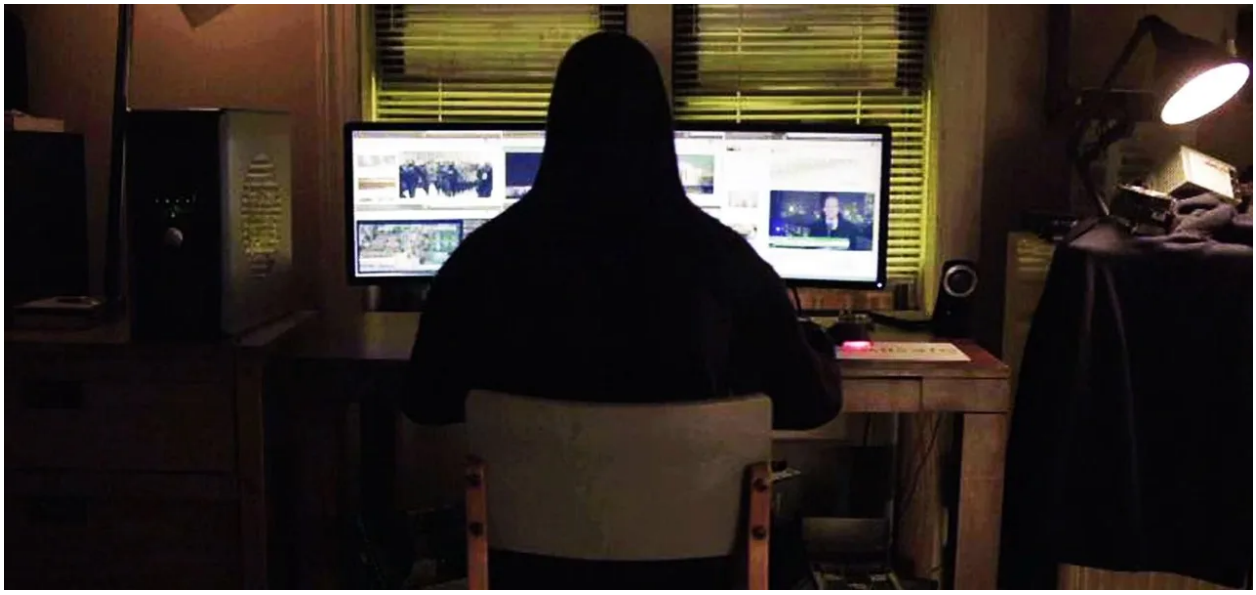
قراصنة الإنترنت .. تأريخ موجز للرعب الإلكتروني

كتبه أحمد عزيز | 12 أغسطس ,2016



حتى أواخر السبعينات من القرن الماضي، لم تكن مصطلحات القرصنة والاختراق الإلكتروني قد عرفت طريقها للعالم، لكن مع انتشار الكمبيوتر بدأت في الشيوع، وسرعان ما تحول السلوك الذي بدا في بدايته انحرافًا لمراهقين شغوفين بالتكنولوجيا، إلى حرب تشن بين الدول تهدد منشآت حيوية كالمفاعلات النووية ومحطات الكهرباء، وتدمر المخزونات النقدية لبنوك ودول، وتهتك أسرارًا كثيرة لم تكن لتظهر للعلن لولاها.

حروب القراصنة

ولم تعد الخلافات السياسية الآن تحسم بالمدافع والطائرات، وتحولت الحروب الساخنة إلى مناوشات إلكترونية بين الدول، خصوصًا الكبرى منها، وبدأت الخلافات تنعكس على شبكات الإنترنت وعالم الهاكرز، وجرائم الاختراق الإلكتروني، خاصة بين الولايات المتحدة الأمريكية وروسيا، وتحولت حربهما معًا إلى سلاح القرصنة وجنوده التقنيين، وتبادل الطرفان العديد من الاتهامات في كل مرة يتم فيها شن هجوم إلكتروني على الطرف الآخر.

اختراق واستقالة

القصة طويلة والاختراقات الإلكترونية وعمليات الهاكرز باتت تقلق الجميع، وكان آخرها ما حدث في الأسبوع الأخير من شهر يوليو الماضي، حينما اخترق هاكر اللجنة الوطنية بالحزب الديمقراطي

الأمريكي، وقام بتسريب عدد كبير من رسائل البريد الإلكترونى الخاصة بالمرشحة الرئاسية الأمريكية هيلارى كلينتون، أظهرت "تحيز" قادة اللجنة لهيلاري كلينتون على حساب منافسها بيرني ساندرز خلال الانتخابات التمهيدية، وهي الواقعة التي تبعها استقالة رئيس اللجنة ديبي واسرمان، وثلاثة من قادة اللجنة، هم الرئيسة التنفيذية إيمي ديسي، ومدير التواصل لويس ميراندا، ورئيس الإدارة المالية براد مارشال.

وبعد ساعات من التسريبات بدأت الاتهامات تتوجه لروسيا، وصرح العديد من المسؤولين بأن روسيا وراء هذا الأمر، مما جعل الحكومة الروسية تخرج لنفي تلك الاتهامات.

لم تكن تلك هي الحالة الأولى، ولن تكون الأخيرة في المناوشات السياسية بين الدول الكبرى، ففي بداية العام 2015 كشفت الصحف أن هناك تقارير إخبارية في وقت سابق من هذا العام تفيد بأن مجموعة من الهاكرز الروسى اخترقوا البيت الأبيض، وحصلوا على معلومات متعلقة بالرئيس الأمريكى باراك أوباما، وتم اختراق أجهزة بها معلومات حساسة عن الأمن القومي الأمريكي، ولم يتضح وقتها ما إذا كان المخترق تمكن من الاطلاع على هذه المعلومات أم لا، وتم توجيه الاتهامات أيضًا للحكومة الروسية، وهو الأمر الذى لم يتم إثباته، ونفته كذلك الحكومة الروسية، وهي ليست المرة الأولى ففي نفس العام 2015 اكتشفت الحكومة الأمريكية وجود برمجيات خبيثة مزروعة على أكثر من مليون جهاز كمبيوتر خاص بالمواطنين والشركات الأمريكية، قادرة على الاستيلاء على معلومات مصرفية، وعناصر للتعريف عبر الإنترنت، وعرضت الولايات المتحدة الأمريكية وقتها مكافأة مالية قدرها 3 ملايين دولار، مقابل معلومات يمكن أن تسمح بتوقيف الهاكرز الروسي المتهم الأول في الاختراق.

هزيمة البيت الأبيض

سبق الواقعتين في العام 2012 عملية اختراق مماثلة استهدفت مواقع أمريكية حساسة، في واقعة تنم عن تطور الحرب الإلكترونية بالعالم، حيث تم اختراق شبكة أجهزة الحاسوب المستخدمة في المكتب العسكري للبيت الأبيض المسؤول عن إصدار الأوامر النووية، وأقر البيت الأبيض وقتها بأن عمليات القرصنة (هاكرز) على مواقع تابعة للحكومة الأمريكية ليست قليلة، مدعيًا بأن أمريكا أعدت برامجًا لاحتواء هذه الظاهرة، وهو ما لم يتم حتى الآن.

نقطة البداية

تاريخيًا بدأ مصطلح "هاكرز" في الظهور عام 1983 عندما تحدثت مجلة النيوزويك الأمريكية عن هؤلاء الأشخاص، ووصفتهم بأنهم ممن يفضلون البحث والتنقيب في أعماق الحاسب الآلي، بدلاً من استخدامه فقط، مضيفة أن هؤلاء لعوبون وفضوليون وأذكياء، ويفضلون العمل الفردي، ولهم شغف كبير تجاه الكمبيوتر والشبكات، ويمثلون كابوس مرعب لمديري الشبكات وخدمات الأمن وأيضًا المباحث الفيدرالية الـFBI.

بعض هؤلاء الهاكرز تركوا تاريخًا تكنولوجيًا مثيرًا خلال علاقتهم بالكمبيوتر، وبعضهم الآخر لعب دور

الهارب في مطاردات خيالية لا تصدق عبر الشبكات اشتركت فيها قوى أمنية كبيرة.

درابر وكيس الشيبس

قبل انتشار فكرة الهاكرز الإلكترونيين بسنوات لمع اسم "جون درابر"، الذي عرف في مجتمع الهاكرز باسم كابتن كرانش، وهو من أوائل الهاكرز في التاريخ، ويأتي اسم شهرته من نوع من رقائق الشيبس التي كانت تباع وتحمل نفس الاسم، وفي إحدى علب هذه الحبوب اكتشف داربر وجود صافرة للأطفال كانت توضع في العلب كنوع من الدعاية للمنتج، واكتشف بذكائه الشديد أن هذه الصافرة تطلق صوتًا بتردد 2600 هرتز، وهو نفس التردد الذي يتم استخدامه من قبل شبكات الهاتف لكي تشير إلى أن الهاتف يعمل، وكان أول من استخدم هذه التقنية والتي أطلق عليها بعد ذلك عملية الفريكينج "Phreaking".

كانت طريقة درابر في اختراق شبكة الهاتف بسيطة جدًا وعبقرية في الوقت ذاته، فقد كان يتصل برقم بعيد المسافة، وبينما يرن جرس الهاتف على الناحية الأخرى، يستخدم درابر الصافرة لإصدار هذا الصوت على تردد 2600 هرتز، كان هذا التردد هو المستخدم لتعريف حالة الخط، وبإطلاق هذا الصوت من الصافرة، يقنع درابر شبكة الهاتف أنه قد أغلق الخط، وكانت هذه العملية تنجح دائمًا، بالرغم من أن الشبكة لم تتلق علامة حقيقية بأن الخط قد أغلق.

بمولد الحركة الجديدة على يد درابر، بدأت نشاطاته غير المشروعة في الظهور، عندما لاحظت شركة الهاتف التابع لها أن حسابه الشهري لم يكن مستقرًا، فبدأت التحقيق في الموضوع وألقي القبض على درابر عام 1972، لكن محاكمته استهلكت وقتًا طويلاً لأنها كانت المرة الأولى في التاريخ التي تعامل فيها النظام القانوني مع هذا النوع من الاحتيال، وبعد أربعة أعوام من المحاكمة، حكم على درابر بالسجن لمدة شهرين.

وزنياك وجوبز

اكتشاف درابر كان بمثابة الملهم للصديقين وزنياك، وهو أحد اثنين قاما فيما بعد بتأسيس شركة آبل لتكنولوجيا الكمبيوتر بمعاونة صديقه الحميم آنذاك ستيف جوبز، وقام الثنائي بإكمال اكتشاف دابر وتحسينه حيث اخترعا معا "الصندوق الأزرق"، وكان هذا الصندوق عبارة عن جهاز يقوم بإخراج نغمات بترددات مختلفة ومطلوبة من أجل خداع شبكات الهاتف، ونجحا في اختراق كل الشبكات، وإجراء كل أنواع المكالمات المجانية، وكانت صناديقهم الزرقاء الأكثر انتشارًا وقتها بين الهاكرز، ومن أشهر قصص الصندوق الأزرق هي المكالمات التي أجراها وزنياك للفاتيكان منتحلاً فيها شخصية وزير الخارجية الأمريكي السابق هنري كسينجر، من أجل الاعتراف بخطاياه.

ميتنيك: عدو البنتاجون

ويأتي على رأس الهاكرز المشهورين أيضًا "كيفين ميتنيك"، وهو الأكثر شهرة وموهبة على الإطلاق في التاريخ، كتب ميتنيك اسمه في التاريخ عام 1981، عندما كان في السابعة عشر من عمره، بعدما تمكن من الدخول على شبكات الهاتف والتحكم فيها، الأمر الذي مكنه من تحويل مكالمات المشتركين إلى أي اتجاه أراد، وفي عام 1983 تمكن من اختراق جهاز كمبيوتر وزارة الدفاع الأمريكية "البنتاجون"، وألقي القبض عليه من المباحث الفيدرالية، وحكم عليه بالسجن لخمس سنوات في التسعينات وهو الآن مستشار أمني ويدير شركته الخاصة ميتنيك للحماية Mitnick Security!.

ميتنيك لم يكن الوحيد، وتبعه كيفين بولسون، ففي عام 1983 عندما كان هو أيضًا في السابعة عشر من عمره، قام بالعديد من الهجمات والاختراقات لشبكات مختلفة، مما تسبب في عدد من المواجهات مع النظام القانوني الأمريكي، واستمر بولسون في أعماله غير المشروعة حتى ألقي القبض عليه في من قبل المباحث الفيدرالية عام 1991 وحكم عليه بالسجن لأربعة أعوام في 1994، وهو الآن رئيس تحرير مجلة وايرد Wired.

بولسون وقصة السيارة

أشهر جرائم بولسون حينما قامت محطة راديو لوس أنجلوس بإطلاق مسابقة، وطلبت من المتسابقين الاتصال ومحاولة كسب سيارة بورش 944، وكان من المفترض أن صاحب المكالمة رقم 102 سيحصل على الجائزة المغرية، بدأ بولسون بالعمل وفرض سيطرة كاملة على شبكة الهاتف الموصلة إلى المسابقة، وحجب كل المكالمات الآتية لكي يضمن أن يكون هو المتحدث رقم 102، وفاز بالسيارة وقتها.

لامو: بعبع مديري الشبكات

ويعد "أدريان لامو" الهاكرز الرئيس المسؤول عن إفقاد أكبر عدد من مديري الشبكات صوابهم،

حيث بدأ بمايكروسوفت وياهو وصن مايكروسيستمز ومكدونالدز وسينجيولار وايه أو إل، وصولاً لاختراق النيويورك تايمز، وحسابات عدد من الشركات والأعمال، ويعمل الآن كمستشار أمني، ويتمتع بحرية تامة في الحركة، بعد أن ظل لسنوات طويلة مراقبًا من قبل السلطات الأمنية الأمريكية.

وفي عام 1994 اخترق فلاديمير ليفين شبكة سيتي بانك الأمريكي المشهور على مستوى العالم، وحصل على بعض الصلاحيات على الشبكة، التي سهلت له الوصول إلى بعض الحسابات البنكية، وبمجرد الدخول إلى هذه الحسابات قام بتحويل 10.7 مليون دولار إلى حسابات أخرى في الولايات المتحدة، وفنلندة، وألمانيا، وإسرائيل، وهولندا.

وألقي القبض على ليفني في مطار هيثرو بلندن في مارس 1995، ولم تبدأ محاكمته حتى سبتمبر 1997 وانتهت بالحكم عليه بالسجن لمدة ثلاث سنوات في فبراير 1998.

جوناثان وناسا

وفي عام 1999 تمكن الهاكر الشاب جوناثان جيمس من اختراق شبكة NASA وكان حينها في سن السادسة عشر، وتسبب في بلبلة كبيرة في ناسا بمجرد استخدام كمبيوتر من نوع بنتيوم العادي، وتمكن من التحرك في الشبكة بمطلق الحرية، وسرق العديد من الملفات ومن بينها كود المصدر الخاص بمحطة الفضاء العالمية.

طبقًا لما قالته ناسا في تقاريرها عن القضية فإن قيمة الملفات التي سرقها جيمس كانت تبلغ 1.7

مليون دولار أمريكي، ولكي تتمكن من إيقاف الهجوم الذي قاده جيمس، اضطرت الوكالة إلى إغلاق النظام كلية، وإعادة تشغيله مما تسبب في خسارة تقدر بـ41 ألف دولار أمريكي، وبالرغم من كل هذه الخسائر، تمكن جيمس من تفادي السجن نتيجة لصغر سنه حينها.

وفي مجال الإعلام كانت أهم ضحية للهاكرز هي صحفية النيويورك تايمز التي استهدفها الهاكر المشهور عالميًا أدريان لامو عام 2002، ونجح في الدخول على الشبكة الداخلية للجريدة، وبدأ في تعديل ملفات مهمة جدًا في الشبكة، وقام ببعض التعديلات في قاعدة بيانات سرية ومن بين هذه التعديلات وضع لامو اسمه على قائمة الخبراء المستشارين للجريدة.

تم اكتشاف هذه التعديلات بسرعة وحررت الجريدة محضرًا بالحادثة، وألقي القبض على لامو في أغسطس 2003 وبعد تحقيق دام 15 شهرًا، حكم عليه بالمراقبة لمدة عامين و65 ألف دولار أمريكي غرامة تم إعطاؤها للجريدة تعويضًا عن الخسائر.

كارثة مايكروسوفت

في صبيحة يوم 12 فبراير 2004 أعلنت مايكروسوفت حالة الطوارئ، بعد سرقة كود المصدر لويندوز 200، والذي سبب خسارة مهولة للشركة العالمية بلغت 600 مليون بايت من البيانات، و30.195 ملف، و13.5 مليون سطر من الكود المكتوب

رابط المقال : https://www.noonpost.com/13377/