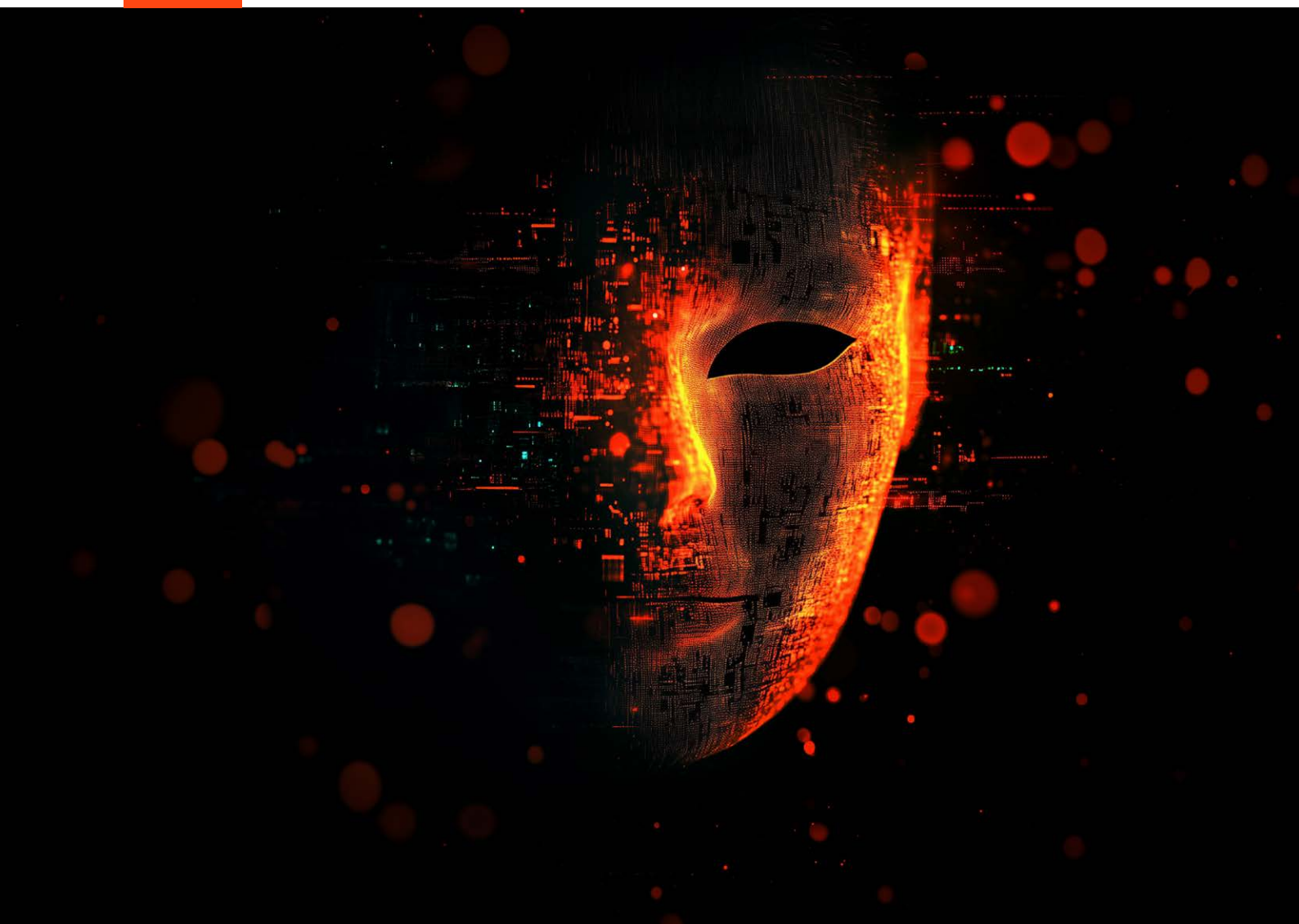
أوريكسلابز

UNMASK

كشف الجانب الآخر من عالم إخفاء الهوية

كتيب المنتج



المقدمة

في المشهد الرقمي اليوم، يلجأ الأفراد الباحثون عن التخفي إلى أدوات متقدمة مثل مواقع الويب المظلمة والشبكات الافتراضية الخاصة والعملات المشفرة والمنصات الاجتماعية. ورغم إمكانية استخدام هذه الأدوات لأغراض مشروعة مثل حماية الخصوصية وحرية التعبير، إلا أنه يتم استغلالها من قبل أشخاص ذوي نوايا خبيثة.

ولعقود طويلة، واجهت الأجهزة الأمنية وجهات إنفاذ القانون تحديات كبيرة في تحديد وتتبع الأفراد الذين يعملون بسرية مطلقة على الإنترنت.

ومن العوامل الرئيسية التي تعزز استمرار هذه الظاهرة هو توفر خدمات متطورة للغاية. تشمل أنظمة معقدة بمجموعات عناوين بروتوكول إنترنت متغيرة باستمرار، والوكلاء السكنيين (Residential Proxies)، وشبكات النظير إلى النظير (P2P)، مما يُمكن المستخدمين من إخفاء هوياتهم والبقاء متوارين عن الأنظار. كما أن تقنيات التشفير وتمويه البيانات تزيد من صعوبة رصد هذه الأنشطة عبر الأساليب الأمنية التقليدية مثل الفحص العميق للحزم DPI.

علاوةً على ذلك، طوّر هؤلاء الأفراد تقنيات لفصل الشبكات، مما يجعل تتبع تحركاتهم أمرًا صعبًا للغاية حتى في حالة كشف عناوين بروتوكول الإنترنت الخاصة بهم. هؤلاء الأفراد ينشطون في عالم يمنحهم فيه التخفي حماية إضافية، وتكون فيه تبعات الأنشطة غير المكتشفة خطيرة جدًا.

نتيجة لذلك، نلاحظ التوجهات التالية:

- **استغلال شبكات التواصل الاجتماعي**
  تُستخدم شبكات اجتماعية مثل تيليجرام وواتساب وسيجنال من قِبل العناصر الخبيثة للتواصل بسرية وتبادل المعلومات.

- **توسع ملحوظ في الشبكة المظلمة**
  شبكة الإنترنت المظلمة، وهي مجموعة فرعية من الإنترنت مخفية عن قصد، تتزايد من حيث الحجم والشعبية.

- **استخدام تقنيات إخفاء الهوية كدرع وقاية**
  استخدام الأدوات التي تضمن التخفي مثل الشبكات الافتراضية الخاصة VPN والعملات المشفرة والمنصات الاجتماعية المتخصصة يجعل تتبع هويات العناصر الخبيثة مستحيلاً، مما يسمح لهم بالعمل بحرية وتجنب الانكشاف.

+2.5M
زائر يومياً للشبكة المظلمة

%90
من شبكة الإنترنت تقع في النطاق العميق والمظلم

%40
ارتفاع في استخدام المنصات اللامركزية (مثل تيليجرام)

176 مليون دولار
الزيادة السنوية في جرائم طلب الفدية عبر العملات المشفرة على الويب المظلم

2.95 مليار
مستخدماً نشطاً بشكل شهري على تطبيق واتس آب

950 مليون
مستخدماً نشطاً بشكل شهري على تطبيق تيليجرام

40 مليون
مستخدماً نشطاً بشكل شهري على تطبيق سجنال

حلولنا

يعد UNMASK محركاً متطوراً لإزالة التخفي، يستفيد من الخبرات العميقة في المجال، وتقنيات استخبارات المصادر المفتوحة، وأتمتة الشبكات، والذكاء الاصطناعي لتوفير أدق وأشمل قاعدة بيانات لعناوين بروتوكول الإنترنت الخاصة بخدمات التخفي.

ويساعد هذا الحل المبتكر الجهات الأمنية في مواكبة التغيرات المستمرة في أساليب التخفي، مما يتيح لها كشف التهديدات المحتملة والتصدي لها بفعالية أكبر ودقة عالية.

ويتيح هذا الحل المبتكر للمستخدمين سهولة الإعداد والتشغيل باستخدام سجلات الشبكات القياسية مثل Netflow/IPFix أو أي صيغة أخرى متوافقة.

وبفضل تقنياته المتقدمة، يتمكن من كشف وتحديد هويات أصحاب الخدمات الخفية ومستخدميها، وكذلك أصحاب الحسابات على المنصات الاجتماعية، حتى في ظل وجود التشفير وأساليب التمويه، مما يسمح بمواجهة وتعطيل الأنشطة الخبيثة بشكل فعال.

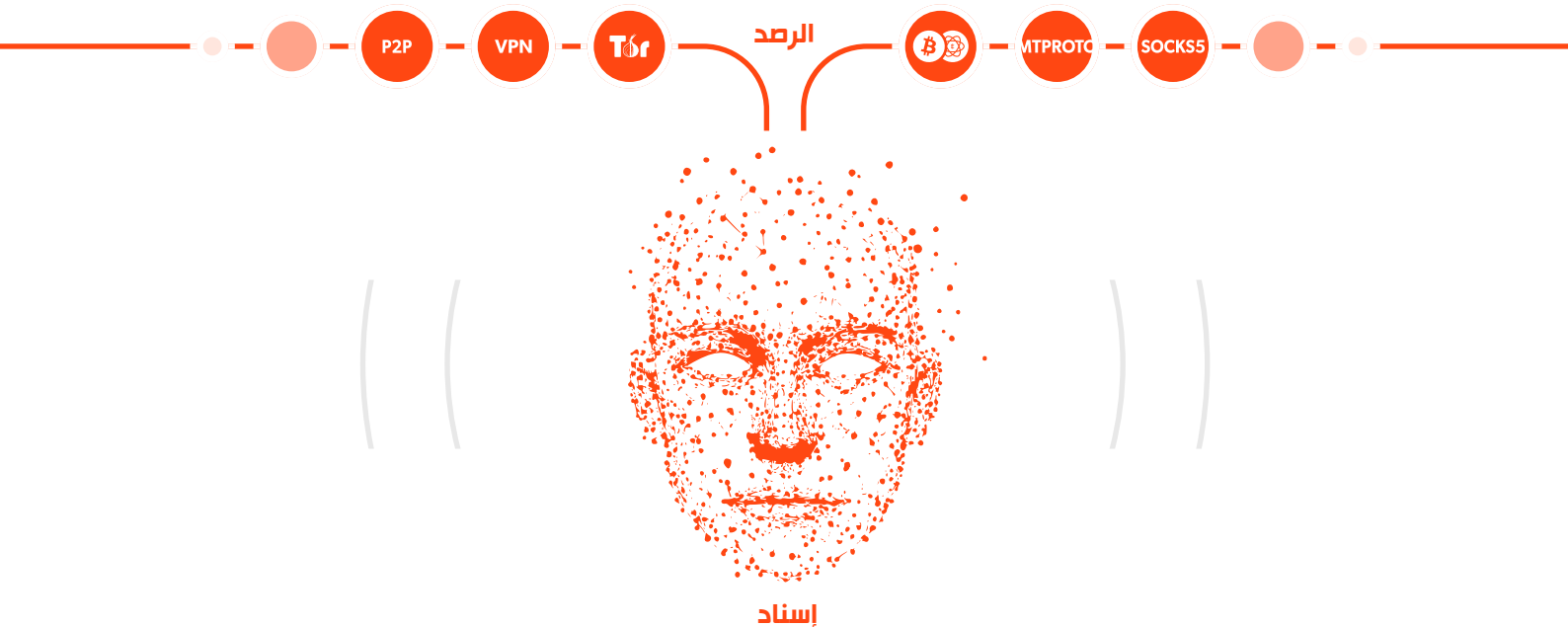
وتستفيد المنصة من المعلومات الاستخبارية من المصادر العلنية وتقنية وسم الشبكات لتوفير رؤية شاملة حول نشاطات الشبكة، بما في ذلك مواقع أونيون وغيرها من الأنشطة الخبيثة.

وبالاعتماد فقط على تحليل سجلات الشبكة، يوفر محرك إزالة التخفي رؤية غير مسبوقة للأنشطة غير القانونية للمستخدمين داخل الشبكات، مما يمكّن الجهات المختصة من اتخاذ الإجراءات المناسبة بشكل سريع وفعال.

» **كشف الأنشطة**
تحديد وصول المستخدمين المشتبه بهم إلى آلاف الخدمات والشبكات المخصصة للتخفي.

» **كشف هوية مستخدمي متصفح تور**
الكشف عن مواقع الويب المظلمة التي يديرها أو يزورها المشتركون المشتبه بهم.

» **كشف هوية مستخدمي الشبكات الاجتماعية**
الكشف عن هويات مشتركي الشبكة المشتبه بهم على منصات مثل تيليجرام وواتساب وسيجنال وتويتر (إكس).



إسناد

ما يميز المنصة بشكل خاص هو قدرتها على كشف جميع أنشطة متصفح تور، بما في ذلك تلك المُموهة وجسور تور غير المنشورة والبروكسيات الخاصة بتيليجرام وغيرها. كما تقوم المنصة بتحديد هوية مستخدمي الخدمات الخفية المُختارين، وتوفر رؤى لا مثيل لها حول الأنشطة المجهولة. كما تكشف عن مديري القنوات والمجموعات المخفية وأعضائها، حتى وإن لم يكن هؤلاء الأعضاء نشطين.

ومن خلال استثمار من هذه الميزات والفوائد الفريدة، يمنح محرك UNMASK الأجهزة الأمنية وجهات إنفاذ القانون أداة فعالة للكشف عن الأنشطة المجهولة عبر الإنترنت وربط المستخدمين بالمواقع التي يديرونها أو يصلون إليها، وربط المشتبه بهم على الشبكات الاجتماعية بملفاتهم الشخصية.

الخصائص

تتمتع منصة UNMASK بمجموعة فريدة من الخصائص التي تميزها عن حلول الأمن السيبراني الأخرى ومنها:

- **قدرات تحديد الهوية**
  إمكانية تحديد هويات الأفراد الذين يعملون بشكل مجهول عبر الإنترنت.
- **رصد المواقع المخفية (أونيون) على شبكة تور**
  الكشف عن مواقع أونيون المستضافة داخل شبكتك وتحديد المواقع التي يصل إليها المستخدمون أو البرمجيات الضارة.
- **خوارزميات الربط المتقدمة**
  استخدام خوارزميات متطورة لكشف وربط الهويات المجهولة، حتى في حالة استخدام التشفير والتمويه.
- **قدرات جمع المعلومات الاستخبارية من المصادر العلنية**
  الاستفادة من تقنيات استخبارات المصادر العلنية لجمع المعلومات من المصادر المتاحة علنًا، مما يوفر رؤية شاملة للأنشطة المجهولة.
- **تقنية الوسم الفريدة**
  تقنية وسم الشبكات الحصرية التي تسمح بتحديد الأنشطة المجهولة في الوقت شبه الحقيقي.
- **رؤى فورية**
  توفير رؤى شبه فورية حول الأنشطة المجهولة، ما يتيح اتخاذ إجراءات سريعة لحماية الشبكات والأصول.
- **تحليل الاتصالات المشفرة**
  تقدم المنصة تحليلات تفصيلية تشمل الأنشطة المشفرة للمشتركين في الشبكة.
- **الاعتماد على سجلات الشبكة فقط**
  تعتمد المنصة فقط على سجلات الشبكة بتنسيق Netflow/IPFix أو أي صيغة متوافقة أخرى كمدخلات.

المزايا

توفر منصة UNMASK مجموعة كبيرة من المزايا والفوائد الحصرية التي تعزز من قدرات أجهزة إنفاذ القانون والمؤسسات الأمنية الأخرى، نذكر منها ما يلي:

- **تحديد الأنشطة المجهولة**
  ربط الأنشطة المجهولة والهويات على الإنترنت في الوقت شبه الحقيقي، مما يعزز من قدرة المستخدمين على كشف اكتشاف العناصر الخبيثة.
- **سهولة الإعداد والنشر**
  سهولة الإعداد والنشر باستخدام سجلات الشبكة فقط بتنسيق NetFlow/IPFix القياسي أو أي تنسيق متوافق مطلوب.
- **كشف الخدمات الخبيثة المخفية**
  كشف وتحديد هويات أصحاب الخدمات الخفية، حتى في ظل وجود التشفير وأساليب التمويه، مما يسمح بمواجهة وتعطيل الأنشطة الخبيثة بشكل فعال.
- **رؤية شاملة للنشاط الشبكي**
  استخراج معلومات دقيقة حول أنشطة كل مشترك في الشبكة، حتى عند استخدام التشفير.
- **استجابة سريعة للتهديدات**
  توفير معلومات شبه فورية تمكن من الاستجابة السريعة للتهديدات الناشئة.
- **رؤية متكاملة لأنشطة الشبكة**
  الاستفادة من المعلومات الاستخبارية من المصادر العلنية وتكنولوجيا وسم الشبكات لتوفير رؤية شاملة حول نشاطات الشبكة، بما في ذلك الشبكات الاجتماعية ومواقع أونيون وغيرها من الأنشطة الخبيثة.

أوريكسلابز

من نحن

تأسست أوريكس لابز في أبوظبي عام 2020 بدافع شغفها بالهندسة المتخصصة في مجال الأمن السيبراني.

ويضم فريقنا المتنوع أفراداً قادمين من أكثر من 22 دولة مختلفة ومن خلفيات ومجالات عملية متنوعة مثل الدفاع الوطني ومؤسسات هندسة البرمجيات الرائدة عالمياً، معاً لإيجاد أفضل الحلول الأمنية ضمن فئتها.

ونوظف البحث والابتكار لتقديم الحلول في أربعة مجالات رئيسية:

- تقييم مستوى الأمن السيبراني
- المراقبة
- الوقاية
- التطوير

توفر حلولنا نهجاً شاملاً لتعزيز الوعي بالأوضاع والتخفيف من الهجمات.

الموقع الإلكتروني
المسح للعرض

فيديو
المسح للعرض

رسالتنا

تتمثل رسالتنا في تزويد فرق الأمن السيبراني بأفضل الحلول الاستخبارية والتقنية التي تعمل بشكل مستمر على تقييم ومراقبة وتحسين البيئات للحد من الهجمات الحالية أو المستقبلية.

لماذا نحن

نتبع في أوريكس لابز نهجاً مرناً وابتكارياً يركز على إيجاد الحلول المتكاملة لتعزيز الأمن السيبراني، ونفخر بما نقدمه لعملائنا من أنظمة مصممة خصيصاً لتلبية احتياجاتهم وحماية أصولهم، الأمر الذي يمنحنا الأفضلية ويميزنا عن منافسينا في المجال.

ونفخر بما نملكه من خبرات رائدة في مجال الذكاء الاصطناعي والتعلم العميق وتحليل البيانات الضخمة وأبحاث الثغرات الأمنية، فضلاً عن شراكاتنا الاستراتيجية مع نخبة من الخبراء العالميين، مما يضمن تعزيز حلولنا وتطويرها بناءً على معلومات موثوقة وحديثة.

جوائز الشركة

2025
أكثر الشركات ابتكاراً في مجال الأمن السيبراني
جوائز التميز في الأمن السيبراني

2024
أكثر الشركات ابتكاراً في مجال الأمن السيبراني
جوائز التميز في الأمن السيبراني

2023
أكثر الشركات ابتكاراً في مجال الأمن السيبراني
جوائز التميز في الأمن السيبراني

2022
من أفضل مزودي حلول الأمن السيبراني في الشرق الأوسط
أمن الشركات

أوريكسلابز

الطابق 21، برج الدار،
شاطئ الراحة
ص.ب: 33289
أبوظبي، الإمارات العربية المتحدة

oryxlabs.ae