يجمع المحتالون بيانات الضحايا لتصميم عمليات استهداف محكمة (Getty)

تتفاقم جرائم المعلوماتية في أميركا، وتتزايد خسائرها عاما وراء عام، إذ بلغت 4,2 مليارات دولار خلال 2020، بزيادة 300% عن 2015، ويجمع المحتالون البيانات لتصميم عمليات استهداف بعضها عشوائي وأخرى محكمة ومعقدة

جرائم المعلوماتية في أميركا

احتيال عابر للحدود يستهدف الأفراد والشركات

واشنطن ـ **محمد الهواري**

تجاهلت المغربية المقيمة في ولاية فلوريدا الأميركية، فدوى سويني، رسالة تلقتها عبر بريدها الإلكتروني في 6 مارس/آذار الماضي من شخص، زعم أنه المسؤول عن «وحدة التفتيش التابعة للأمم المتحدة» بمطار هارتسفيلد جاكسون (أتلانتا الدولي)، قائلا: «وجدنا صندوقين كبيرين وبداخلهما 8 ملايين دولار، وعليهما اسمك وبريدك الإلكتروني، ونحن بحاجة لصورة هويتك وعنوانك وهاتفك لإيصالهما لك».

لم تقع سويني في شباك النصاب الإلكتروني، وعلى الفور حذفت الرسالة، إذ سبق وأن قرأت العديد من التحذيرات عن سرقة البيانات الشخصية، غير أن عديدين يقعون كل يوم ضحايا جرائم المعلوماتية، وهو ما يؤكد تلقي مكتب التحقيقات الفيدرالي 2000 شكوى يوميا، بحسب تقريره عن جرائم الإنترنت التي وقعت في عام 2020، والصادر في 17 مارس 2021.

سرقة البيانات

يستغل المحتالون بيانات الضحايا في تصميم عمليات استهداف مالية، وهو ما جرى مع اللبنانية سارة زيدان والتي تلقت رسالة عبر بريدها الإلكتروني في 17 أغسطس/آب 2020، تفيد بأنها قُبلت في وظيفة بمقر الأمم المتحدة الرئيسي في نيويورك، وبعد اجتيازها اختبارا ومقابلة عبر الإنترنت اتصل بها شخص من رقم أميركي ادعى أنه المسؤول عن ترتيب أمور إقامتها ونصحها باستئجار مسكن بدلاً من فنادق نيويورك باهظة الثمن، وعرض عليها ترتيب الأمر مقابل 4500 دولار. أثار هذا الطلب مخاوف والد سارة، لكنه رضخ لرغبتها وسط حماسها الكبير للوظيفة الأولى، بعد حصولها على ماجيستير إدارة الأعمال من الجامعة اللبنانية الأميركية في العام الماضي، وبالفعل صدقت توقعات الوالد، إذ اختفى المتصل والوظيفة عقب التحويل الذي فشل في إيقافه بعد إدراك الخدعة التي وقعوا فيها. لكن كيف وصل المحتال الإلكتروني إلى سارة؟ تجيب الضحية قائلة لـ«العربي الجديد»، «نشرت سيرتي الذاتية على مواقع إعلانات أميركية لإيجاد وظيفة، وما جعل الأمر مألوفا ودفعني للاستجابة أن الرسالة وصلت من بريد staffing@ngosocdev-un.org ورغم أنه مزيف لكنه بدا وقتها وكأنه حقيقي». في حالة سارة استهدفها المحتال بشكل محدد بعد حصوله على بريدها الإلكتروني المنشور في إعلانها، بينما يجمع آخرون بيانات من مواقع التواصل الاجتماعي لتصميم عملية نصب تلعب على احتياجات المستهدف، وفق ما يرصده خبير الأمن الإلكتروني عمار فيتور، والذي يميز بين النوع الأول الذي يقوم على خطة محددة، ونوع يقوم على إرسال رسالة إلى ملايين الأشخاص عشوائيا دون استهداف ضحية محددة، ومن ذلك رسالة تستهدف مساعدة في تحويل أموال عبر حساب المستلم في مقابل نسبة من المال، وعقب الوصول إلى بيانات الضحية المالية والشخصية تجري سرقة حسابه.

4,2 مليارات دولار خسائر مالية ناجمة عن الجرائم المعلوماتية في 2020

2000 شكوى متعلقة بجرائم الإنترنت يتلقاها مكتب التحقيقات الفيدرالي يوميا

شركات الضمان وعدم تسليم المشتريات

يعدّ إتمام عمليات مالية عبر شركات الضمان المالي «Escrow» أمرا شائعا في أميركا وخاصة في عمليات البيع والشراء عبر الإنترنت، إذ تضمن هذه الشركات وصول الأموال لشخص أو شركة عبر تعاقد الأطراف معها لتتعامل نيابة عنهم، وهو ما فتح بابا جديدا لمحتالين يؤسسون شركات يضيفون كلمة «Escrow» لاسمها، للادعاء بأنها شركة ضمان، في ظل سهولة إنشاء هذا النوع من الشركات، إذ تقر جميع الولايات، منذ عام 1996 إنشاء الشركات الصغيرة ذات المسؤولية المحدودة LLC بعد ما خضع هذا النوع لقانون الضرائب، بحسب منظمة Better Business Bureau، (خاصة مقرها فيرجينيا تقيم مصداقية الشركات).

وتؤكد المنظمة ردا على أسئلة «العربي الجديد» أن النصب من قبل شركات صغيرة يزعم مالكها بأنها شركة ضمان مالي في تزايد، وخاصة في عمليات بيع السيارات المستعملة. وهو ما وقع للسورية ريم رضوان والتي استعانت بموقع Craigslist (شبكة إعلانية عبر الإنترنت) لشراء سيارة، ووجدت إعلانا لبيع سيارة تويوتا كامري موديل 2017 بسعر 5000 دولار في مدينة ريتشموند بولاية فيرجينيا، رغم أن ثمنها الأصلي يصل إلى 10 آلاف دولار. وتواصلت ريم عبر البريد مع المعلنة التي ادعت ان اسمها لورا وأنها مجندة في الجيش وعليها أن تلتحق بوحدتها في ألمانيا سريعا، لذلك اضطرت لبيع السيارة بهذا السعر موضحة أنها موجودة في مدينة أوستن بولاية تكساس، وعرضت على ريم وضع ثمن السيارة في حساب بنكي لشركة ضمان مالي تتولى إيصاله لها، إلى أن يتم شحن السيارة. وبالفعل حولت ريم المبلغ إلى حساب الشركة، لكن اختفت البائعة والسيارة.

ما حدث مع ريم يرجع إلى أنها لم تقرأ التحذيرات المتكررة على موقع Craigslist، بأن يتم إجراء عمليات الشراء بشكل مباشر، لأن الكثير من الإعلانات المبوبة وهمية، ما أسفر عن وقوعها في شباك المحتالة، موضحة أنها قدمت بلاغا للمباحث الفيدرالية وما تزال في انتظار الرد. وتكرر ما حدث لريم مع تاجر السيارات السعودي بلال البقعاوي والذي شاهد إعلاناً على إنستغرام لبيع سيارة مرسيدس 2021/G63 بسعر جيد، فتواصل مع الشركة المعلنة والتي تدعى wulf export وزعمت أن مقرها في سان دييغو، وأرسلت للبقعاوي مستندات عمل تذكر أنها تصدر مئات السيارات لدول مختلفة، ما دعاه إلى الإقبال على التعامل معهم وتحويل 150 ألف دولار لحساب الشركة لكن لم تصله السيارة رغم مضي 7 أشهر.

وعبر تتبع مكتب الشركة في كاليفورنيا وجد معدّ التحقيق أنها من نوع المسؤولية المحدودة، (لا تزيد تكلفة إنشائها على 100 دولار)، وتمتلك موقعا على الإنترنت ولكنها لا تمتلك أي مكان لعرض أو بيع السيارات.

شيكات بنكية مزوّرة

تعرض سمسار العقارات في لوس أنجليس محمد بابكر، للنصب من قبل محتال ادعى أنه مستثمر عرف نفسه باسم كريغ تواصل معه عبر موقع Craiglist، طالبا منه تجهيز قائمة بالمنازل الملائمة والمعروضة للبيع ومتوسط سعرها بين نصف مليون ومليون ونصف المليون دولار، في مقابل أن يدفع لبابكر 125 دولارا في الساعة نظير خدماته، وبالفعل تلقى بابكر شيكا مقبول الدفع بقيمة 5 آلاف دولار من كريغ، وأودعه في حسابه، ليصل إليه شيك آخر في اليوم التالي بقيمة 9 آلاف دولار وطلب منه كريغ إيداعه في حسابه أيضا من أجل تأجير منزل للإقامة فيه بعد أن يصل إلى لوس أنجليس لتفقد المنازل، لكن بابكر تلقى بريدا من كريغ بأنه مضطر للذهاب إلى كندا طالبا منه أخذ أتعابه من المبالغ التي وصلت إليه وتحويل الباقي له عبر ويسترن يونيون في كندا كونه لا يمتلك حسابا بنكيا هناك. وبالفعل قام بابكر بتحويل 7000 دولار إلى كريغ وأرسل له صورة إيصال التحويل، حينئذ اختفى وتوقفت وسائل التواصل معه بمجرد سحب المبلغ من ويسترن يونيون.

بعد 3 أيام تلقى بابكر اتصالا من البنك يخبره أنه لم يستطع تحصيل الشيكين المصرفيين المودعين. وتوضح كارولين رمبرغر المدير السابق لبنك «رجز» Riggs PNC بواشنطن أن الشيك بعد إضافته إلى رصيد العميل، يقوم البنك بتحصيله من البنك الصادر عنه، خلال فترة من خمسة إلى تسعة أيام، وفي هذة الفتره يعمل المحتالون على إقناع ضحاياهم بأن يرسلوا لهم جزءا كبيرا من مبالغ الشيكات عن طريق ويسترن يونيون أو موني غرام، وبعد اكتشاف أمر الشيكات المزورة يكون الوقت قد فات والضحية أرسل الأموال للمحتال، ولا تتوقف الخسائر عند هذا الحد، إذ يفرض البنك مصاريف التحصيل علي الضحية.

الفدية الرقمية

بلغت الأضرار الناجمة عن الجرائم الإلكترونية المبلغ عنها عنها 4,2 مليارات دولار في عام 2020، بعد أن كانت مليار دولار عام 2015، بحسب تقرير مكتب التحقيقات الفيدرالي، وتكبد الضحايا الذين تزيد أعمارهم عن 60 عامًا ما يقرب من 28% من إجمالي خسائر الاحتيال، ما أدى إلى ضياع مليار دولار تعود لكبار السن. ويمثل الرقم السابق زيادة بنحو 300 مليون دولار مقابل ما أبلغ عنه الضحايا الذين تجاوزوا الستين من عمرهم في عام 2019. وتتفاقم مخاطر تلك الجرائم التي تهدد أعمال الشركات الأميركية، إذ اعتقل مكتب التحقيقات الفيدرالي في الثاني من يونيو/ حزيران 2021 المواطن النيجيري تشارلز أونوس والذي حاول تنفيذ عمليات اقتحام إلكترونية لـ 5500 حساب لشركات تتعامل مع مؤسسة تقدم خدمات الموارد البشرية لأصحاب العمل في أميركا، بهدف سرقة ودائع رواتب قيمتها 800000 دولار.

وأدين 11 شخصا بارتكاب جرائم معلوماتية خلال يونيو 2021، بينما تم توقيف 11 متهما آخرين، بالإضافة إلى كشف شبكة Dark Side Group التي بلغ عدد المتضررين من الهجوم الذي نفذته 90 شخصا، وبلغت الخسائر المالية الناجمة عن الجرائم المرتكبة عبر الإنترنت خلال ذات الشهر 74 مليونا و477 ألف دولار. وفقا لرصد أجراه «العربي الجديد» عبر تتبع بيانات منشورة على الموقع الإلكتروني لمكتب التحقيقات الفيدرالي. ويعتبر البروفيسور جون سنسيش، والذي عمل سابقا في المباحث الفيدرالية ومدير مركز بنسلفانيا لعلوم التحقيق والطب الشرعي أن الحكومة لا تقوم بعمل كاف لإيقاف جرائم الإنترنت، ولم يجر تطوير تطبيقات للمساعدة على تنبيه المستهدفين لعدم الوقوع في شراك المحتالين. ويزيد اتساع المدى الجغرافي للجرائم الإلكترونية أمر مكافحتها تعقيدا، فلا تستطيع ولاية واحدة مجابهتها، كما أن القانون الفيدرالي الخاص بجرائم الإنترنت رقم 18 1030.U.S.C لا يردع النصابين وفقا لسنيش، لذلك ترتفع أعداد الضحايا خلال الأعوام الماضية.