DIGITAL DEVELOPMENT CENTER
مركز التطوير الرقمي

مخاطر الويب المظلم: كيف تحمي نفسك؟

تحرير وترجمة
مركز التطوير الرقمي

عن المركز

مركز التطوير الرقمي منظمة عراقية غير حكومية تأسست سنة ٢٠٢٠ ، مسجل لدى دائرة المنظمات غير الحكومية في الأمانة العامة لمجلس الوزراء .

يسعى المركز إلى سد الفجوة الرقمية والتحول إلى مجتمع رقمي ومواطنة رقمية Digital Citizenship لبناء اقتصاد رقمي متطور وتحسين جودة حياة المواطن.

إنَّ من أهم أهداف المركز تنمية الموارد البشرية في مجال تكنولوجيا المعلومات والاتصالات ، وبما يتناسب مع متطلبات المرحلة ويلبي احتياجات سوق العمل المحلي والدولي ، ونشر الوعي الرقمي والثقافة الرقمية بين أبناء المجتمع ، ودعم قطاع الاتصالات من خلال ورش العمل ، الندوات ، المؤتمرات ، والدراسات والبحوث.

ومن ضمن أولويات المركز خلق بيئة رقمية مناسبة لتشجيع الشركات وأصحاب الاهتمام المشترك من الشركات في الدول والاستثمار في هذا القطاع الحيوي، ويسعى المركز إلى رعاية القدرات والطاقات الشابة من المواهب والمتميزين في مراحل الدراسة الأولية ، والمساهمة في دعم حملة الشهادات العليا بما يسهم في تشجعيهم على إعداد الدراسات البحثية وتقديم الاستشارات العلمية ، والمواءمة بين المنظمات المحلية والدولية من خلال التواصل مع المنظمات العالمية والإقليمية، ولتحقيق هدف المواطنة الرقمية ومحو الأمية الرقمية يسعى المركز ليكون حلقة وصل بين القطاع العام والخاص وتقديم المشورة لدوائر الدولة والمؤسسات الخاصة، والمساهم في بلورة القرارات الاستراتيجية للدولة العراقية بما يتعلق بتقنيات المعلومات والاتصالات .

info@ddc.iq

إن الإنترنت واسع جداً، حيث يحتوي على الملايين من مواقع الويب والمنتديات والخوادم وقواعد البيانات التي تتبادل المعلومات على مدار الساعة طوال أيام الأسبوع، ولكن هذا هو الجانب "المرئي" فقط من الإنترنت، مما يعني أنه يمكن العثور بسهولة على كل هذه المواقع والخوادم بإستخدام محرك بحث غوغل ومحركات البحث الأخرى. تسمى هذه الشبكة السطحية، وفي ما يلي قصة مختلفة عن الويب المظلم.

مكان للنشاط الإجرامي

تصف وسائل الإعلام والمواقع الإخبارية شبكة الويب المظلمة (Dark Web) بأنها مركز للنشاط الإجرامي، وهناك بعض الحقيقة في ذلك. تظهر الأبحاث أن نشاط الويب المظلم قد زاد بنسبة ٪300 منذ عام 2017، مما أدى إلى زيادة الجرائم الإلكترونية والأنشطة الخبيثة.

إن مواقع الويب والأشخاص الذين لا يريدون أن يتم العثور عليهم يجعلون الويب المظلم مكاناً خطيراً. في حين أن بعض الناس يجدون هذه الفرصة مثالية للتهرب من الضوابط والرقابة الحكومية، ينغمس آخرون في نشاط غير قانوني للغاية حيث يختبئون وراء إخفاء هويتهم. فعلى سبيل المثال، يحتاج المستخدم إلى متصفح خاص للدخول إلى هذه المواقع، مما يجعل من الضروري الحفاظ على سرية نشاطه على الإنترنت وخصوصيته عند زيارتها.

تشمل هذه الأنشطة غير القانونية على تزوير معلومات بطاقة الدفع الأمنية، وتسريب شفرات المصدر (Source Code)، وسرقة الهويات، والمحتوى الإباحي. وعلى الرغم من الإجراءات الأمنية المتزايدة وأنظمة الدفاع المعقدة، غالباً ما تخسر المؤسسات المعركة ضد هذه الهجمات الإلكترونية.

ومن بين جميع الأنشطة الإجرامية غير القانونية على الويب المظلم، كانت هناك حوادث مفرطة لسرقة الهويات والإحتيال، حيث خسر المستهدفون ما يقارب الـ 63 مليار دولار بسبب سرقة الهويات منذ آذار 2020، وخسر مستخدمو المتاجر الإلكترونية ما يقارب الـ 370 مليون دولار بسبب عمليات الإحتيال المرتبطة بجائحة كورونا.

ما هو الويب المظلم بالتحديد؟

هو مجموعة من مواقع الإنترنت التي لم تتم فهرستها، وتم إخفائها من خلال إجراءات أمنية قوية مثل التشفير (Encryption) والجدران النارية (Firewalls). هذا ما يجعل شبكة الويب المظلمة ملاذاً آمناً للمستخدمين الذين يحاولون البقاء المجهولين (Anonymous).

وكما ذكرنا سابقاً، فقد إكتسب الويب المظلم سمعة واسعة للمحتوى غير القانوني والإجرامي، كما يمثل ملاذاً آمناً لمواقع "التجارة غير القانونية"، حيث يمكن شراء جميع أنواع السلع والخدمات غير القانونية وتداولها. ولكن هذا لا يعني أنه لا توجد أطراف قانونية فيه. فبفضل متصفح Tor، يمكن الآن لأي شخص زيارة المواقع على Dark Web.

ليس هناك مانع من زيارة الويب المظلم، حيث لا توجد أي قوانين تمنع ذلك، ولكن قد يتعرض المستخدم لأنواع أخرى من المشاكل إذا لم يقم بتشفير بيانات الإعتماد بشكل فعال. يمكن أن يعرض مستخدم الويب المظلم لمخاطر غير ضرورية، وإذا لم يكن مدركاً تماماً لتهديداته، فيمكن للآخرين إستغلال معلوماته.

توجهات السوق السوداء التي تشكل تهديداً لسلامة المستخدمين

عندما يتعلق الأمر بأمان المستخدم على الويب المظلم، فإن المخاطر هنا تختلف تماماً عما قد يواجهه على الويب السطحي. أدناه المزيد من التفصيل عن هذه المخاطر:

1- تقنية التزييف العميق (Deepfake):

بالإمكان إنتحال هوية مستخدمي الويب المظلم في حال عدم تأمينها بشكل ملائم، حيث كان التحقق من الهوية الرقمية هدفًا رئيسياً للعديد من الجرائم الإلكترونية والأنشطة الخبيثة، ومنها عمليات إستخدام برامج التزييف العميق (Deepfake) على الويب المظلم.

إن تقنية التزييف العميق هي تقنية مستخدمة في الويب المظلم تستخدم المعرفة العميقة بالذكاء الإصطناعي لتزوير الصور ومقاطع الفيديو والهويات والأحداث. على سبيل المثال، يمكن للقراصنة الرقميين إستخدام التزييف العميق لتزوير الهويات ومقاطع

الفيديو بإستخدام البيانات المتوفرة عن شخص معين، وذلك بقصد إلحاق الضرر به وعمله، ووفقاً للأبحاث، تم إستخدام تقنية التزييف العميق أيضاً كسلاح ضد النساء عبر المحتوى الإباحي.

2- نسخ بصمة الصوت:

بإستخدام تقنية التزييف العميق، يمكن للمخترقين المحترفين أيضاً إنشاء حسابات مزورة على وسائل التواصل الإجتماعي للتجسس على المستخدمين، سواء الأجانب أو المحليين. حيث يمكنهم حتى تحرير الملفات الصوتية لإنشاء نسخ صوتية لهم.

في آذار 2019، دفع الرئيس التنفيذي لشركة ألمانية كبيرة ما يقارب الربع مليون دولار فيما وصفه خبراء الجرائم الإلكترونية بأنه حالة غير إعتيادية من جرائم التزييف العميق بإستخدام الذكاء الإصطناعي، حيث تم تقليد صوت المستهدف من خلال الإستنساخ الصوتي المدعوم بالذكاء الإصطناعي للمطالبة بهذا المبلغ من المال بشكل فدية.

3- أسواق الويب المظلمة:

تحاكي أسواق الويب المظلمة الأسواق الكبار مثل eBay و amazon، مع إستكمال إمكانات التجارة الإلكترونية مثل عربات التسوق والمشتريات المخصصة وردود المستخدمين. ولكن هذه الأسواق أكثر خطورة، لأنها تخزن المزيد من المعلومات. إن التسوق هنا يعني ترك التفاصيل الشخصية والسجلات المالية الخاصة التي تسمح لمجرمي الإنترنت بتنفيذ هجمات ضارة بسهولة.

ومع إنتشار العملات الرقمية المبنية على تقنية السلاسل الكتلية (Blockchain)، أصبح بإمكان المجرمين إخفاء هوياتهم بشكل أكثر فعالية للمتاجرة بشكل السري، حيث أن لديهم حافز أكبر لإرتكاب جرائم سرقة الهوية. وفقاً للأبحاث، كانت دلائل الإستخدام للأغراض الخبيثة هي فئة المنتجات الأكثر شيوعاً لمستخدمي الويب المظلم (49٪)، تليها المعلومات الشخصية (15.6٪).

كيف تحمي بياناتك من الويب المظلم؟

يجب إتخاذ تدابير أمنية كافية للحفاظ على البيانات الشخصية وبيانات العمل والعملاء والموظفين من التسريب إلى الإنترنت المظلم. ولكن قبل نشر أي أدوات إضافية لتأمين ذلك، يجب التأكد من أن جميع التطبيقات والشبكات والعمليات تلتزم بأعلى ممارسات الأمن السيبراني. وبمجرد التأكد من أن جميع التطبيقات والشبكات آمنة، يمكن تضمين طبقات الأمان الإضافية التالية:

1- الإلتزام بعمل نسخ إحتياطية:

يجب التأكد من الإتساق في العمل بإستخدام النسخ الإحتياطية السحابية الآمنة التي يمكنها إستعادة البيانات بسرعة في حالة حدوث خرق للبيانات. في هذه الحالة، يكون نظام النسخ الإحتياطي عن بعد مثالياً.

إن تخزين جميع البيانات ونسخها إحتياطياً على نفس الجهاز يجعل من السهل على المتسللين إتلاف حتى النسخة الإحتياطية منها. ولكن تكون النسخ الإحتياطية عن بُعد أكثر جدوى، لأنها تتيح الوصول إلى البيانات المهمة حتى إذا تم إختراق الخادم الرئيسي. سواء كان خادماً قائماً على السحابة، أو منصة مادية مخصصة، فإن النسخ الإحتياطية البعيدة ضرورية لتجنب التلف والتسريب.

2- مراقبة الويب المظلم:

إن من الحلول الفعالة إستخدام أدوات مراقبة الويب المظلم للإبقاء على دراية بأي تناقضات في البيانات ومراقبة الويب المظلم بحثاً عن البيانات المفقودة أو المسربة. تساعد أدوات مراقبة الويب المظلم أيضاً الشركات على البقاء يقظين بشأن معلومات التعريف الشخصية (Personal Identification Information)، مثل أرقام الهوية أو معلومات بطاقة الائتمان أو معلومات تسجيل الدخول إلى وسائل التواصل الاجتماعي أو معلومات تسجيل الدخول البيومترية.

كلما كانت المؤسسة أكثر تشدداً في مراقبة الويب المظلم، كلما كانت أفضل إستعداداً للهجمات الخبيثة.

3- إستخدام أدوات مراقبة إنتحال الهوية:

إن من الإضافات الأخرى القيّمة لإستراتيجيات الحماية هي خدمات مراقبة الهوية، التي تراجع تطبيقات الويب للمستخدمين بحثاً عن أي أنشطة مشبوهة وتوفر تنبيهات منتظمة، مع قابلية إستعادة البيانات التامة.

قد تكون مراقبة سرقة الهوية هي الطريقة الأكثر فعالية لضمان الحفاظ على خصوصية المعلومات وعدم إساءة إستخدامها أبداً، حيث أن البيانات الشخصية والتجارية لها سعر على شبكة الويب المظلمة، ويمكن بيعها بسهولة. تتضمن البيانات أرقام الحسابات المصرفية وكلمات المرور وأرقام الهويات والعناوين وما إلى ذلك.

يمكن للجهات الخبيثة إستخدام هذه المعلومات لتدمير الإئتمان وسرقة الأموال بإستخدام هويات حقيقية مسروقة، يمكن أن تضر بسمعة الأفراد والمؤسسات من خلال عمليات الإحتيال.

4- البقاء مطلعاً على آخر أخبار الأمن السيبراني:

هناك طريقة أخرى لتأمين البيانات، وهي تحديد الأنماط الإحتيالية. من خلال تحليل الهجمات الإلكترونية السابقة على مؤسسات أخرى، يمكن تحديد أي إجراء قد يبدو مشكوكاً به قبل أن يصبح مشكلة للمؤسسة.

على سبيل المثال، يمكن أن يشير الإرتفاع المفاجئ في العقود الملغاة إلى نشاط مشبوه، حيث يجب مراقبة أخبار جرائم سرقة الهوية لفهم التقنيات التي يستخدمها المتسللون وتمييز أنماط الإحتيال المستخدمة.

الإستنتاج

تعرضت بعض أكبر الشركات عبر الصناعات لخسائر كبيرة بسبب خروقات البيانات والسرقات. ومع تحسن التكنولوجيا، أصبح لدى المهاجمين المزيد من السبل لإستغلالها، مثل إستخدام الذكاء الإصطناعي للتعمق في شبكات الشركات والعثور على المعلومات لتسريبها أو تدميرها.

لذلك، فمن الضروري إتخاذ الإحتياطات الأمنية ومراقبة تطبيقات الويب بإنتظام بحثاً عن أي أنشطة مشبوهة.

—

المصدر

January 25, 2022 by Gabija Stankevi□i□t□

/https://www.idenfy.com/blog/dangers-of-the-dark-web