PRESS CLIPPING SHEET

PUBLICATION:	**Al Amwal**
DATE:	**20-June-2021**
COUNTRY:	**Egypt**
CIRCULATION:	**5,000**
TITLE:	**Group-IB Reveals a Large-Scale, Multi-Phased Scam Attack Targeting the Middle East and Africa**
PAGE:	**Back Page**
ARTICLE TYPE:	**Agency-Generated News**
REPORTER:	**Ali Kenawy**
AVE:	**7,750**

«Group-IB» تكشف عن موجة احتيال متعددة المراحل تستهدف منطقة الشرق الأوسط وأفريقيا

مصر من بين أكثر خمس دول مُستهدفة وفقًا للتحليلات المطروحة في مؤتمر "آي جروب" للمخاطر الرقمية 2021

كتب - على قناوى

كشفت "جروب - آي بي" (Group-IB)، الشركة العالمية الرائدة في مجال التصدي للتهديدات الإلكترونية واستقصاء بيانات ومعلومات التهديدات الإلكترونية والتحقيق بالجرائم الإلكترونية المتقدمة وكشفها النقاب عن موجة احتيال متواصلة واسعة النطاق تستهدف منطقة الشرق الأوسط وأفريقيا، إذ تم فيها استغلال ما يقرب من 140 علامة تجارية مشهورة في 16 دولة في المنطقة من قبل المحتالين الذين أنشأوا صفحات مزيفة بهدف سرقة معلومات المستخدمين الشخصية وبيانات الدفع الخاصة بهم - وفقًا للمعلومات، فإن ما لا يقل عن ثمان علامات تجارية مُستغلة في موجة الاحتيال متعددة المراحل هذه تعود إلى جمهورية مصر العربية.

ولقد أصدرت هذه النتائج، التي تم الحصول عليها بمساعدة منصة تحديد المخاطر الرقمية وتخفيف حدتها الموجهة بتقنيات الذكاء الاصطناعي التي تحمل اسم نظام الحماية من المخاطر الرقمية والمقدمة من جروب - آي بي، أثناء انعقاد مؤتمرها "جروب-آي بي" للمخاطر الرقمية 2021 (Group-IB's Digital Risk Summit 2021) عن بُعد الأسبوع الماضي ولقد شملت قائمة المشاركين في هذا المؤتمر "مركز الحوسبة الدولي التابع للأمم المتحدة" (UNICC)، والشركة العالمية في أبحاث السوق والاستشارات "فوريستر" (Forrester)، إضافة إلى "سكام أدفايزر" (Scamadviser)، وهو عبارة عن مشروع مستقل متخصص في تقديم خدمات مراقبة المواقع الإلكترونية وخلال فعاليات المؤتمر، أشار محللو المجموعة أيضًا أن مصر واحدة من أبرز خمس دول التي تستهدفها موجة الاحتيال المتواصلة ومتعددة المراحل.

يقوم المحتالون في هذه العملية بإنشاء صفحات إلكترونية مـزورة، ليتلقى الضحية النموذجي بعدها رابطًا إلكترونيًا، إما عبر قنوات وسائل التواصل الاجتماعي أو من خلال تطبيق للمراسلة، أو قد يُصادف إعلانًا في محركات البحث يدعوه للمشاركة في السحب على جوائز أو الحصول على عروض ترويجية أو ملء استبيان يرتبط بعلامة تجارية مشهورة أو باسم أحد المشاهير. تتضمن الصفحة الإلكترونية التي يصل إليها الضحية نموذجًا إلكترونيًا مُصممًا لاستخراج التفاصيل الشخصية الرئيسية المتعلقة به، وبمجرد القيام بتعبئة النـموذج، يجد الضحية نفسه فائزًا بالجائزة ويُطلب منه بعدها مشاركة الرابط مع جهات الاتصال لديه. وبعد أن يُوسّع الضحية سطح الاحتيال، يُعاد توجيهه إلى موارد احتيال أخرى، كهدايا جديدة أو مواقع للتصيُّد الاحتيالي أو مواقع قد تُعرّض أجهزة المستخدم لخطر الإصابة ببرامج ضارة. وقد بلغ العدد الإجمالي الشهري للجمهور المستهدف كمرحلة أخيرة في العمليات الاحتيالية حوالي 500,000 شخص.

إن غالبية العلامات التجارية المستهدفة عبر موجة الاحتيال متعددة المراحل هذه تنتمي إلى قطاع الاتـصـالات بنسبة بلغت 34.8%، في حين تمثل 10.4% منها خدمات عامة و9.6% تنتمي لقطاع البيع بالتجزئة. وتشمل القطاعات الأخرى المتأثرة كلاً من قطاع الترفيه، والوجبات السريعة، والسيارات، والإلكترونيات، وقطاعي النفط والغاز، والخدمات المصرفية والتـأمين إلـى جانب ذلـك، اكتشف المحللون لدى المجموعة أكثر من 4300 صفحة إلكترونية احتيالية مسجلة باستخدام خدمات نشر مدونات مشروعة هذا العام فقط، منها 160 صفحة احتيالية تستغل علامات تجارية مصرية

أدّت الحاجة إلى دفع الشركات باتجاه التحول الإلكتروني، إذ تبلغ نسبة صفقات المشتريات التي تتم عبر قنوات وسائل التواصل الاجتماعي 40% في الوقت الحاضر. وهذا يُمثل نموًا غير مسبوق، لكنه أدّى في الآن ذاته إلى مضاعفة مستوى التهديدات. وبالمجمل، تشكّل عمليات الاحتيال 73% من إجمالي الهجمات الإلكترونية 56% منها عبارة عن عمليات احتيال تجذب الضحايا وتدفعهم إلى الكشف طوعًا عن بيانات حساسة، ومنها 17% هجمات تصيُّد احتيالي تُفضي في نهاية المطاف إلى سرقة تفاصيل البطاقة المصرفية.

وبهذا الصدد، يتحدث أشرف كحيل، مدير عام وحدة تطوير الأعمال في الشرق الأوسط وأفريقيا لدى "جروب - آي بي" قائلاً: "لا تستطيع المؤسسات التعامل مع هذا الوباء الاحتيالي من خلال نهج المراقبة الكلاسيكية وحظر الروابط بشكل فردي، فحجم النشاط الاحتيالي آخذ في الازديـاد. الأمر الذي من شأنه أن يفرض متطلبات جديدة للأدوات المصممة لمكافحته ينبغي أن تكون أنظمة الحماية من المخاطر الرقمية الشاملة قادرة على اكتشاف جميع مكونات البنية التحتية التي يضعها المحتال ورؤية جميع العناصر المتعلقة بها. وإن النهج المتمحور حول المحتالين، على غرار النهج الذي تتبعه "جروب - آي بي" يُثري نتائج المراقبة ويجعل عملية المراقبة أكثر تطورًا وتعقيدًا وقابلية للتوسع".

وأشارت "جروب - آي بي" التي فتحت مؤخرًا أبواب مركزها الأول المتخصص بجمع المعلومات وإجراء الأبحاث بشأن التهديدات الإلكترونية في منطقة الشرق الأوسط وأفريقيا، أن عمليات الاحتيال والتصيُّد الإلكتروني التي اكتشفتها الشركة في الشرق الأوسط قد ازدادت بنسبة 27.5% في عام 2020، مقارنة بالعام السابق. ولقد قدّمت أيضًا تحليلات مُستمدة من العديد من مخططات الاحتيال الأخرى التي تم الكشف عنها باستخدام نظام "استقصاء العمليات الاحتيالية" (SCAM Intelligence)، ففي عام واحد فقط، ساعد النظام في توفير ما يصل إلى 443 مليون دولار للشركات في منطقة آسيا والمحيط الهادئ وروسيا وأوروبا والشرق الأوسط من خلال منع الأضرار المحتملة المرتبطة بالعمليات الاحتيالية.