



# Les Nouvelles du Front

# DUDIX CTI

Semaine 33

19 août 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**

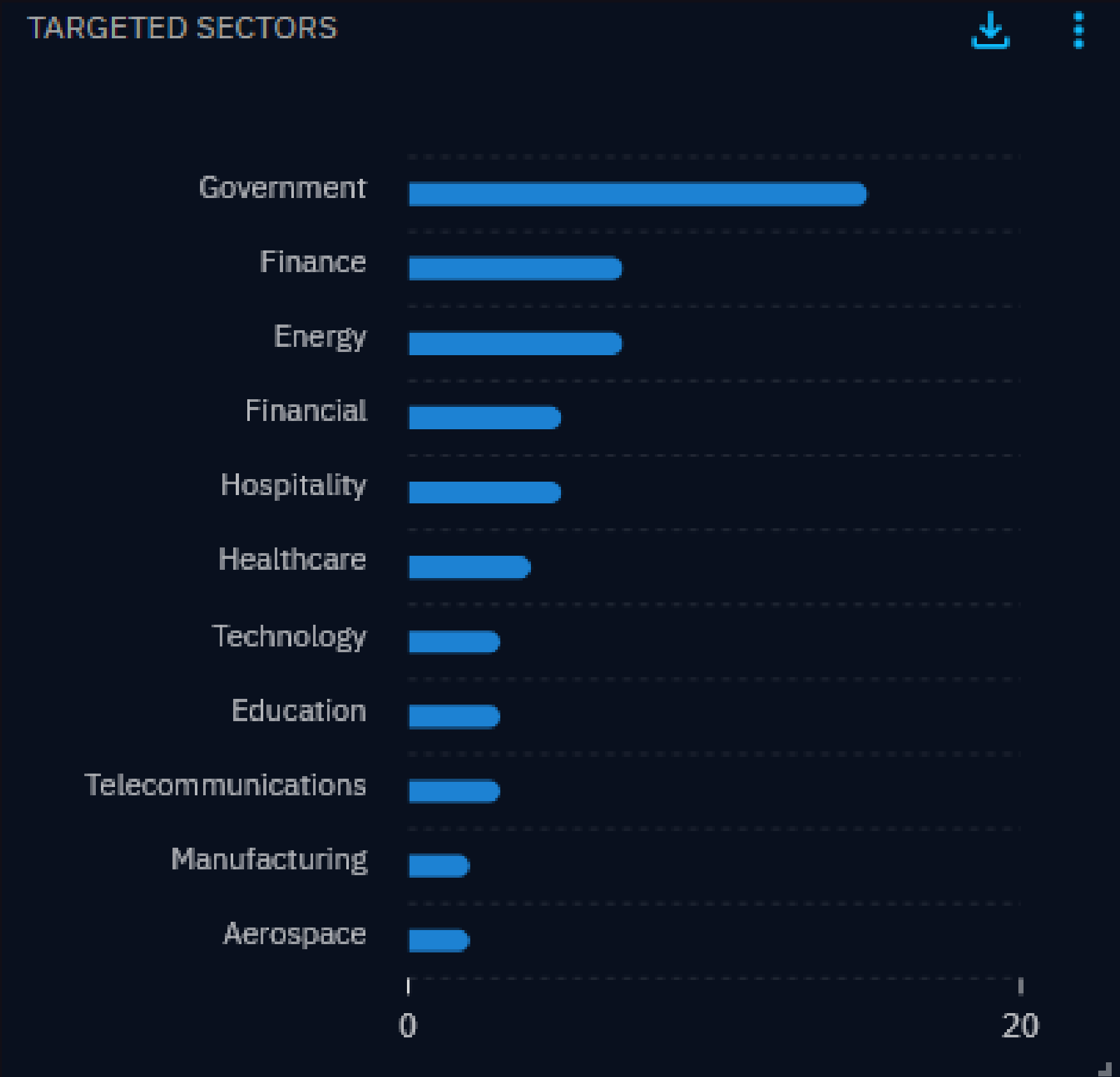
**Active Intrusion Set: ERMAC, Curly  
COMrades**

**Active Vuln: CVE-2025-6543**

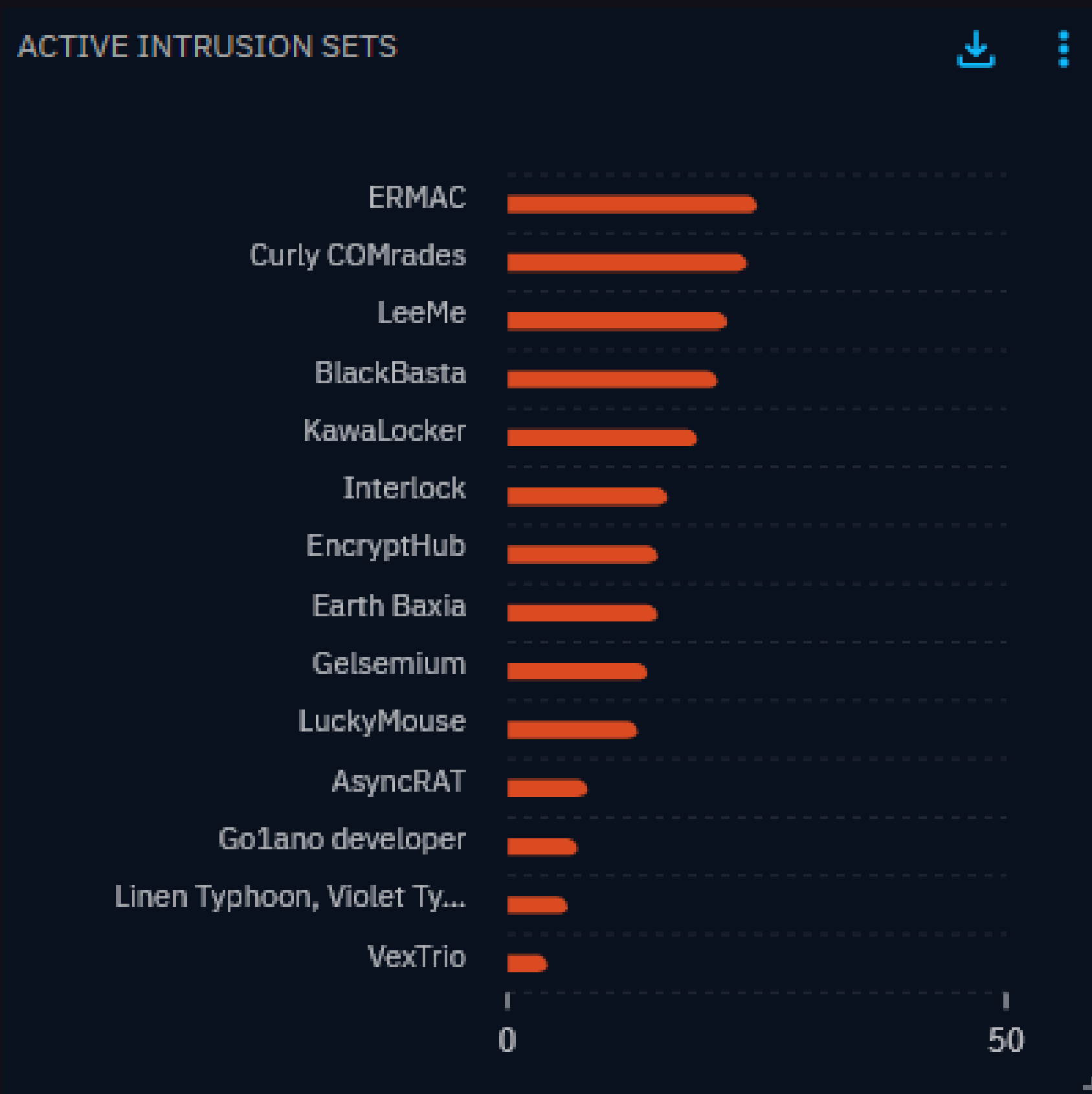
**Active TTP: T1020**

**Active Malware: PS1bot**








# Top Targeted Sectors



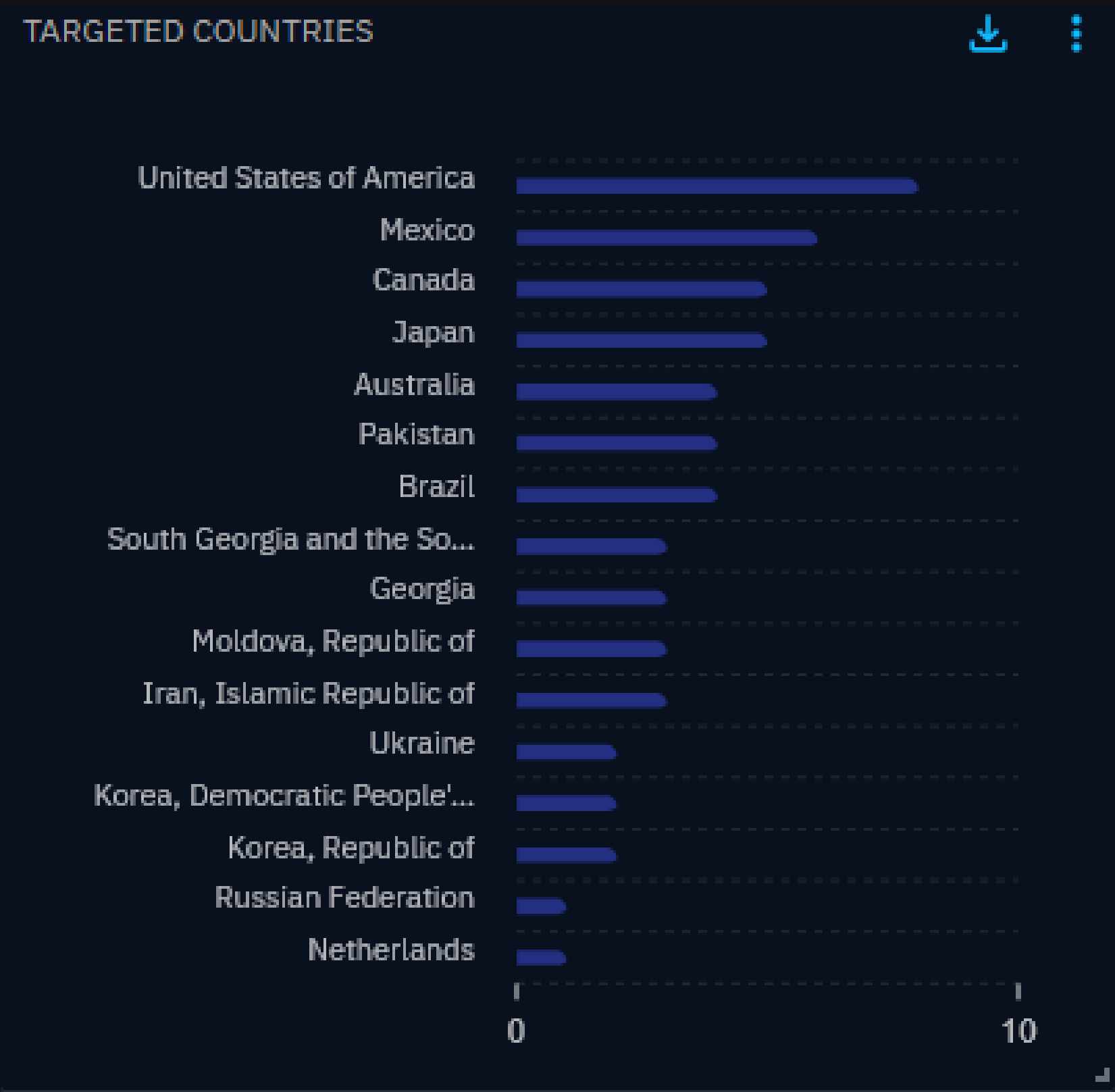
# Active Intrusion Sets



# Top Active Vulns

ACTIVE VULNERABILITIES			⋮
	CVE-2025-6543	20	
	CVE-2025-26633	8	
	CVE-2025-49706	5	
	CVE-2025-49704	5	
	CVE-2025-53771	5	
	CVE-2025-53770	4	
	CVE-2017-11882	1	

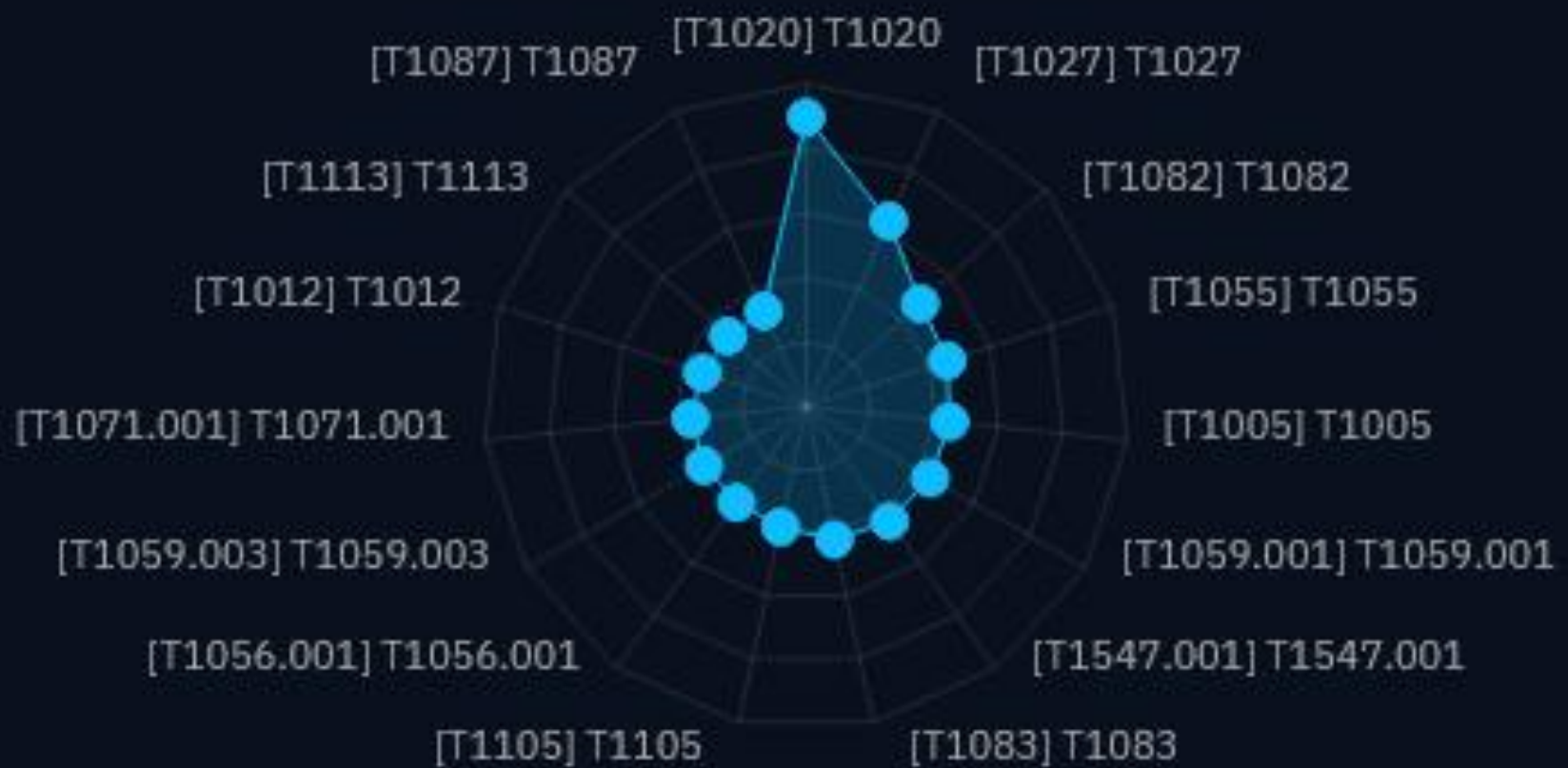
# Targeted Countries



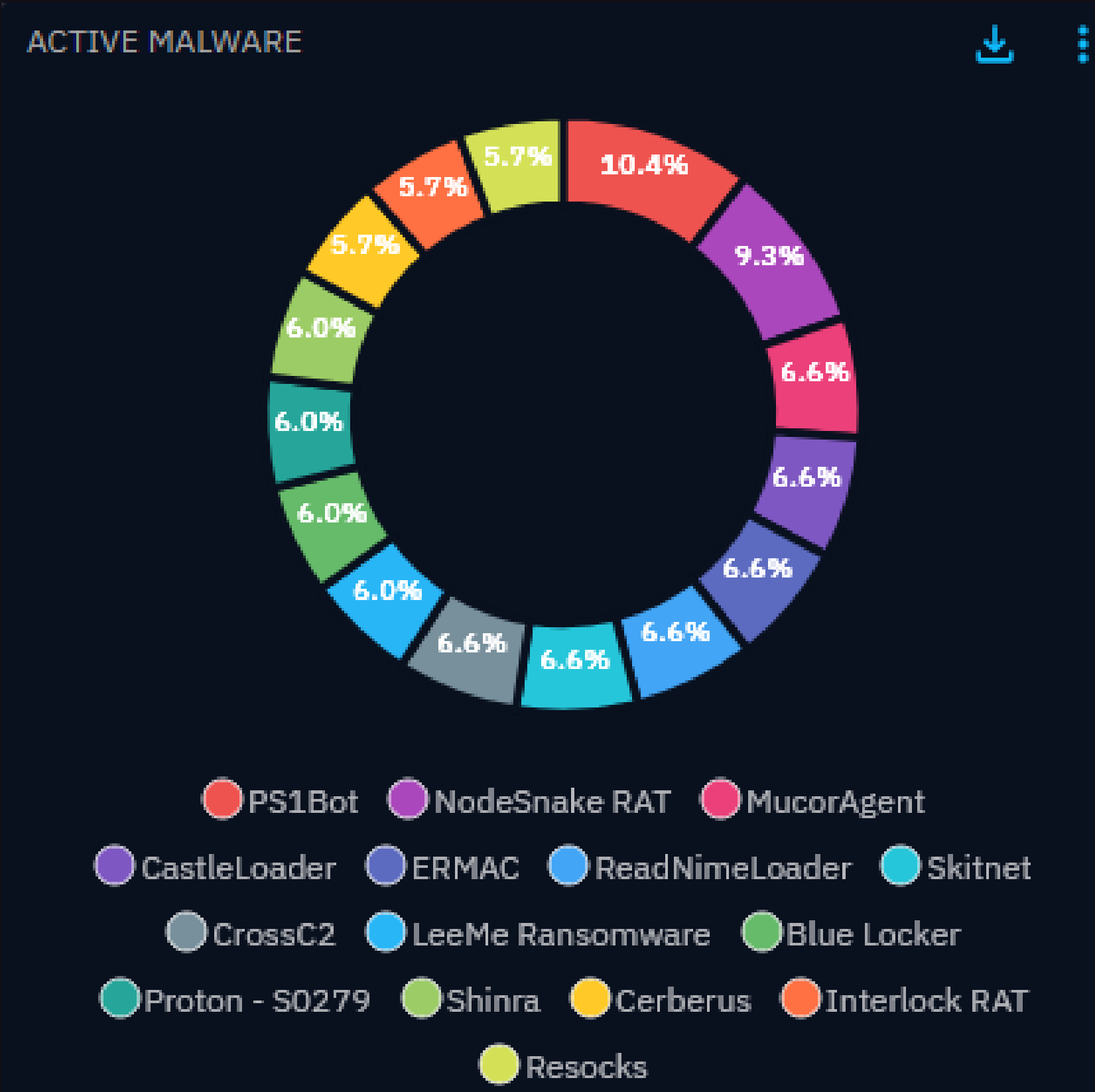


# ACTIVE TTPS

ACTIVE TTPS

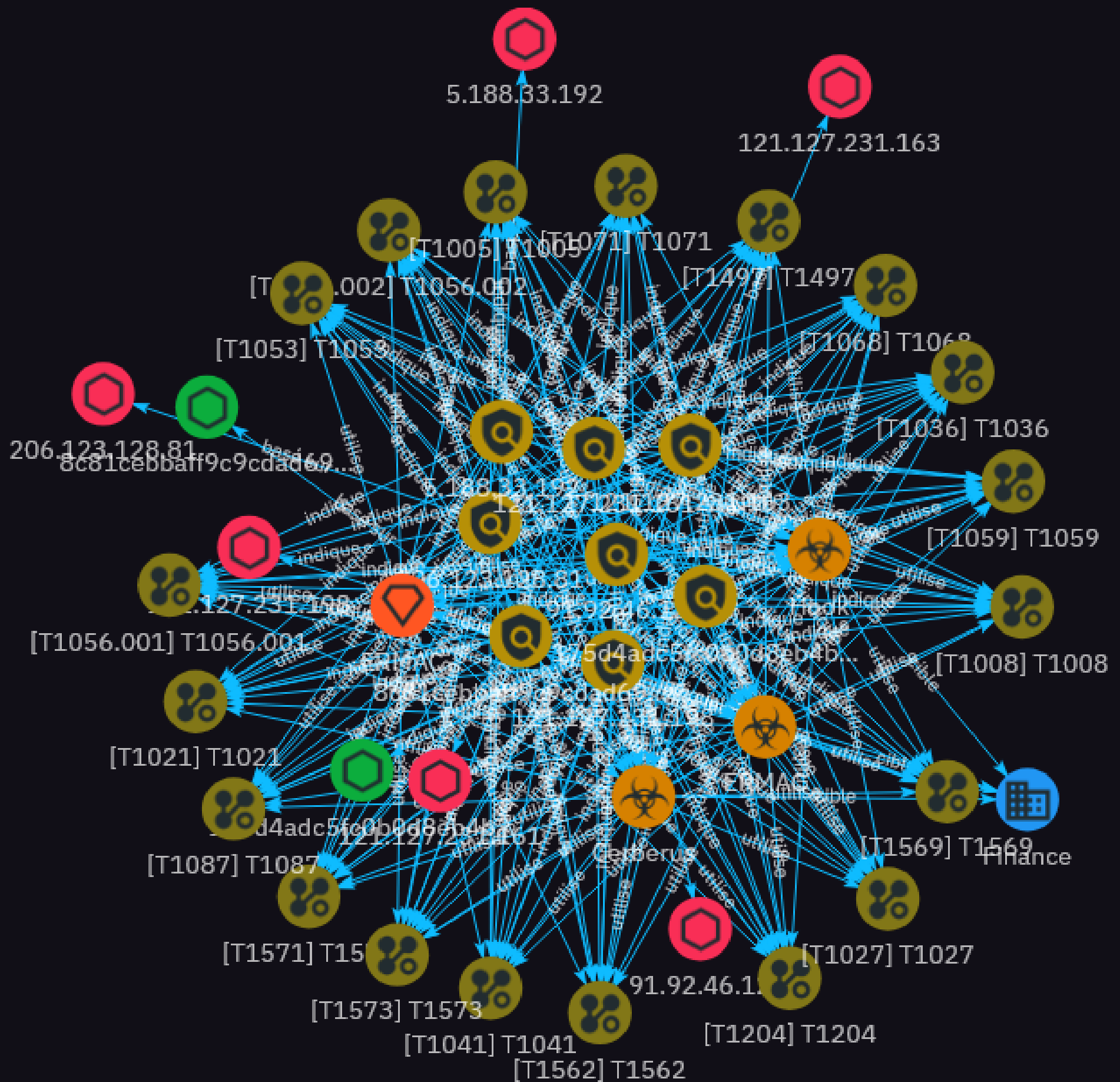


# ACTIVE MALWARE





## ACTIVITIE OF THREAT : ERMAC



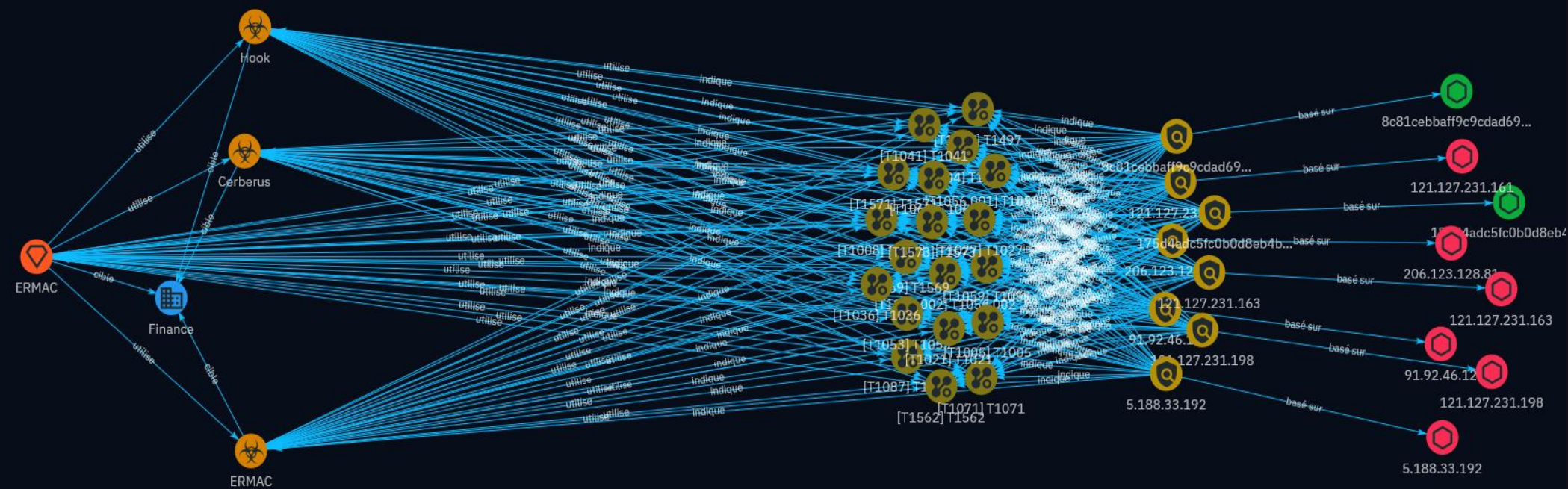
# ACTIVITIE OF THREAT : ERMAC

## ERMAC V3.0 Banking Trojan: Full Source Code Leak and Infrastructure Analysis

APERÇU CONNAISSANCE CONTENU ENTITÉS OBSERVABLES DONNÉES

MODIFIER

3




































3D

Rechercher ces résultats

+

# ACTIVITIE OF THREAT : ERMAC Global Kill Chain

	command-and-control				^
	<b>T1008</b> - T1008 Aucune description de cet usage	<div>TLP:CLEAR</div>	<div>Aucun</div>	<div></div>	
	<b>T1573</b> - T1573 Aucune description de cet usage	<div>TLP:CLEAR</div>	<div>Aucun</div>	<div></div>	
	<b>T1571</b> - T1571 Aucune description de cet usage	<div>TLP:CLEAR</div>	<div>Aucun</div>	<div></div>	
	<b>T1071</b> - T1071 Aucune description de cet usage	<div>TLP:CLEAR</div>	<div>Aucun</div>	<div></div>	
	execution				^
	<b>T1569</b> - T1569 Aucune description de cet usage	<div>TLP:CLEAR</div>	<div>Aucun</div>	<div></div>	
	<b>T1204</b> - T1204 Aucune description de cet usage	<div>TLP:CLEAR</div>	<div>Aucun</div>	<div></div>	
	<b>T1059</b> - T1059 Aucune description de cet usage	<div>TLP:CLEAR</div>	<div>Aucun</div>	<div></div>	
	<b>T1053</b> - T1053 Aucune description de cet usage	<div>TLP:CLEAR</div>	<div>Aucun</div>	<div></div>	
	privilege-escalation				^
	<b>T1068</b> - T1068 Aucune description de cet usage	<div>TLP:CLEAR</div>	<div>Aucun</div>	<div></div>	
	defense-evasion				^
	<b>T1027</b> - T1027 Aucune description de cet usage	<div>TLP:CLEAR</div>	<div>Aucun</div>	<div></div>	
	<b>T1497</b> - T1497 Aucune description de cet usage	<div>TLP:CLEAR</div>	<div>Aucun</div>	<div></div>	
	<b>T1036</b> - T1036 Aucune description de cet usage	<div>TLP:CLEAR</div>	<div>Aucun</div>	<div></div>	
	<b>T1562</b> - T1562 Aucune description de cet usage	<div>TLP:CLEAR</div>	<div>Aucun</div>	<div></div>	
	collection				^
	<b>T1056.002</b> - T1056.002 Aucune description de cet usage	<div>TLP:CLEAR</div>	<div>Aucun</div>	<div></div>	
	<b>T1005</b> - T1005 Aucune description de cet usage	<div>TLP:CLEAR</div>	<div>Aucun</div>	<div></div>	
	<b>T1056.001</b> - T1056.001 Aucune description de cet usage	<div>TLP:CLEAR</div>	<div>Aucun</div>	<div></div>	
	exfiltration				^
	<b>T1041</b> - T1041 Aucune description de cet usage	<div>TLP:CLEAR</div>	<div>Aucun</div>	<div></div>	
	discovery				^
	<b>T1087</b> - T1087 Aucune description de cet usage	<div>TLP:CLEAR</div>	<div>Aucun</div>	<div></div>	
	lateral-movement				^
	<b>T1021</b> - T1021 Aucune description de cet usage	<div>TLP:CLEAR</div>	<div>Aucun</div>	<div></div>	
	lateral-movement				↗
	<b>T1021</b> - T1021 Aucune description de cet usage	<div>TLP:CLEAR</div>	<div>Aucun</div>	<div></div>	
	inconnu				↗
	Hook Aucune description de cet usage	<div>TLP:CLEAR</div>	<div>Aucun</div>	<div></div>	
	Cerberus Aucune description de cet usage	<div>TLP:CLEAR</div>	<div>Aucun</div>	<div></div>	
	ERMAC Aucune description de cet usage	<div>TLP:CLEAR</div>	<div>Aucun</div>	<div></div>	

# ACTIVITE OF THREAT :

## ERMAC

Le code source complet d'ERMAC V3.0, un trojan bancaire distribué en Malware-as-a-Service (MaaS), a été récemment découvert et soumis à une analyse approfondie. Cette opportunité fournit une visibilité exceptionnelle sur les mécanismes internes d'une plateforme criminelle encore active. ERMAC présente une capacité de ciblage étendue, couvrant plus de 700 applications financières et liées aux cryptomonnaies.

Ses fonctionnalités incluent notamment :

- Injection de formulaires afin de dérober des identifiants,
- Canaux de communication chiffrés pour l'exfiltration et le pilotage à distance.

L'évaluation du code a mis en évidence plusieurs faiblesses structurelles exploitables par les défenseurs :

- Présence d'identifiants codés en dur,
- Utilisation de tokens par défaut dans la gestion des accès.

Sur le plan infrastructurel, ERMAC repose sur une architecture modulaire :

- Backend C2 développé sous Laravel,
- Interface d'administration en React,
- Service d'exfiltration en Golang,
- Implant Android fortement obfusqué servant de vecteur d'infection.

Cette analyse met en évidence les risques opérationnels associés au modèle MaaS, en soulignant la fragilité de l'écosystème criminel face à une exploitation ciblée de ses vulnérabilités. Elle fournit également aux équipes de défense des axes concrets de détection, de suivi et de perturbation des campagnes liées à ERMAC.