

كيف استخدم قراصنة إيرانيون حيلة "المرأة الجميلة" لاصطياد أهدافهم؟

كتبه دوستين فولز | 2 أغسطس, 2017



ترجمة حفصة جودة

أفاد أحد الأبحاث أن قراصنة يُعتقد أنهم يعملون لصالح الحكومة الإيرانية انتحلوا شخصية مصورة شابة على وسائل التواصل الاجتماعي لأكثر من عام، بهدف إغراء الرجال الذين يعملون في صناعات استراتيجية مهمة لخصوم طهران الإقليميين.

قال الباحثون في شركة "Dell SecureWorks" إن شخصية المدعوة ميا آش كانت نشطة على مواقع من ضمنها لينكد إن وفيسبوك وواتساب وبلوجر منذ شهر أبريل العام الماضي.

أظهرت الحملة أن إيران تشارك في مؤامرة هندسية اجتماعية لتحقيق أهدافها من خلال "مصيدة مخترقي الشبكات" (هوني بوت) وهي طريقة قديمة للتجسس تتضمن الإغواء كما أنها أكثر شيوعًا بين القراصنة الإجراميين.

البرامج الضارة المعروفة باسم "PupyRAT" تمنح المهاجم التحكم الكامل في جهاز الحاسب المُخترق

لاحظت "Dell SecureWorks" أن ميا أرسلت برامج ضارة معينة مخفية في المرفقات كأنها مسح

فوتوغرافي لأحد الضحايا، وهي تتطابق مع برامج ضارة أرسلها مجموعة قراصنة إيرانيين تُسمى “Cobalt Gypsy” في محاولة غير ناجحة لاختراق البريد الإلكتروني لنفس الضحية (صاحب العمل) في يناير الماضي.

هذه البرامج الضارة المعروفة باسم “PupyRAT” تمنح المهاجم التحكم الكامل في جهاز الحاسب المُخترق وإمكانية الوصول إلى أوراق اعتماد الشبكة وفقاً لما يقوله التجسس الحكومي، لكن الباحثين لم يتمكنوا من معرفة كيف اخترقت الأهداف وما الذي جنته ميا من الوصول إلى تلك الأجهزة.

تؤمن شركة “Dell SecureWorks” أن شخصية “ميا” صنعها وشغلها مجموعة من القراصنة الإيرانيين

استخدم الملف الشخصي المزيف صورًا متاحة للعمامة على وسائل التواصل الاجتماعية لمصورة حقيقية من أوروبا الشرقية، حيث خلقوا شخصية وهمية جذابة لامرأة في منتصف العشرينيات تعيش في لندن وتستمتع بالسفر وكرة القدم وتسمع للموسيقيين المشهورين مثل إيد شيران وإيلي غولدنغ، أما سيرتها الذاتية على وسائل التواصل الاجتماعي فيبدو أن تفاصيلها منقولة من ملف شخصي على لينكد إن لمصور من نيويورك.

تؤمن شركة “Dell SecureWorks” أن شخصية ميا صنعها وشغلها مجموعة من القراصنة الإيرانيين يعملون تحت اسم “Cobalt Gypsy”، وحتى الآن لم يرد المسؤولون الإيرانيون على طلب التعليق على هذا الأمر.

أغرت ميا آش رجلاً في منتصف العمر يعملون كفنيين أو مهندسين في شركات الغاز والبتروك والفضاء وكذلك شركات الاتصالات في الشرق الأوسط، وكانت مجموعة القراصنة الإيرانيين قد استهدفت الأشخاص من قبل، هؤلاء الأشخاص يعملون في المملكة العربية السعودية و”إسرائيل” وكذلك الهند والولايات المتحدة الأمريكية.

يقول أليسون ويكوف باحث أمني كبير في شركة “Dell SecureWorks” والذي تتبع نشاط ميا آش إن جميع ضحاياها فشلوا في ملاحظة أن ملفها الشخصي لا يتضمن أي طريقة للتواصل معها بشأن خدماتها الفوتوغرافية.

اعتبر مسؤولون في الأمن الغربي منذ سنوات أن إيران من بين أكثر الخصوم السبيرانيين تطوراً

ويضيف ويكوف “هؤلاء الأشخاص لم يتعاملوا معها من أجل التصوير، كان الشيء الرئيسي الذي جذبهم أنها صغيرة ولطيفة وتحب السفر، إنهم يعتقدون أنها غريبة الأطوار، كانت لينكد إن قد

حذفت ملف ميا آش الزيف قبل أن تنهي الشركة تحقيقها، أما على فيسبوك - حيث كتبت ميا آش أنها في علاقة معقدة - فقد حذفت الإدارة ملفها الشخصي بعد التواصل مع الشركة.

كانت "Cobalt Gypsy" المعروفة أيضًا باسم "OilRig" قد أتهمت سابقًا بإدارة شبكة من الملفات الشخصية الوهمية على لينكد إن وتظاهروا بأنهم شركة للتوظيف في الشركات الكبيرة ومن ضمنها "Northrop Grumman Corp" و"General Motors Co"، لكن شخصية ميا آش أظهرت مستوى عالٍ من المثابرة.

كان مسؤولون في الأمن الغربي قد اعتبروا منذ سنوات أن إيران من بين أكثر الخصوم السيبرانيين تطورًا في الدول القومية جنبًا إلى جنب مع روسيا والصين وكوريا الشمالية.

قال تقرير آخر نُشر هذا الأسبوع لباحثين بشركة "Trend Micro" في طوكيو و"ClearSky" في "إسرائيل" إن الجهود المبذولة لانتحال شركات تكنولوجيا كبيرة مثل تويتر ومايكروسوفت تقوم بها مجموعات قرصنة أخرى يُشتبه في أن لها علاقة بإيران.

المصدر: رويترز

رابط المقال : [/https://www.noonpost.com/19171](https://www.noonpost.com/19171)