

منصة الكترونية : احذروا الاختراق الصهيوني لمستخدمي منصات التواصل العرب برعاية إماراتية!



الأحد 11 يونيو 2023 08:47 م

كشفت منصة إيكاد أكبر اختراق أمني "صهيوني" للمستخدمين العرب عبر إعلانات موجهة على منصات التواصل الاجتماعي، الاختراق الإسرائيلي يتم عبر شركات تملك غطاءً إماراتياً قانونياً من خلال شركات استثمار رقمية موثقة في الإمارات

وأثبتت (إيكاد) أن منصتي "Evest" و "Mister Market Pro" تعملان ضمن شبكة ضخمة من العلامات التجارية يديرها رجال أعمال "إسرائيليون"، تحاول اختراق أجهزة المستخدمين المتواجدين في قطر والخليج للحصول على معلوماتهم الحساسة

وأكدت أن هذه المجموعة (المنصتين) التي كشفت عنها ما هي إلا جزء من شبكة أكبر بكثير من عمليات اختراق إسرائيلية تستمر إيكاد في تتبعها لتكشف عنها تباطؤاً

إعلانات كثيفة

ولاحظ محققي إيكاد موجة إعلانات كثيفة تروج لمنصات استثمار وتداول، أبرزها شركتا "Evest" و "Mister Market Pro" اللتان ظهرتتا خلال الأشهر الماضية بشكل زخم في يوتيوب وتويتر وفيسبوك
وأضافت أن الإعلانات في الوهلة الأولى بدت طبيعية، ومقنعة، فهي تعتمد على بعض الوجوه الإعلامية المعروفة مثل "محمد السويدان" و"مهند الوادية"، وهم أسماء تظهر بكثرة في قنوات تلفزيونية معروفة مثل MBC وCNBC العربية
وأوضحت أن منصات التداول المشبوهة EvestOfficial@ و MisterMarketPro@ تظهر بشكل متكرر في عدة صحف إماراتية مثل UAE Times وموقع Zawya، وتم تصدير المنصة ذاتها في مؤتمرات عديدة بدبي مثل Crypto Expo Dubai و Forex Expo Dubai 2021.

وأوضحت أنه بالبحث عن "Evest" فإن المنصة وبحسب مؤسسة "Cyprus Securities and Exchange Commission" المعنية بمراقبة المشاريع التجارية ومصداقيتها في قبرص، تعد "غير آمنة" ويتم استخدامها لأعمال غير قانونية ولا يوجد لها سجل قانوني

وصفحة منصة الاستثمار "Evest" تحذر زائريها بأن خدماتها غير موجهة لسكان ومواطني أمريكا وكندا وروسيا وإسرائيل والاتحاد الأوروبي ودول أخرى، وذلك بسبب إيقاف خدماتها في دول الاتحاد الأوروبي حسب تقارير إعلامية سابقة
واشارت إيكاد أنه من خلال تحليل روابط الإعلانات لمنصة التداول الأولى "Evest"، اكتشفنا وجود برامج اختراق متطورة يصعب كشفها في أجهزة المستخدم، تعمل على جمع المعلومات من الجهاز المخترق وإرسالها لعدة جهات فور دخول المستخدم للرابط

وحذرت من أن رابط الإعلان يقوم بتمرير بيانات المستخدم الذي تم اختراق جهازه على عدة خوادم حول العالم، أحدها موجود في روسيا، وآخر في إسرائيل

ميستر ماركت

وأشارت إيكاد ثانياً إلى منصة التداول "Mister Market Pro" والتي تقدم دورات مجانية لتعليم أسس الاستثمار للجميع، فتستخدم رابط إعلانات يحتوي على عدة برامج ضارة تُستخدم جميعها لسرقة بيانات الحسابات المصرفية والمعلومات الشخصية من جهاز المستخدم

وأبانت أن هذه المعلومات الأولية دفعتنا للبحث حول مُلاك منصتي "Evest" و" Mister Market Pro"، والنتائج كانت غير متوقعة. وبالبحث عن شركة "Evest"، وجدنا أنها علامة تجارية تملكها شركة "Atriafinancial Holdings LTD" المسجلة في بريطانيا، ويرأسها شخصان، أحدهما يُدعى "محمد شيخ سليمان" يحمل الجنسية الإسرائيلية. وترتبط أيضا بشركة أخرى تُدعى "Evest Ltd" مُسجلة في قبرص ويديرها كذلك رجل الأعمال الإسرائيلي "Nir Menashe". وقالت إنه بالبحث عن الشركة الأخيرة "Evest Ltd"، وجدنا أنها ترتبط بشركة "Leadcapital Holdings LTD" التي بدورها تدير "Mister Market Pro"، العلامة التجارية التي تستهدف قطر بإعلانات موجهة كما ذكرنا سابقاً. وذكرت أن شركة "Leadcapital Holdings LTD" هي في الحقيقة غطاء لمجموعة "Lead Capital Holding (TCH) Limited" التي يرأسها ويملكها الإسرائيلي "Roi Gavish".

وتوصلت إلى أن الخلاصة "أنا أمام شبكة شركات معقدة، أظهر تحليلها جميعاً أنها ترتبط برجال أعمال إسرائيليون".

الرعاية الإماراتية

وحذرت المنصة المستخدمين العرب من أن اللافت للنظر أن نشاطات مجموعة "Lead Capital Holding (TCH) Limited" مُصرح لها في الإمارات بشكل قانوني، ويُسمح لشركاتها "منصات الاستثمار" بتقديم دورات مجانية داخل الإمارات كذلك.

وأضافت أن "لدى مجموعة "Lead Capital" التي يديرها الإسرائيلي "Roi Gavish" ارتباط بشركات تقوم بالخدع ذاتها لاختراق المستخدمين من خلال منصات تداول مُرَوَّجة".

وأن شركة "Tplus Technologies" أسسها "Roi Gavish" وكلا الشركتين تقدمان الخدمات المالية ذاتها على الإنترنت وتعملان معاً. موضحة أن لدى مجموعة "Lead Capital" التي يديرها الإسرائيلي "Roi Gavish" ارتباط بشركات تقوم بالخدع ذاتها لاختراق المستخدمين من خلال منصات تداول مُرَوَّجة.

وذكرت أن "Roi Gavish" عمل سابقاً في شركة "PlayTech" مع شخصية إسرائيلية أخرى وهي "Bat-El Azerad"، والتي تعمل الآن مديرة تنفيذية في شركة "NovoShield" الإسرائيلية المختصة بتقديم "الحلول السيبرانية".

تداخل خبرات

وعن حسابات @NovoShield_Pro و @BatElNovoShield قالت إيكاد إن الحساب الأول (بحسب تحقيقات سابقة) يتبع شركة "إسرائيلية" تقدم حلولاً استخباراتية لاختراق الأجهزة والاتصالات للجهات الأمنية والعسكرية والحكومات.

نمط إعلاني

وربطت المنصة الاللكترونية المتخصصة في كشف الاختراق الصهيوني عبر شبكات التواصل الاجتماعي أن نمط الإعلانات الذي قمنا بكشفه يتشابه مع نمط تتبعه الاستخبارات الإسرائيلية في تجنيد عناصر من خلال إعلانات موجهة عبر وسائل التواصل الاجتماعي. وقالت: "تقوم الاستخبارات بضخ إعلانات عن وظائف بمرتبات عالية، تستهدف الطبقة البسيطة "المحتاجة" من المواطنين العرب، وفي حال تقدّم أحدهم للحصول على هذه الوظيفة يعرضون عليه تجنيده في الموساد الإسرائيلي".

وأردفت أن قوى الأمن الداخلي في لبنان مطلع عام 2022 تمكنت من القبض على شبكة عملاء لدى الموساد تم تجنيد أحد عناصرها من خلال إعلان بمنصة فيسبوك لوظيفة في قطر، بحسب تقارير سابقة.

وأكدت أنه طلب من العميل بعد تجنيده تحميل أحد البرامج وعمل مسح لأي شبكة إنترنت "واي فاي" يستطيع الدخول عليها، وهذا يتشابه مع طريقة عمل تلك الإعلانات بحسب التحقيقات التي رصدتها (إيكاد).

وتابعت المنصة أن "استخدام إعلانات للاستثمار وتقديم وعود بالثراء المالي أو تقديم عروض وظيفية بمرتبات عالية لم يكن عبثاً، فإسرائيل تحاول بهذه الحملات إغراء المستخدمين بالمال لتجنيده، ولا يمكن معرفة كم الأشخاص الذين خدعتهم الإعلانات وتم تجنيدهم بالفعل حتى الآن".

<https://twitter.com/EekadFacts/status/1667569338830692352>