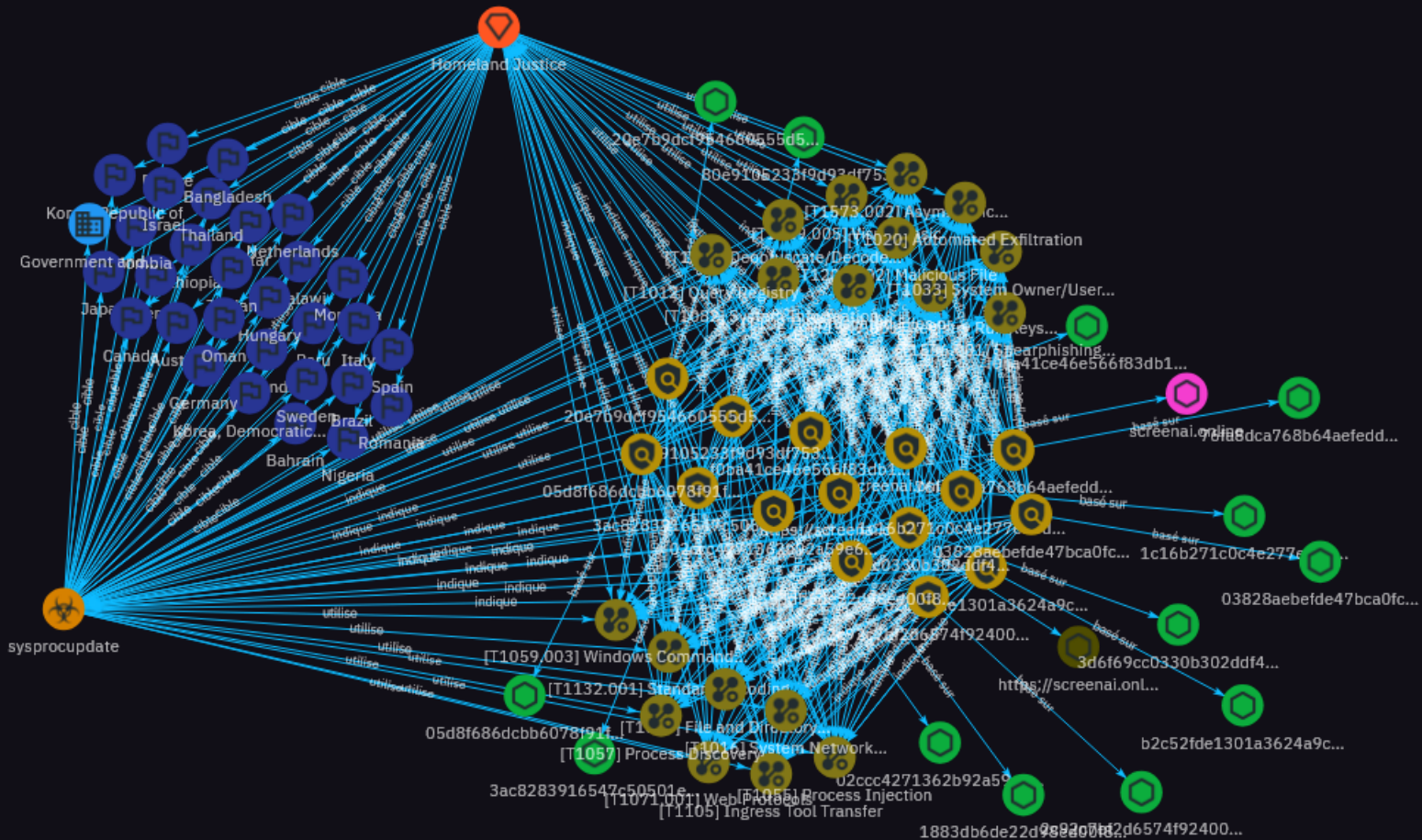


- sysprocupdate
- Info3c Stealer
- Phantom Stealer
- Warp Stealer
- Umbral-Stealer
- pondrat
- Stealerium
- Blank Grabber
- poolrat
- Rungan
- Zunput
- Gamshen
- Comdai
- RapperBot
- Dire Wolf

ACTIVITIE OF THREAT : Homeland Justice



ACTIVITIE OF THREAT : Homeland Justice



La menace cyber « Homeland Justice » désigne un groupe de hackers soutenu par l'État iranien, spécialisé dans les attaques disruptives mêlant ransomware, wipers, et fuite de données sensibles contre des gouvernements et des infrastructures critiques, principalement dans le but politique et géostratégique.

Il est également identifié sous d'autres pseudonymes tels que **Void Manticore** (chez **Check Point**), **Storm-0842** (**Microsoft**) ou encore **Druidfly** dans certaines publications spécialisées.

ORIGINE ET OBJECTIFS:

Homeland Justice est actif depuis mai 2021 et s'est illustré initialement par des attaques contre l'Albanie, notamment en juillet et septembre 2022. Leurs actions visaient spécifiquement les réseaux gouvernementaux albanais et le camp de réfugiés de l'organisation d'opposition iranienne MEK, installé dans ce pays.

ACTIVITE OF THREAT : Homeland Justice

TACTIQUES, TECHNIQUES ET PROCÉDURES (TTP):

Homeland Justice emploie un arsenal avancé, aligné sur le framework MITRE ATT&CK :

- **Accès initial** : exploitation de vulnérabilités critiques (ex. CVE-2019-0604 – SharePoint).
- **Persistence** : déploiement de web shells (pickers.aspx, error4.aspx...).
- **Élévation de privilèges** : usage de Mimikatz pour extraire des identifiants LSASS.
- **Mouvement latéral** : RDP/SMB/FTP.
- **Défense évasion** : désactivation de Windows Defender, suppression de logs.
- **Impact** : wipers et ransomwares entraînant une destruction irréversible des systèmes.

ACTIVITE OF THREAT : **Homeland Justice**

VICTIMES ET IMPACTS:

Les attaques visent des états et des infrastructures critiques, souvent dans des contextes de tensions géopolitiques, avec une portée grandissante vers l'Europe, l'Amérique du Nord et l'Asie-Pacifique. Les motivations sont idéologiques/politiques et répondent à des enjeux liés à l'opposition iranienne ou à la rivalité avec des états occidentaux ou régionaux.

ACTUALITÉ ET ÉVOLUTION:






































Depuis 2022, Homeland Justice multiplie les menaces et les revendications offensives sur des canaux publics comme Telegram, et de nouvelles vagues d'attaques sont observées en 2025 contre diverses cibles, en lien avec la montée des tensions au Moyen-Orient. Les experts conseillent de renforcer les défenses, notamment dans les secteurs énergie, télécom, finances et infrastructures publiques.

Homeland Justice s'impose comme un acteur cyber offensif majeur du paysage iranien, incarnant la mutation des APT en véritables armes de guerre numérique. Les campagnes de 2022 et 2025 démontrent la vulnérabilité des services publics face à des attaques étatiques coordonnées.

Au-delà des enjeux de détection technique, il s'agit de renforcer la résilience nationale ; redondance des systèmes, sauvegardes robustes, plan de continuité – et d'intégrer la cybersécurité comme un enjeu géopolitique stratégique.

ANNEXE

KILL CHAIN GLOBALE

	command-and-control		
	T1105 - Ingress Tool Transfer Aucune description de cet usage	TLP:CL...	Aucun
	T1071.001 - Web Protocols Aucune description de cet usage	TLP:CL...	Aucun
	T1573.002 - Asymmetric Cryptography Aucune description de cet usage	TLP:CL...	Aucun
	T1132.001 - Standard Encoding Aucune description de cet usage	TLP:CL...	Aucun
	execution		
	T1059.005 - Visual Basic Aucune description de cet usage	TLP:CL...	Aucun
	T1059.003 - Windows Command Shell Aucune description de cet usage	TLP:CL...	Aucun
	T1204.002 - Malicious File Aucune description de cet usage	TLP:CL...	Aucun
	T1059 - Command and Scripting Interpreter Aucune description de cet usage	TLP:CL...	Aucun
	discovery		
	T1012 - Query Registry Aucune description de cet usage	TLP:CL...	Aucun
	T1083 - File and Directory Discovery Aucune description de cet usage	TLP:CL...	Aucun
	T1057 - Process Discovery Aucune description de cet usage	TLP:CL...	Aucun
	T1016 - System Network Configuration Discovery Aucune description de cet usage	TLP:CL...	Aucun
	T1082 - System Information Discovery Aucune description de cet usage	TLP:CL...	Aucun
	T1033 - System Owner/User 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
	T1176 - Software Extensions Aucune description de cet usage	TLP:CL...	Aucun
	T1547 - Boot or Logon Autostart Execution Aucune description de cet usage	TLP:CL...	Aucun
	exfiltration		
	T1020 - Automated Exfiltration Aucune description de cet usage	TLP:CL...	Aucun
	defense-evasion		
	T1055 - Process Injection Aucune description de cet usage	TLP:CL...	Aucun
	T1027 - Obfuscated Files or Information Aucune description de cet usage	TLP:CL...	Aucun
	T1562 - Impair Defenses Aucune description de cet usage	TLP:CL...	Aucun
	T1140 - Deobfuscate/Decode Files or Information Aucune description de cet usage	TLP:CL...	Aucun
	initial-access		
	T1566.001 - Spearphishing Attachment Aucune description de cet usage	TLP:CL...	Aucun
	lateral-movement		
	T1021 - Remote Services Aucune description de cet usage	TLP:CL...	Aucun
	impact		
	T1486 - Data Encrypted for Impact Aucune description de cet usage	TLP:CL...	Aucun
	inconnu		
	sysprocupdate Aucune description de cet usage	TLP:CL...	Aucun
	ransomware Aucune description de cet usage	TLP:CL...	Aucun
	webshell Aucune description de cet usage	TLP:CL...	Aucun
	Wiper Aucune description de cet usage	TLP:CL...	Aucun