الخليج

اقتصاد, تقنية وسيارات

17 مايو 2022  16:30 مساء

# يمكّن محتالي الإنترنت من تجنّب الانكشاف «HTML» استخدام مرفقات

دبي: «الخليج»

حذّر خبراء «كاسبرسكي» المستخدمين من التهديد المتنامي المتمثل بالأعداد المتزايدة من رسائل البريد الإلكتروني وحظر باحثو «كاسبرسكي» بين يناير/ كانون الثاني وإبريل/ نيسان من .«HTML» المخادعة، التي تحتوي على ملفات ويُعدّ «HTML» العام الجاري ما يقرب من مليوني رسالة بريد إلكتروني تصيدية تحتوي على مرفقات من ملفات في رسائل التصيّد أحد أحدث الحيل الشائعة التي يلجأ إليها المحتالون في محاولاتهم «HTML» استخدام ملفات الإيقاع بالمستخدمين. وعادةً ما تكتشف محركات مكافحة البريد الإلكتروني غير المرغوب فيه، أو برمجيات مكافحة في رسائل البريد تلك سمح لمجرمي الإنترنت «HTML» الفيروسات، هذه الروابط بسهولة، لكن استخدام مرفقات بتجنب انكشافهم.

ولا يدرك الكثير من المستخدمين أن الملفات المرفقة في رسائل البريد الإلكتروني التي تصلهم، ومنها ملفات قد تكون غير آمنة، لذا فهم يفتحون تلك المرفقات باطمئنان، ليتبيّن أنها أسلحة خطرة وموجهة يستخدمها «HTML» لتبدو متطابقة مع صفحات في مواقع «HTML» مجرمو الإنترنت للإيقاع بهم. ويمكن للمحتالين تصميم مرفقات

الويب الرسمية لبعض الشركات والخدمات، مستهدفين مستخدمي تلك المواقع لخداع ضحاياهم والإيقاع بهم، عبر دفعهم إلى إدخال بيانات حساسة في نموذج خاص ضمن الصفحة الاحتيالية.

برابط تصيّد، أو «HTML» التي يستخدمها مجرمو الإنترنت: ملفات «HTML» وهناك نوعان أساسيان من مرفقات يحتوي على نص «HTML» صفحات خبيثة كاملة. أما الحالة الأولى، فيرسل فيها المهاجمون إلى المستخدم ملف يدّعون أن فيه بيانات مهمة، كإشعار بنكي بشأن محاولة لتحويل مبلغ مالي كبير من حسابه، ويُطلب منه النقر فوق رابط إلى موقع البنك لإيقاف المعاملة، ما يقوده إلى صفحة تصيّد. وفي بعض الحالات، لا تضطر الضحية حتى إلى النقر فوق سيوجّهه تلقائياً إلى صفحة خبيثة، يُطلب منه فيها ملء نموذج «HTML» الرابط، فعندما يحاول المستخدم فتح مرفق بيانات لمراجعة الملفات المتعلقة بالعمل أو، في الحالة المذكورة، حماية حسابه المصرفي من محاولة تحويل المال، أو حتى تلقي مدفوعات حكومية، ليكتشف لاحقاً أن بياناته الشخصية وتفاصيله المصرفية قد سُرقت.

عبارة عن صفحات تصيّد كاملة، إذ تُعفي هذه الملفات مجرمي الإنترنت من تحمّل «HTML» النوع الثاني من مرفقات رسوم استضافة مواقعهم وتُجنِّبهم استخدام مواقع الويب؛ لأن نموذج التصيّد والبرنامج النصيّ المستخدم لجمع البيانات مُضمَّنان بالكامل في الملف المرفق، الذي يمكن عند استخدامه موقع تصيّد، تخصيصه اعتماداً على الهدف المقصود وناقل الهجوم المستخدم لكسب ثقة الضحية. وبوسع المحتال، مثلًا، أن يوزع بريداً إلكترونياً تصيّدياً بين خبيث. وتحتوي «HTML» موظفي شركة ما، بحيث يبدو وكأنه يطلب التحقق من أحد العقود، ولكنه في الواقع ملف هذه المرفقات على جميع السمات المرئية لتلك الشركة: شعارها وشكل هويتها المرئية وحتى اسم أحد المسؤولين فيها، باعتباره مرسل رسالة البريد. ويُطلب من الضحية عند فتح الملف إدخال بيانات اعتماد الدخول (اسم المستخدم وكلمة المرور) إلى حساب الشركة، من أجل الوصول إلى المستند، فتقع هذه البيانات مباشرة في أيدي مجرمي الإنترنت الذين يمكنهم استخدامها لاقتحام الشبكة المؤسسية.