القرصنة والاختراقات في ظلّ فيروس كورونا

محمد معاذ

*** نُشرت هذه المقالة ضمن حملة "تنبّه" لتعزيز الوعي وثقافة الأمن السيبراني التي نظّمها المركز الإقليمي العربي للأمن السيبراني (ITU - RCC) – أبريل 2020**

بينما نحاول تجنّب الإصابة بفيروس "كوفيد 19" المعروف بكورونا، واتخاذ إجراءات للوقاية منه، يستغل القراصنة والمتسللون من كافة أنحاء العالم تفشي الوباء، ويحاولون اختراق حواسيبنا وهواتفنا ببرامج ضارة لهدف واحد هو: الحصول على المعلومات.

ويكشف المركز الوطني للأمن السيبراني في بريطانيا الشهر الماضي، عن مجموعة من الهجمات التي تُرتكب عبر الإنترنت، حيث يسعى القراصنة إلى استغلال فيروس كورونا لسرقة المعلومات من خلال جذب الضحايا بوعد الحصول على المعلومات ومتطلبات الحماية من الفيروس، ليصبح أحد التكتيكات الأكثر نمواً، وهذا ما تؤكده أرقام الشركة الأمنية "Zscaler" عن ارتفاع نسبة تهديدات القرصنة في ظل انتشار كورونا إلى 20% بعد أن كانت 15% شهرياً منذ بداية العام.

ويقول "ديبين ديساي" نائب رئيس البحوث الأمنية في "Zscaler" إنّ الشركة رصدت في شهر مارس الماضي قرابة 20000 حادثة من هجمات التصيّد الاحتيالي، والتي تقود إلى مواقع ويب زائفة لإدخال معلومات حساسة مثل كلمات المرور أو أرقام بطاقات الائتمان. كما تم العثور على أكثر من 7000 حادثة تم فيها خداع الضحايا لبدء تنزيل البرامج الضارة، والتي تضمّنت جميعها عبارات عن فيروس كورونا.

أنماط الاحتيال المتّصلة بفيروس كوفيد 19:

1. التصيد الاحتيالي (Phishing):

هي رسائل إلكترونية يُفترض أنها صادرة عن أجهزة وطنية أو هيئات صحية عالمية من أجل خداع الضحايا وحملهم على توفير معلومات شخصية، أو فتح ملفات تحتوي على برمجيات خبيثة.

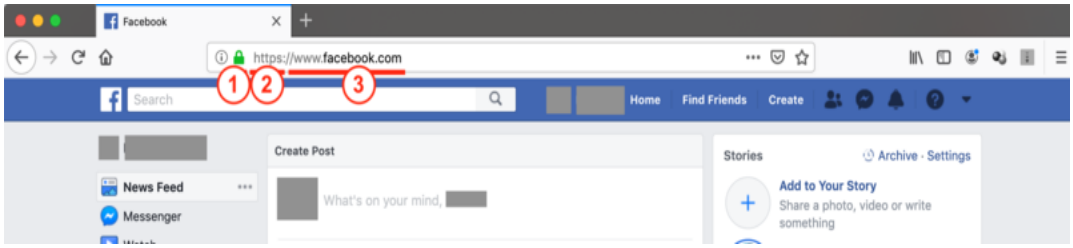
ويستخدم المحتالون رسائل بريد إلكتروني أو نصوص مزيفة لجعلنا نتشارك معلومات قيّمة مثل أرقام الحسابات أو معلومات عن تسجيل الدخول وكلمات المرور الخاصة بنا لسرقة هويتنا أو أموالنا، أو للوصول إلى جهاز الكمبيوتر الخاص بنا. وبمجرد النقر على الرابط، يمكن للقراصنة تثبيت برامج الفدية أو برامج أخرى يمكنها حجب بياناتنا وسرقة المعلومات.

ويعمل المحتالون على استخدام أسماء شركات مألوفة أو يتظاهرون بأنهم أشخاص نعرفهم. وأدناه، مثال عن عملية احتيال حيث انتحل القراصنة أنهم من منظمة الصحة العالمية (WHO):

بريد إلكتروني مزيف عليه شعار منظمة الصحة العالمية (Sophos Ltd)

أمّا عن كيفية منع التصيّد الاحتيالي، فالخطوة الأولى تكمن في التحقّق من المرسِل عن طريق فحص عنوان البريد الإلكتروني، ففي حال كان البريد من منظمة الصحة العالمية مثلاً، نتأكد من أن المرسِل لديه نطاق (Domain) بريد إلكتروني مثل "person@who.int" وإذا كان هناك أي نطاق خلاف "who.int" بعد الرمز "@"، فهذا يعني أن المرسِل ليس منظمة الصحة العالمية. وينبغي أن نكون مدركين أن المنظمة لا ترسل رسائل بريد إلكتروني من عناوين نطاقات تنتهي بـ "@who.com" أو "@who.org" أو "@who-safety.org".

وبالنسبة للروابط، يجب التحقق قبل النقر عليها، ولنتأكد أنه يبدأ ببروتوكول "https" وليس "http". كما يمكن الاستعانة بأداة موقع "فايروس توتال" (Virus Total) وهي خدمة لفحص وتحليل الملفات والروابط المشبوهة. أما المواقع التي قد تطلب كلمات مرور فقبل إدخال أي معلومات يجب التأكّد من وجود رمز القفل بجوار العنوان، وبروتوكول "https" والعنوان الصحيح للموقع الذي نرغب تسجيل الدخول إليه كما في المثال التوضيحي أدناه:



ولا بدّ من التشديد على عدم الاستعجال أو الشعور بالضغط، فالمتسللون والقراصنة يستغلون حالات الطوارئ والأخبار الساخنة لخداع ضحاياهم ولجعل الناس تتخذ القرارات بسرعة، لذلك فلنعمل على التفكير جيداً في أي طلبٍ للحصول على معلوماتنا الشخصية، وما إذا كان الطلب مناسبًا. أما في حال الاشتباه بتقديم معلومات حساسة إلى المجرمين الالكترونيين، فلا داعي للذعر، ولنقم على الفور بتغيير بيانات الاعتماد الخاصة بنا على كل موقع نستخدمها فيه.

2. السلع غير المستلَمة:

في ظل الظروف الراهنة، يدّعي البائعون عبر الإنترنت أن لديهم منتجات مطلوبة، مثل أدوات التنظيف والمستلزمات الصحية والطبية. وتشكّل المعدات الطبية المقلدة، وأقنعة الوجه، ومعقمات اليدين،

والمناديل وغيرها، محور اهتمام المجرمين الإلكترونيين، فقد نقدم طلبًا، لكن قد لا نحصل على شحنتنا أبدًا. ولنتذكر على الدوام أنه يمكن لأي شخص إنشاء متجر عبر الإنترنت تحت أي اسم تقريبًا بمن فيهم المحتالين.

لكن كيف نتصرّف؟

قبل اتخاذ القرار بأيّ عملية شراء، علينا التحقق بشكلٍ مستقل من الشركة أو الشخص الذي يعرض المستلزمات علينا، من خلال إجراء البحث عن اسم الشركة أو الشخص ورقم الهاتف وعنوان البريد الإلكتروني، بالإضافة إلى كلمات مثل "مراجعة" أو "شكوى" أو "احتيال". وإذا تحقّقنا من ذلك، يتم الدفع ببطاقة الائتمان على أن نحتفظ بسجل المعاملة أو الايصال. أمّا إذا كنا قلقين بشأن تسعير المنتجات، نبادر بالاتصال بمسؤولي حماية المستهلك في منطقتنا للتأكد من الأسعار.

3. **الجمعيات الخيرية الزائفة:**

عندما يقع حدثٌ صحي كبير كما نرى مع فيروس كورونا، قد يلجأ بعضنا للمبادرة بالمساعدة أوالتبرع وهذه نقطة يستغلّها المحتالون من خلال انتحال أسماء تشبه إلى حدَ كبير أسماء المؤسسات الخيرية الحقيقية. أما عمّا يجب القيام به فهو أن نقوم بالبحث عن الجمعيات الخيرية وإذا اعتقدنا أننا وقعنا ضحية عملية احتيال فلنتصل مباشرةً بالمصرف لوقف عملية الدفع.

لنغسل أيدينا ولنعمل على تحديث البرامج

صحيحٌ أنّ الاستعانة بمصادر المعلومات المتاحة عبرالانترنت أصبحت مرجعاً للحصول على الأخبار حول فيروس كورونا، لكن في المقابل هناك انتشار وتداول للبرمجيات الخبيثة التي تحاول الدخول إلى أجهزتنا وتعمد لسرقة البيانات الشخصية والمالية وغيرها من المعلومات القيّمة.

وطبعاً لن تكون المرة الأخيرة التي يحاول القراصنة والمتسللون من خداع ضحاياهم سواء في ظل تفشي الفيروس أو غيره. وأفضل طريقة للتصدي هو تحديث أجهزتنا لتصحيح الثغرات التي يحاول المتسللون استغلالها، والامتناع عن تنزيل أي برامج أو النقر على الروابط القادمة من أشخاص مجهولين أو لا نعرفهم، والإلتزام دائماً بمصادر موثوقة للحصول على المعلومات سواء عن الفيروس أو أي موضوع آخر قد نهتم بالبحث عنه.

*** نبذة عن الكاتب**

زميل سياسة Google وباحث في الذكاء الاصطناعي والأمن السيبراني وسياسات الانترنت.

كاتب تقني لدى "إم آي تي تكنولوجي ريفيو".

يرتكز عمله المهني على توفير المهارات الاستراتيجية لدعم وفهم الذكاء الاصطناعي.

خبير في التطوير المفاهيمي والتقني لحوادث الأمن الرقمي.

شغوف بالبيانات وعلوم OSINT، GEOINT و Fact Checking.