الدارك ويب"الانترنت المظلم"

نظرة عامة

ربما سمعت بمصطلح الدارك ويب «الانترنت المظلم» الذي يستخدمه الآخرون أو من خلال وسائل الإعلام وتساءلت ما هو الدارك ويب؟ أو هل يجب أن أفعل شيئًا حيال ذلك؟ نوضح من خلال النشرة التعريفية ما هو الدارك ويب أو الانترنت المظلم وماذا يعني لك.

مما يتكون الدارك ويب "الانترنت المظلم"

تتكون شبكة دارك ويب من مجموعة من الأنظمة مصممة للاتصال أو مشاركة المعلومات بشكل آمن ومجهول على الإنترنت. لا يوجد شبكة دارك ويب واحدة؛ إنه ليس مثل Facebook تديره منظمة واحدة. بل إن شبكة الدارك ويب عبارة عن مجموعة من الأنظمة والشبكات المختلفة التي يديرها أشخاص مختلفون تُستخدم لأغراض متنوعة. لا تزال هذه الأنظمة متصلة بالإنترنت وتشكل جزءًا منه، ومع ذلك لن تجدها عمومًا باستخدام محركات البحث العادية. غالبًا ما تحتاج إلى برنامج خاص على الكمبيوتر للعثور عليها أو الوصول إليها. ومن أمثلتها مشروع تور. للوصول إلى شبكة الدارك ويب حيث تقوم بتنزيل وتثبيت متصفح Tor. عند الاتصال بخوادم الويب باستخدام متصفح Tor، تتنقل حركة المرور المشفرة عبر أجهزة كمبيوتر أخرى تستخدم Tor أيضًا وهو ما يعني أن عنوان المصدر IP عندما تصل إلى موقع الويب، يتم تغيره بما يعني أنه تم إخفاء نشاطك عبر الإنترنت. ومن الأمثلة الأخرى على برمجيات الدارك ويب Zeronet و Freenet و I2P.

من يستخدمه؟

مجرمو الإنترنت هم من كبار مستخدمي شبكة الدارك ويب، إنهم يحتفظون بمواقع ومنتديات في شبكة الويب المظلمة لتمكين أنشطتهم الإجرامية مثل شراء المخدرات أو بيع كميات كبيرة من البيانات المخترقة، كل ذلك يتم بطريقة تضمن للمستخدم أن يكون مجهول الهوية وآمن. على سبيل المثال، عندما يخترق مجرِم إنترنت بنكًا أو متجرًا للتسوق عبر الإنترنت، فإنهم يسرقون أكبر قدر ممكن من المعلومات، ثم يبيعون هذه المعلومات لمجرمي الإنترنت الآخرين على مواقع الدارك ويب.

هناك أيضًا استخدامات مشروعة للإنترنت المظلم. على سبيل المثال، يمكن للأشخاص في البلدان التي تنتشر فيها الرقابة استخدام شبكات الدارك ويب لتبادل المعلومات ومعرفة ما يحدث في العالم مع حماية خصوصيتهم وعدم الكشف عن هويتهم. يمكن للصحفيين

والأشخاص الذين يفكرون في الخصوصية استخدام شبكة الانترنت المظلمة لزيادة عدم الكشف عن هويتهم وتجاوز الرقابة. بالإضافة إلى ذلك، يمكن للأفراد من أمثالهم استخدام تقنيات مثل متصفح Tor، ليس فقط للوصول إلى شبكة الانترنت المظلمة، ولكن لتصفح الإنترنت العادي بشكل مجهول.

ماذا يجب أن أفعل؟

ما لم يكن لديك سبب محدد للوصول إلى شبكة الانترنت المظلمة، فإننا نحذرك من استخدامها. حيث يتم استخدام بعض مواقع الدارك ويب لأغراض غير قانونية، وسوف تستخدم العديد من المواقع جهازك الحاسوب في شبكة P2P لتحقيق أهدافها، وفي بعض الحالات قد يتم فحص جهازك أو مهاجمته. تقدم بعض الشركات خدمات مراقبة لإعلامك بما إذا كان اسمك أو معلوماتك الأخرى قد سرقها مجرمو الإنترنت وتم العثور عليها على شبكة الويب المظلمة. القيمة الفعلية لهذه الخدمات مشكوك فيها. أفضل طريقة لحماية نفسك هي افتراض أن بعض معلوماتك موجودة بالفعل على شبكة الدارك ويب التي يستخدمها مجرمو الإنترنت. لذلك عليك اتباع النصائح التالية:

- تأكد من أي مكالمات هاتفية أو رسائل بريد إلكتروني تتظاهر بأنها منظمة رسمية وتضغط عليك لاتخاذ إجراء، مثل دفع غرامة. قد يستخدم المجرمون المعلومات التي وجدوها عنك لإنشاء هجوم شخصي.
- مراقبة بطاقتك الائتمانية والبيانات المصرفية. ربما حتى إعداد تنبيهات يومية على أي معاملة ممكن أن تحدث على البطاقة. بهذه الطريقة يمكنك اكتشاف ما إذا كان هناك أي احتيال مالي في حال حدوثه. إذا اكتشفت ذلك، فأبلغ شركة بطاقات الائتمان الخاصة بك أو المصرف على الفور.
- قم بتحديد الاماكن المسموح بها استخدام بطاقتك « تجميد البطاقة». وهو أحد أكثر الخطوات الفعالة التي يمكنك اتخاذها لحماية نفسك من سرقة الهوية.

الضيف المحرر

Micah Hoffman (@WebBreacher) هو الباحث الرئيسي في Spotlight Infosec LLC ، وهو مدرس معتمد لمعهد SANS ومؤلف دورات SANS OSINT. يهتم في مشاريعه ودرواته وأسلوب تدريسه بإظهار الذكاء السيبراني والأنظمة مفتوحة المصدر.

مصادر إضافية

Personalized Attacks: https://www.sans.org/u/RfW
Social Engineering: https://www.sans.org/u/Rg1
Identity Theft: https://www.identitytheft.gov
Credit Freeze: https://krebsonsecurity.com/2018/09/credit-freezes-are-free-let-the-ice-age-begin/
Tor Browser: https://www.torproject.org/
SANS OSINT Course: https://sans.org/sec487