WWW.DUDIX-CONSULTING.FR

Les Nouvelles du Front

DUDIX CTI

Semaine 27
7 juillet 2025

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

TOP THREAT

Targeted sector: Defense

Active Intrusion set: TA828

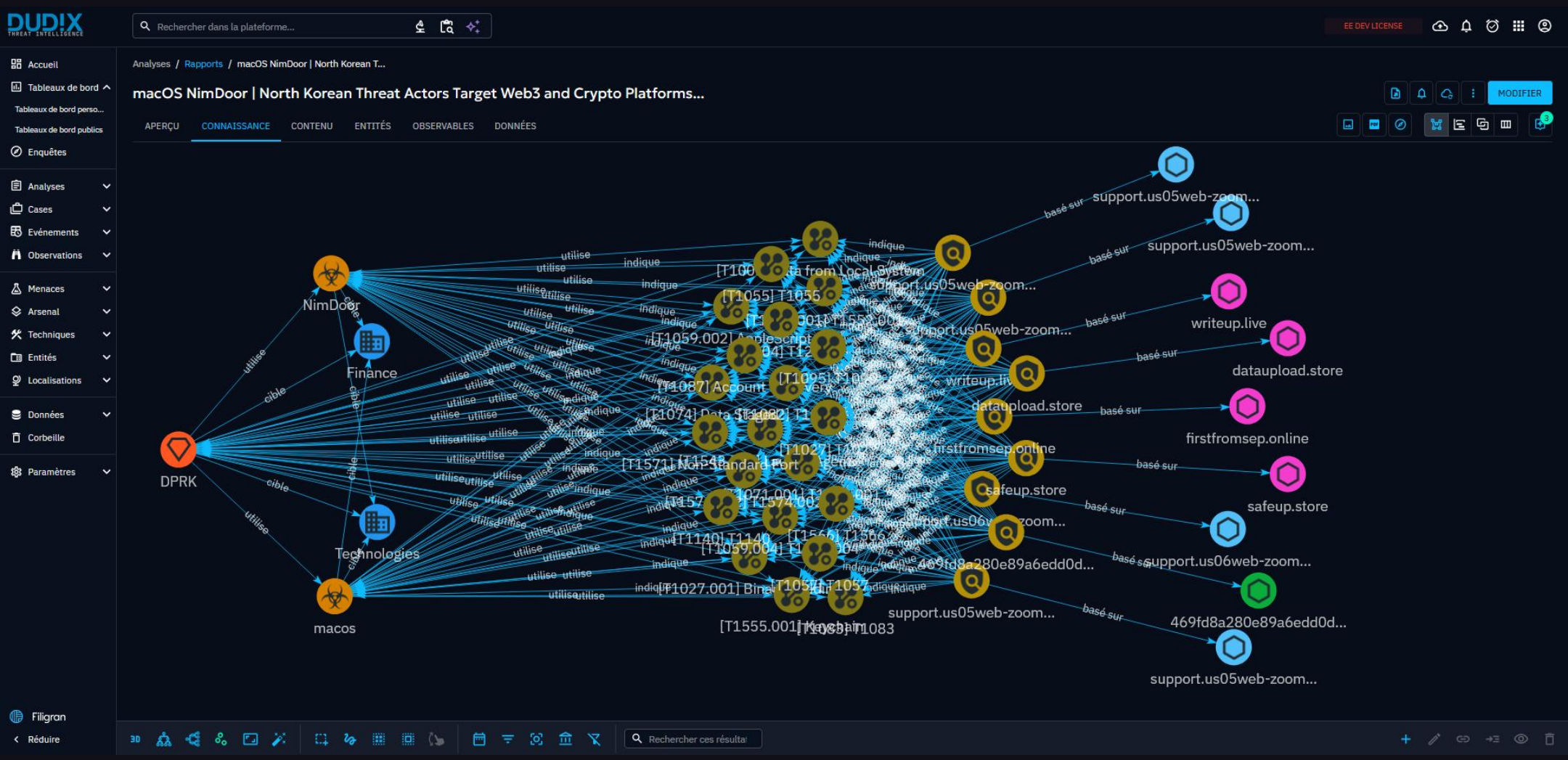
Targeted countries: Ukraine

Active vuln: CVE-2010-2568

Active TTP: T1082, T1027

Active Malwares: NimDoor

ACTIVITIES OF THREAT ACTOR: NimDoor (DPRK)



Le malware **NimDoor** est une menace récente et sophistiquée attribuée à des groupes de hackers nord-coréens (DPRK) ciblant spécifiquement les entreprises du secteur Web3 et des cryptomonnaies sur macOS.

Voici les points clés à connaître sur NimDoor :

- Développé par des acteurs liés à la Corée du Nord, NimDoor vise principalement les organisations Web3 et crypto, cherchant à voler des données sensibles et des cryptomonnaies.
- Les attaquants utilisent des techniques de social engineering en contactant les victimes via Telegram, puis les incitent à planifier un appel Zoom via Calendly. Ils envoient ensuite un email avec un faux script de mise à jour Zoom malveillant qui installe NimDoor de manière furtive.
- NimDoor est écrit en langage Nim, un choix rare qui complique sa détection.
- Il utilise une persistance sophistiquée basée sur la gestion des signaux SIGINT/SIGTERM, ce qui lui permet de se réinstaller automatiquement même après avoir été tué ou après un redémarrage du système.
- Il emploie des techniques rares sur macOS, comme l'injection de processus et des communications chiffrées via WebSocket TLS (wss).
- Il exfiltre des données sensibles telles que les historiques de navigation, les identifiants stockés dans le trousseau d'accès (Keychain) et les données Telegram.