كيف غرق الألمان في كوابيس الجرائم الإلكترونية؟

كتبه مارتين بيرنشتاين | 18 أكتوبر, 2017

ترجمة وتحرير: نون بوست

في الواقع، ترتكب العديد من الأجهزة الإستخباراتية في الشرق الأوسط جرائم إلكترونية في حق شركات ألمانية كبرى. وقد يصل الأمر إلى الابتزاز الرقمي والاستيلاء على اللوحات الإشهارية الإلكترونية داخل محطات القطار، فضلا عن جرائم الاحتيال التي تحدث في صلب شبكات بعض الشركات. وفي هذا الصدد، أفاد العديد من الخبراء أن شركتين من أصل ثلاث شركات ألمانية تتعرض للجرائم الإلكترونية.

مؤخرا، اكتشف معرض ميونخ الدولي وجود "فجوة في السوق" على مستوى الأمن الإلكتروني. وفي الأثناء، تقرر تنظيم المؤتمر الدولي للأمن الإلكتروني تحت مسمى "كوماند كنترول" خلال السنة القادمة. والجدير بالذكر أن هذا المؤتمر سينظم على طريقة المؤتمر الأمني السنوي بمدينة ميونيخ. وفي هذا السياق، صرح رئيس معرض ميونخ الدولي كلاوس ديتريش، أن "تقنية المعلومات في السابق كانت مسألة بسيطة، أما اليوم فقد أصبحت العديد من الشركات تعتمدها".

في الحقيقة، لا يمكن اعتبار الحواسيب أو الموظفين في الشركات بمنأى عن أيدي المخترقين وعمليات القرصنة. وفي هذا الإطار، تسجل الوكالة الألمانية للشبكات في بايرن 40 ألف محاولة قرصنة بشكل يومي. وفي شهر أيار/مايو الماضي، أثار هجوم "وانا كراي" الإلكتروني جدلا واسعا، حيث امتد فيروس الفدية إلى حواسيب مطار مدينة ميونيخ. وقد تم التصدي لهذا الفيروس قبل أن يحدث أضرار

حقيقية بالحواسيب. وعلى خلفية ذلك، تقرر إحداث مركز دفاع إلكتروني بالمطار المذكور آنفا، مع العلم أنه سيكون جاهزا بحلول شهر كانون الثاني/يناير المقبل.

في المقابل، لن تتمكن الشركات الصغرى من إحداث مراكز دفاع إلكتروني مشابهة. ففي الواقع، غالبا ما تكون هذه الشركات واثقة من أن طلبات الشغل الجذابة التي تصلها عبر البريد الإلكتروني، ستمنحها دون شك موظفا جديدا يتمتع بقدرات هائلة. في المقابل، يقع العديد من رؤساء الشركات في فخ الضغط على ملفات خبيثة دون التفطن إليها .ويؤدي ذلك في معظم الحالات إلى تسرب برمجيات خبيثة تشفر النظام الأساسي للحاسوب. وبالتالي، تضطر الشركات إلى التعامل مع المخترقين من خلال عملة البيتكوين الرقمية خشية ضياع البيانات.

ومن المثير للاهتمام أنه وفي سنة 2015، سجلت شرطة مدينة ميونيخ 91 جريمة إلكترونية، علما وأن عدد الجرائم من هذا النوع بلغ 151 جريمة في سنة 2014. وحيال هذا الشأن، صرح خبراء لدى مديرية الأمن أن "الأمر الملفت للنظر في هذا الصدد يتمثل في طرق التشفير التي أصبحت أكثر تعقيدا ".

> تطلق الشرطة الإلكترونية اسم "احتيال الرؤساء التنفيذيين" على جرائم الاحتيال التي يقوم بها الرؤساء التنفيذيون عن طريق موظفيهم

من جانب آخر، أصدرت مديرية الأمن بميونيخ تقريرا أمنيا تطرقت من خلاله إلى الهجوم الذي تعرض له مستشفى بالمدينة، وذلك عن طريق برمجية "حصان طروادة" الخبيثة. وقد وقع تشفير العديد من البيانات المسجلة في الخادم الخاص بالمستشفى، ومن بينها معطيات تتعلق بالمرضى. وفور التفطن لعملية القرصنة، تم غلق الحاسب الخادم، في حين تمكنت مصلحة الإعلامية بالمستشفى من استرجاع البيانات بفضل نظام حماية فعال.

خلال مؤتمر الأمن الرقمي الذي سينظمه معرض ميونخ الدولي، سيلعب العامل البشري دورا هاما بالإضافة إلى الجانب التقني. وفي هذا الإطار، أورد منظم المعرض أن "سلامة البيانات أصبحت مهمة تماما مثل نظافة اليدين في ظل انتشار موجة الفيروسات. وسنحاول إقناع زوار مؤتمر " "كوماند كنترولّ" بذلك".

في سياق متصل، تطلق الشرطة الإلكترونية اسم "احتيال الرؤساء التنفيذيين" على جرائم الاحتيال التي يقوم بها الرؤساء التنفيذيون عن طريق موظفيهم .في الواقع، يبادر الرئيس التنفيذي لإحدى الشركات ببعث رسالة إلكترونية لأحد موظفيه يأمره من خلالها بتحويل مبلغ كبير من المال من حساب الشركة بشكل سريع قصد تمويل مشروع سري. وفي سنة 2016، سجلت مديرية الأمن بميونيخ قرابة 79 جريمة من هذا النوع، علما وأن عدد الجرائم قد يكون أكثر من ذلك بكثير.

خلال السنتين الماضيتين، خسرت شركة هندسة ميكانيكية بميونيخ قرابة 11 مليون يورو عقب احتيال رئيسها التنفيذي على الموظفين هناك. ومؤخرا، رفعت مخبزة كبرى قضية احتيال ضد بنك

خاص بتهمة تهريب ما يناهز 1.9 مليون يورو من حسابها إلى هونغ كونغ. وحسب مديرية الشرطة بمدينة ميونيخ، تمكنت محاسبة لدى إحدى الشركات من تهريب أكثر من 200 ألف يورو إلى سنغافورة.

في الحقيقة، يتكفل مكتب الشرطة الجنائية الذي يضم مكتبا مركزيا للجرائم الإلكترونية بمثل هذه القضايا. وخلال سنة 2016، حقق هذا المركز في حوالي 130 جريمة احتيال من قبل رؤساء تنفيذيين، لينخفض عدد الجرائم إلى 110 في سنة 2017. ووفقا للرئيس الأول للمباحث الجنائية، فيرنر كريتش، سجل المكتب المركزي للجرائم الإلكترونية سلسلة من الجرائم التي يقوم فيها المجرم بالاحتيال على ضحيته عبر إجباره على الضغط على رابط خبيث مثبت في بريد إلكتروني وهمي. ونتيجة لذلك، يتسرب الفيروس إلى الحاسوب.

من جهتها، تتدخل هيئة حماية الدستور في حال التأكد من تورط جهاز إستخباراتي أجنبي في الجريمة. ومن المثير للاهتمام أن الهيئة المذكورة آنفا تراقب عن كثب تحركات المخابرات الخارجية الروسية ووزارة أمن الدولة الصينية. فضلا عن ذلك، تعمل هذه الهيئة على تتبع مجموعات القراصنة على "فانسي بير" "وأوبيريشن كليفر" "ووينيت"، مع العلم وأن هذه المجموعات تقف وراءها الأجهزة الإستخباراتية الروسية والإيرانية والصينية.

خلال السنة الماضية، سجل المكتب المركزي للجرائم الإلكترونية 84 هجوما إلكترونيا نصفها من تدبير أجهزة إستخباراتية أجنبية. وفي هذا الإطار، أفاد الناطق الرسمي باسم هيئة حماية الدستور، ماركو شيفرت، أنه "عندما لا نكشف من الوهلة الأولى تورط جهاز إستخباراتي أجنبي في هجوم إلكتروني ما، نعتبر الأمر بمثابة جريمة إلكترونية. وفي الأثناء، تتخذ الشركة المتضررة قرارا بنقل الأمر إلى أنظار القضاء من عدمه".

وفي سياق متصل، صرح الناطق الرسمي باسم معرض ميونخ الدولي، فيليه بوك، أن "المعرض في حد ذاته كان عرضة للعديد من عمليات القرصنة المتكررة، لكن كل الهجمات باءت بالفشل". في الأثناء، أبى السيد بوك التصريح بحقيقة الوصفة السرية للتصدي لعمليات الاختراق معللا ذلك، قائلا: "لا نرغب في أن نجعل الأمر سهلا بالنسبة للمخترقين".

المصدر: صحيفة زود دويتشه تسايتونغ

رابط المقال : https://www.noonpost.com/20324/