WWW.DUDIX-CONSULTING.FR

DUDIX Consulting

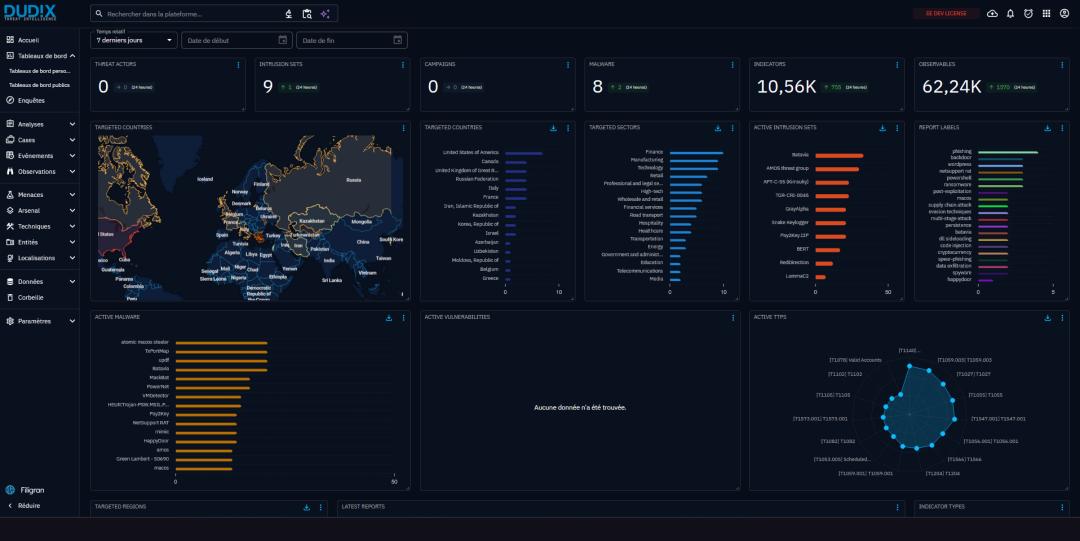


Les Nouvelles du Front

DUDIX CTI

Semaine 28 14 Juillet 2025

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



TOP THREAT

Targeted Sector: Finance

Top Targeted Countrie: USA

Active Intrusion Set: Batavia

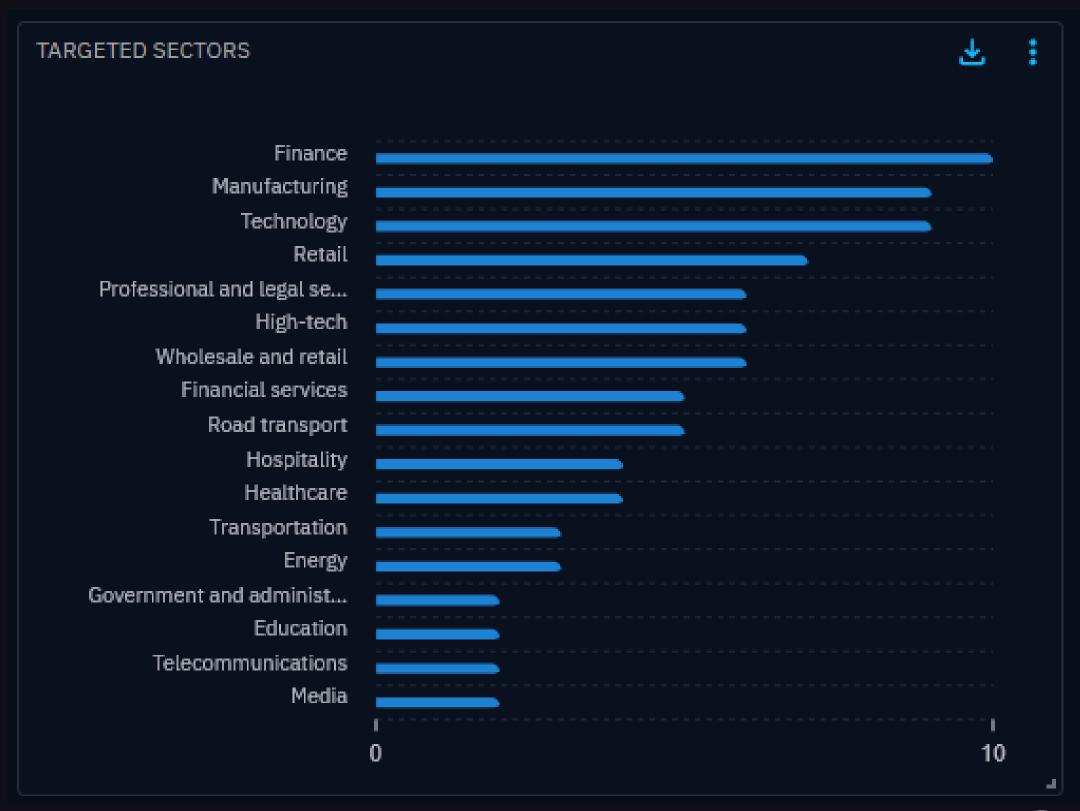
Active Vuln: CVE-2024-8190

Active TTP: T1140

Active Malware: Batavia



Top Targeted Sectors





Active Intrusion Sets



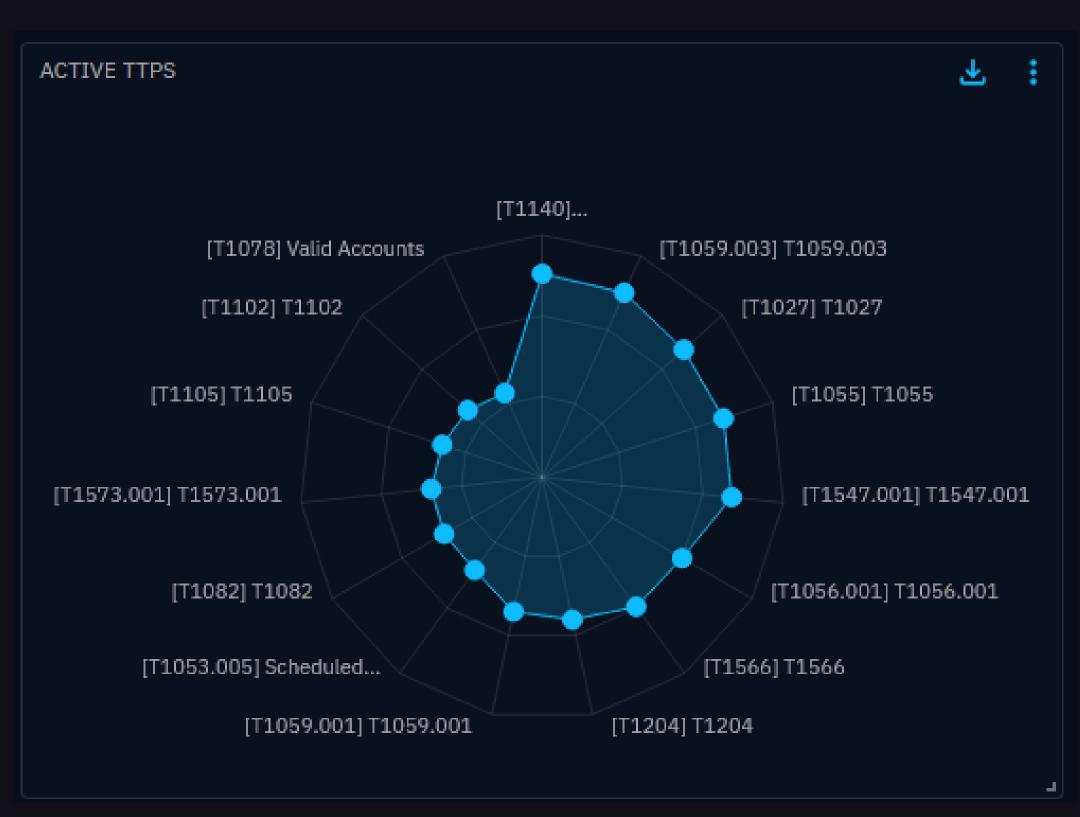


Targeted Countries



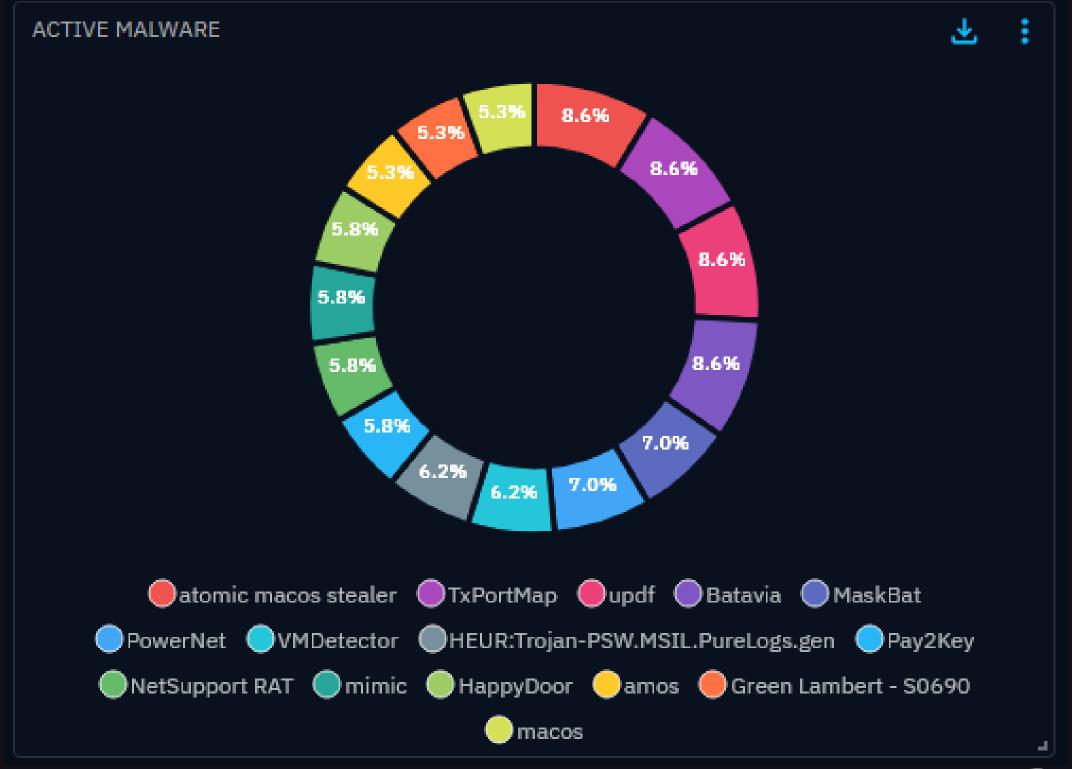


ACTIVE TIPS



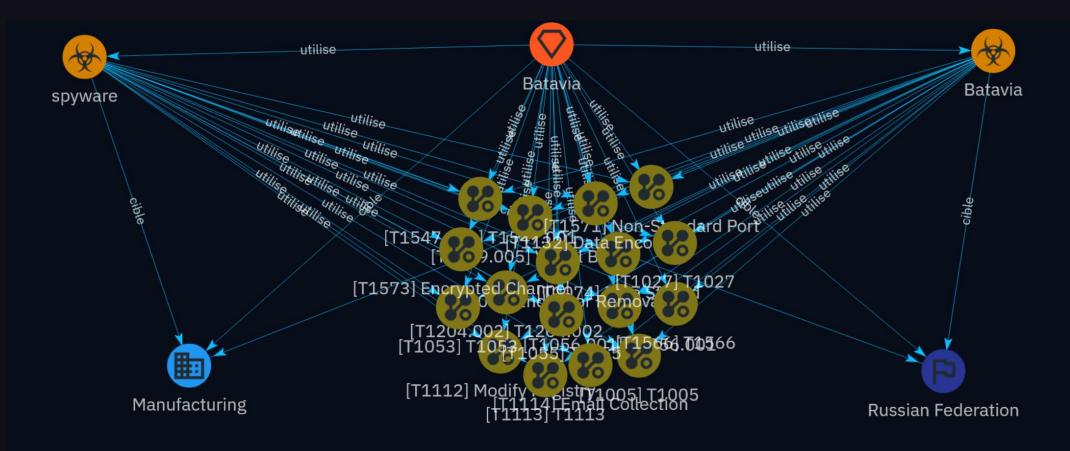


ACTIVE MALWARE





ACTIVITIE OF THREAT: BATAVIA



Batavia est un logiciel espion qui cible des entreprises industrielles russes depuis juillet 2024 par le biais d'une opération de phishing sophistiquée. La campagne utilise des e-mails appâts déguisés en contrats pour inciter les employés à télécharger des scripts malveillants, déclenchant ainsi un processus d'infection en plusieurs étapes.

L'objectif ultime du logiciel espion est d'exfiltrer des documents internes sensibles et des données système. L'attaque comprend plusieurs étapes, notamment le téléchargement de scripts VBS chiffrés, l'exécution d'exécutables Delphi et le déploiement de logiciels malveillants en C++ pour un vol de données étendu.

Batavia utilise des tactiques d'évasion et des mécanismes de persistance avancés, ce qui en fait une menace importante pour la sécurité des organisations. La campagne reste active et risque d'entraîner des dommages supplémentaires en raison de sa capacité à télécharger des charges utiles supplémentaires.

