ORYXLABS

UNMASK

EXPOSER LE CÔTÉ SOMBRE DE L'ANONYMAT

BROCHURE PRODUIT

INTRODUCTION

Dans le paysage numérique actuel, les personnes en quête d'anonymat utilisent de plus en plus des outils avancés tels que les sites du dark web, les VPN, les crypto-monnaies et les plateformes sociales. Bien que ces outils puissent être utilisés à des fins légitimes, telles que la protection de la vie privée et de la liberté d'expression, ils peuvent également être exploités par des personnes ayant des intentions malveillantes.

Depuis des décennies, les services de police et de sécurité sont confrontés à la difficulté d'identifier et de suivre les individus qui opèrent en ligne de manière anonyme.

La disponibilité de services sophistiqués est un facteur clé qui contribue à la persistance de l'anonymat. Ces services incluent des systèmes complexes avec des pools d'adresses IP tournantes, des proxys résidentiels et des réseaux P2P, qui permettent aux individus de masquer leur identité et de rester en dessous des radars. En outre, les techniques de cryptage et d'obscurcissement du trafic rendent difficile la détection de leurs activités par les mesures de sécurité traditionnelles, telles que l'inspection approfondie des paquets (Deep Packet Inspection - DPI).

En outre, les individus ont mis au point des techniques de séparation des réseaux, ce qui rend difficile le suivi de leurs mouvements, même lorsque les adresses IP sont compromises. Ils opèrent dans un domaine où l'anonymat offre une couche de protection, et les conséquences des activités non détectées peuvent être significatives.

Aussi observons-nous les tendances suivantes :

- **L'EXPLOITATION DES RÉSEAUX SOCIAUX**
  Les réseaux sociaux tels que Telegram, WhatsApp ou Signal sont utilisés par des acteurs malveillants pour communiquer de manière anonyme et partager des informations.
- **L'EXTENSION DU DARK WEB**
  Le dark web, un sous-ensemble d'Internet intentionnellement caché, gagne en ampleur et en popularité.
- **L'ANONYMAT EST UN BOUCLIER**
  L'utilisation d'outils anonymes comme les VPN, les crypto-monnaies et les plateformes sociales spéciales rend impossible le suivi de l'identité des cyber-pirates. Cela leur permet d'opérer en toute impunité et d'échapper à la détection.

+ de 2,5 millions
de visiteurs quotidiens du dark web

90%
Du web comprend le deep web et le dark web

40%
D'augmentation dans l'utilisation des plateformes décentralisées (Telegram)

176 millions de $
Augmentation annuelle des crimes liés aux cryptomonnaies par rançongiciel sur le dark web

2,95 milliards
D'utilisateurs actifs mensuels de WhatsApp

950 millions
D'utilisateurs actifs mensuels sur Telegram

40 millions
D'utilisateurs actifs mensuels sur Signal

NOTRE SOLUTION

UNMASK UNMASK est un moteur de désanonymisation qui s'appuie sur une expertise approfondie du domaine, sur l'Open-Source Intelligence (OSINT), sur l'autonomisation du réseau et l'IA pour générer le flux IP de services d'anonymat le plus complet et le plus précis qui soit.

Cette solution puissante aide les agences à garder une longueur d'avance sur l'évolution des tendances en matière d'anonymat, ce qui leur permet d'identifier et de traiter les menaces potentielles de manièreefficace et plus précise.

Notre solution permet aux utilisateurs de mettre en place et de déployer le système en utilisant uniquement des journaux réseau au format standard Netflow/IPFix ou tout autre format compatible disponible.

Nous détectons et attribuons sans effort les propriétaires et utilisateurs de services cachés ainsi que les propriétaires de profils de comptessociaux, même en présence d' obscurcissement et de cryptage, afin de perturber et d' appréhender les acteurs malveillants.

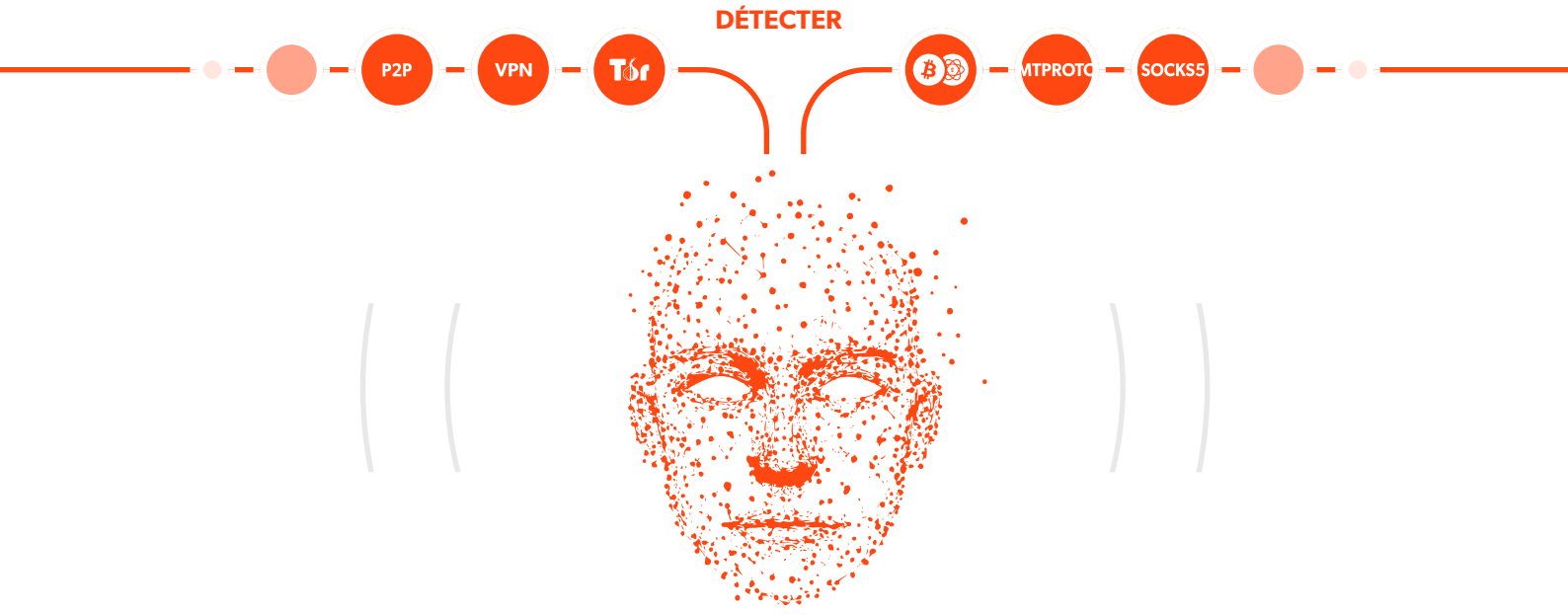
La plateforme s'appuie sur la technologie OSINT et la technologie unique de filigrane du réseaupour fournir une vue d'ensemble de l'activité du réseau, y compris des sites Onion et d'autres activités malveillantes.

Basé uniquement sur l'analyse des journaux réseau, notre moteur de désanonymisation offre une visibilité sans précédent sur les activités illégales en ligne des abonnés au réseau dans le pays.

» **ACTIVITÉ DÉTECTION**
Détecter l'accès des abonnés au réseau suspectéà des milliers de services et réseaux anonymes et différents.

» **TOR DÉ-SANONYMISATION**
Révéler les sites du dark web (Onion) exploités ou consultés par les abonnés du réseau suspect.

» **RÉSEAUTAGE SOCIAL DÉ-SANONYMISATION**
Révéler les identités Telegram WhatsApp, Signal et Twitter (X) au réseau suspect.



L'un des principaux facteurs de différenciation de la plateforme est sa capacité à détecter l'ensemble du trafic TOR, y compris les trafics obscurcis et les ponts TOR non publiés, les proxies Telegram et bien d'autres encore. Nous attribuons des utilisateurs de service cachés sélectionnés, ce qui permet d'obtenir des informations inégalées sur des activités anonymes. Notre solution révèle également les administrateurs et les abonnés des groupes cachés, même lorsque les utilisateurs susmentionnés restent silencieux.

En tirant parti de ses caractéristiques et avantages uniques, UNMASK offre aux services de police et de sécurité une solution puissante pour désanonymiser les activités en ligne, avec la possibilité d'associer les abonnés aux sites auxquels ils accèdent et qu'ils gèrent, et d'associer les suspects des réseaux sociaux à leurs profils respectifs.

FONCTIONS

UNMASK offre une série de caractéristiques uniques qui nous distinguent des autres solutions de cybersécurité :

- **CAPACITÉS D'ATTRIBUTION D'IDENTITÉ**
  La capacité de désanonymisation permet d'attribuer des identités à des personnes opérant anonymement en ligne.
- **DÉTECTION DE SITES ONION**
  Rechercher tous les sites Onion hébergés sur votre réseau et sélectionner les sites Onion auxquels accèdent les utilisateurs ou les logiciels malveillants de votre réseau.
- **CORRÉLATION AVANCÉE ALGORITHMES**
  L'utilisation d'algorithmes avancés permet de détecter et d'attribuer des identités anonymes en ligne, même lorsqu'elles sont obscurcies et cryptées.
- **CAPACITÉS OSINT**
  Exploiter l'OSINT pour recueillir des renseignements à partir de sources accessibles au public, offrant ainsi une vue d'ensemble des activités anonymes.
- **TECHNOLOGIE DE FILIGRANE UNIQUE**
  L'utilisation d'une technologie propriétaire de filigrane en réseau permet d'attribuer presque en temps réel des activités en ligne anonymes.
- **INFORMATIONS EN TEMPS QUASI RÉEL**
  Offrir une attribution en temps quasi réel des activités en ligne anonymes, permettant aux utilisateurs de prendre des mesures rapides pour protéger leurs réseaux et leurs actifs.
- **ANALYSE DES COMMUNICATIONS CHIFFRÉES**
  La plateforme permet d'extraire des informations uniques pour chaque abonné du réseau, y compris les activités cryptées effectuées par l'abonné.
- **NÉCESSITE UNIQUEMENT DES JOURNAUX RÉSEAU**
  Notre plateforme ne requiert en entrée que des journaux/logs réseau au format standard Netflow/IPFix ou tout autre format compatible.

AVANTAGES

UNMASK offre de nombreux avantages aux organismes chargés de l'application de la loi et de la sécurité, notamment :

- **ATTRIBUTION DES ACTIVITÉS ANONYMES**
  Attribuer des identités et des activités anonymes en ligne en temps quasi réel, permettant à nos clients d'identifier les cyber-pirates cachés.
- **UNE INSTALLATION ET UN DÉPLOIEMENT AISÉS**
  Facile à mettre en place et à déployer avec seulement des journaux réseau au format standard Netflow/IPFix ou tout autre format compatible requis.
- **EXPOSITION DES SERVICES MALVEILLANTS CACHÉS**
  Détecter et attribuer les propriétaires et utilisateurs de services cachés, même en présence d'obscurcissement et de cryptage, afin de perturber et d'appréhender les acteurs malveillants.
- **OBTENTION D'UN APERÇU SUR L'ACTIVITÉ DU RÉSEAU**
  Extraire des informations uniques pour chaque abonné, y compris lorsque le trafic réseau est crypté.
- **RÉPONSE AUX MENACES EN TEMPS QUASI RÉEL**
  Attribuer des activités anonymes en ligne en temps quasi réel, ce qui permet de réagir rapidement aux menaces émergentes.
- **VUE COMPLÈTE DE L'ACTIVITÉ DU RÉSEAU**
  Tirer parti de l'OSINT et d'une technologie unique de filigrane pour obtenir une vue d'ensemble de l'activité des réseaux, y compris les réseaux sociaux, les sites Onion et d'autres activités cachées.

ORYXLABS

QUI SOMMES-NOUS

ORYXLABS a été fondée à Abou Dhabi en 2020 avec une passion pour l'ingénierie axée sur la cybersécurité.

Une équipe fièrement diversifiée, originaire de 22 pays différents, avec des antécédents allant de la défense nationale à des organisations d'ingénierie logicielle de renommée mondiale, s'est unie pour développer des solutions de sécurité de premier ordre.

Nous nous appuyons sur la recherche et l'innovation pour fournir des solutions dans quatre domaines clés :

- Évaluation de la cybersécurité
- Surveillance
- Prévention
- Perfectionnement

Combinées, les solutions ORYXLABS offrent une approche holistique de la connaissance de la situation et de l'atténuation des attaques.

SITE WEB
Scanner pour voir

VIDÉO
Scanner pour voir

NOTRE MISSION

Notre mission consiste à doter les équipes de cybersécurité de renseignements et de solutions techniques de premier ordre qui permettent d'évaluer, de surveiller et d'améliorer en permanence les environnements afin d'atténuer les attaques en cours ou à venir.

POURQUOI NOUS

En tant qu'entreprise agile et innovante spécialisée dans la cybersécurité, nous sommes fiers de concevoir des solutions hautement personnalisées pour répondre aux besoins exacts de nos clients, et non des produits « à formule unique » comme le font nos concurrents dans ce domaine.
Grâce à notre expérience combinée en matière d'apprentissage poussé, d'IA, de recherche sur les vulnérabilités et de big data, ainsi qu'à nos partenariats avec des experts en la matière de renommée mondiale, vous pouvez être certain que nos solutions sont construites et exploitées sur la base d'informations opportunes et exactes.

POURQUOI NOUS

2025
ENTREPRISE LA PLUS INNOVANTE EN MATIÈRE DE CYBERSÉCURITÉ
Prix d'excellence en cybersécurité

2024
ENTREPRISE LA PLUS INNOVANTE EN MATIÈRE DE CYBERSÉCURITÉ
Prix d'excellence en cybersécurité

2023
ENTREPRISE LA PLUS INNOVANTE EN MATIÈRE DE CYBERSÉCURITÉ
Prix d'excellence en cybersécurité

2022
FOURNISSEUR DE SOLUTIONS DE CYBERSÉCURITÉ DE PREMIER PLANMOYEN-ORIENT
Sécurité d'entreprise

ORYXLABS

21e étage, Aldar HQ
Al Raha Beach
Boîte Postale : 33289
Abou Dhabi, ÉMIRATS-ARABES UNIS

oryxlabs.ae