الفصل السادس:
رواد قراصنة الإنترنت ومشاهيرها

كان لقب (هاكر) يطلق -سابقاً- على المبرمج الموهوب، ومن ثم أصبح كل من يقوم باستخدام نظم التشغيل والبرامج في الدخول على الأجهزة والشبكات بشكل غير مباشر أو غير مصرح، يحمل صفة هاكر (مخترق). وقد انطبعت الصورة الذهنية السيئة عن الهاكرز لدى الجميع، نتيجة أفعالهم واختراقاتهم، وبغية تعديل هذا المفهوم وتحسين الصورة الذهنية للهاكرز وإيضاح أن ليس جميعهم من الأشرار، بل هم أشخاص لديهم قدرات عقلية وتقنية عالية؛ اجتمع في نيويورك قراصنة الحاسب الآلي (الهاكرز) في قمة استمرت لمدة ثلاثة أيام. وشارك في هذا الاجتماع عدد من كبار الشخصيات في عدد من الشركات العالمية، مثل ستيف وزنياك أحد مؤسسي شركة (آبل) وكيفن ميتنيك الهاكر الذائع الصيت. ويعد هذا التجمع هو الخامس من نوعه منذ عام ١٩٩٤. ويقدم هذا الفصل تعريفاً بأشهر الهاكرز عبر الحقبة التقنية وروادها، ومنهم:

٦-١ جون درابر

يُرجع الكثير من المختصين عمليات الاختراق والاستخدام غير الشرعي للحواسيب إلى ما ظهر في سبعينات القرن المنصرم، وسمي بالفريكينج (Phreaking) كخطوة مهمة إلى ما نراه اليوم من جرائم على شبكة الإنترنت، بصورها المتنوعة من الاختلاس إلى التزوير والتحريض على الفسق والفجور، وإغواء الأحداث، بالإضافة إلى الجرائم التي تقع على الحاسب الآلي ذاته وبرامجه كما سنرى لاحقاً عبر الصفحات الآتية .

شكل ٦ - ١: جون درابر

يرجع ظهور الفريكينج إلى جون درابر الذي ولد عام ١٩٤٤، واستخدم طريقة بسيطة وذكية في الوقت نفسه في اختراق شبكة الهاتف، فقد كان يتصل برقم تليفون معين، وبينما يرن جرس الهاتف على الناحية الأخرى، يستخدم درابر صافرة عادية جداً كانت تسمى (كابتن كرانش)، وهي مخصصة للأطفال! لإصدار صوت على تردد ٢٦٠٠ هرتز. وكان هذا التردد هو المستخدم لتعريف حالة الخط، وبإطلاق هذا الصوت من الصافرة، يقنع درابر شبكة الهاتف أنه قد أغلق الخط، وكانت هذه العملية تنجح دائما بالرغم من أن الشبكة لم تتلق علامة حقيقية بأن الخط قد أغلق.

شكل ٦ - ٢: كابتن كرانش

وقد ألقي القبض عليه فيما بعد وظلت محاكمته حوالي أربع سنوات كاملة، لحداثة هذا النوع من الجرائم، فلم يكن هناك نص قانوني حينذاك، يجرم مثل تلك الأنواع من الجرائم، وفي النهاية صدر الحكم بحبسه لمدة شهرين!!!

وقد كانت فكرة درابر غير المشروعة هي السبب في ظهور مجموعات من الهاكرز، والفريكرز، وحركات جديدة هدفها في البداية هو التهرب من دفع الفواتير، والآن اقتحام مواقع الإنترنت وشبكات الحاسب وتخريبها، ومن أوائل تلك الحركات مجموعة سميت (مجموعة ٢٦٠٠)، كان هدفها إيجاد طرق جديدة للتهرب، أو التوقف عن دفع فواتير الهاتف.

ثم تطورت الفكرة فيما بعد على يد صديق درابر (ستيف وزنياك) الذي أكمل اكتشاف درابر وحسنه، ثم اسماه (الصندوق الأزرق) الذي كان جهازًا يقوم بإخراج نغمات بترددات مختلفة ومطلوبة من أجل خداع شبكات الهاتف.

وقد كان الصندوق الأزرق أكثر احترافية وتعقيدًا من صافرة الأطفال التي استخدمها جون درابر. إذ كان قادراً على تقليد كل الأصوات على كل الترددات التي استخدمتها شبكات الهاتف، مما أدى إلى بيع الكثير من هذه الصناديق الزرقاء في السبعينات من القرن الماضي. ومن أشهر قصص الصندوق الأزرق هي المكالمات التي أجراها (وزنياك) للفاتيكان منتحلا فيها شخصية وزير الخارجية الأمريكي السابق هنري كسينجر. وجدير بالذكر أن الصندوق الأزرق سمي بهذا الاسم لأن أول جهاز تم مصادرته كان في إطار بلاستيكي أزرق.

شكل ٦ - ٣ : الصندوق الأزرق
معروض في متحف تاريخ الكمبيوتر

٦-٢ المخترق الأعظم كيفن ميتنك (Kevin Mitnick)

شكل ٦ - ٤ : كيفن ميتنك

لعل أبلغ تعبير يوجز صفات هذا الرجل، ما وصفته به فاطمة نعناع في مجلة إنترنت العالم العربي، حيث تقول: «الهاكر الأكبر،نسر ينقض على شبكات الكمبيوتر». إن كيفن يملك أصابع سحرية ما إن يضعها على لوحة مفاتيح الحاسب، حتى تنزاح أمامه أسوار الدفاعات المنيعة لمؤسسات وشركات ومنظمات، فيجد طريقه بسهولة ويسر إلى خزائن أسرارها، ونفائس مكنوناتها. فهو قد نجح ولمدة ثمانية عشر عاماً في اختراق شبكات العشرات من المؤسسات والشركات، بدءاً من شركة الهاتف المحلية للمدينة التي نشأ فيها، وانتهاء بوزارة الدفاع الأمريكية (البنتاجون). وبذلك أصبح أسطورة اختراق شبكات الحاسب الآلي في التاريخ الحديث.

حلّق كيفن مبكراً في هذا المجال على الرغم من أنه لم يكن من المتفوقين في الدراسة أو النابغين فيها، بل كان متوسط المستوى لا يلفت الانتباه، بدوافع تعويضية نجمت عن تفكك الأسرة وانفصال الوالدين، وعدم الاستقرار المعزز بسوء الوضع المالي ورقة الحال. ففي سن السابعة عشرة من العمر، انطلق كالبرق الصاعق (Three Days of the Condor) ملقبًا نفسه بالنسر تيمناً بفيلم أيام الكوندور الثلاثة، الذي تدور قصته حول باحث مطارد من قبل وكالة الاستخبارات الأمريكية، فيستخدم خبرته كضابط سابق في سلاح الإشارة في البحرية الأمريكية، للتحكم بشبكة الهاتف، وتضليل مطارديه.

وعندما شاع في أوائل الثمانينيات استخدام الحاسب الشخصي مع مودم للتحكم عن بُعْد بمقاسم شركات الهاتف، برع كيفن في الدخول إلى بدالات الهاتف المحلية، وتمكن من إجراء مكالمات هاتفية مجانية، وربما على حساب آخرين قد لا يعلمون بذلك أبداً. وتطور ذلك إلى الاقتحام والتنصت على محادثات الآخرين، فتكون لديه مخزون من الأسرار عن أشخاص من الأغنياء وذوي السلطة والنفوذ، فأشبع ذلك غروره، ومنحه إحساساً بالقوة والتفوق يعوضانه عما يحس به من الدونية والصَّغَار. وتعرَّف بعد ذلك على مجموعة من الشباب من ذوي الخبرة والمهارة في اختراق شبكات الهاتف باستخدام الحاسب، وشكلوا جماعة تستغل الهاتف، فيجرون محادثات مجانية على حساب الآخرين، أو على حساب شركات الهاتف. وكانوا يدخلون إلى شبكات الهاتف، ويهزؤون بالناس، وكل ذلك بحثاً عن المتعة والإثارة، ودفعاً للملل كما يقولون. وأصبحوا مصدر إزعاج ومضايقة سرعان ما تحول إلى أذى بارتكاب سلسلة من الجرائم. فقد قام أحد أعضاء المجموعة بإتلاف وتخريب ملفات إحدى شركات الهاتف في سان فرانسيسكو، ولم تتمكن الشرطة طوال عام كامل من معرفة الفاعل.

وفي يوم من عام ١٩٨١ تسلل كيفن واثنان من أصدقائه إلى المركز الرئيس لشركة الهاتف في مدينة لوس أنجلوس، ووصلوا إلى الغرفة التي تحتوي على الحاسب الذي يدير العمليات، وسرقوا كتب التشغيل، وقوائم سجلات شيفرة فتح الأبواب في تسعة مراكز أساسية تابعة لشركة الهاتف في تلك المدينة. ومرة أخرى لم تتمكن الشرطة من معرفة الفاعل. وبعد عام من ذلك التاريخ سارعت الشرطة إلى اعتقال كيفن ورفيقيه، بعد أن وشت بهم فتاة من أعضاء المجموعة. وحكم على كيفن بالسجن لمدة ثلاثة أشهر يقضيها في إصلاحية الأحداث بتهمة السرقة وإتلاف بيانات عبر شبكة حاسب آلي مع وضعه سنة تحت المراقبة في لوس أنجلوس. ولم يصلح حاله رغم محاولات مركز الخدمة الاجتماعية مساعدته على تطوير خبرته والاستفادة منها في عمل قانوني، بل أدت إلى نتيجة سلبية، لأنه سعى إلى تعلم أمور محددة وحِيَلٍ ماكرة تعينه على ممارسة هوايته غير البريئة بصورة أفضل. فكان نتيجة ذلك مزيداً من الأخطاء والجرائم المتتالية.

ومرة أخرى في عام ١٩٨٣ ضبط كيفن يحاول استخدام حاسب جامعة شمال كاليفورنيا لاختراق شبكة، ليصل من خلالها إلى وزارة الدفاع الأمريكية (البنتاجون)، وحكم عليه بقضاء ستة شهور تدريب في سجن للأحداث في كاليفورنيا. وبعد سنة اعتقل مرة أخرى متهماً بالعبث بالحاسب الخاص بحسابات إحدى الشركات، والشيء غير العادي هنا هو أنه بقي رهن الاعتقال دون محاكمة لمدة عام كامل، والغريب في الأمر أن ملفه اختفى من مركز الشرطة دون أن يعلم عنه أحد شيئاً.

وفي عام ١٩٨٧ أدين كيفن بسرقة برامج من إحدى شركات البرمجيات في كاليفورنيا، عن طريق الشبكة بعد أن اكتشفت الشرطة ذلك، من خلال تتبع خط الهاتف الذي تمت من خلاله العملية، وقادهم هذا إلى مسكن كيفن. وتعرض كيفن في هذه الحادثة للإهانة والضرب من قبل الشرطة، ووضع تحت المراقبة لمدة ثلاث سنوات زادته إصراراً وعزيمة على مواصلة ممارسة هوايته المؤذية له وللآخرين. وفي عام ١٩٨٨ تملكته (VMS Microcomputer) فكرة الحصول على نسخة من نظام تشغيل الحاسب الرقمي الصغير الخاص بشركة ديجيتال. فعكف لساعات طوال مع صديقه دييجو الذي يعمل في قسم دعم البرامج لإحدى شركات الحاسب في مقر عمله الذي كان يذهب إليه كل مساء، يحاولان الدخول إلى مختبرات شركة ديجيتال. وعند إحساس المسؤولين بالشركة بهذه المحاولات، وفشلهم في تتبع مصدرها أو تحديده ، طلبوا العون من الشرطة المحلية ومكتب التحقيقات الفدرالي (FBI) الذين عملوا بالتعاون مع خبراء شركة ديجيتال، ولم يتمكنوا لأيام عديدة من التوصل إلى نتيجة، لأن كيفن الماكر كان قد اتخذ احتياطات ذكية تحول دون اكتشافه، وذلك باستخدامه جهازي حاسب (VMS) يحاول من خلال الأول اختراق شبكة شركة ديجيتال، والحصول على نظام تشغيل ومن خلال الثاني مراقبة مركز مؤسسة الهاتف، وتتبع محاولات اكتشافه. وإمعاناً في التضليل قام باختراق شبكة الهاتف والعبث بمقاسمها الهاتفية. ونتيجة لذلك بذلت شركة ديجيتال الكثير من الجهد والوقت في مراقبة أجهزة الشركة وتطبيق إجراءات جديدة للحماية، فكلفها ذلك مبالغ

طائلة.

وأخيراً، تمكن رجال مكتب التحقيقات الفدرالي بفضل وشاية من ديجو صديق كيفن ورفيقه في المحاولات، وليس بفضل جهودهم، من القبض على كيفن الذي أثار حنق ديجو، وأغضبه بمزاحه الثقيل، حيث اتصل بمدير ديجو في العمل، وأخبره بأن ديجو يعاني من مشاكل كبيرة مع مصلحة الضرائب. وأحيل كيفن للمحكمة بتهمة سرقة برامج قيمتها ملايين الدولارات، والتسبب في خسائر لشركة ديجيتال تزيد عن ٢٠٠ ألف دولار، صرفتها لمنعه من الوصول إلى أجهزتها. وقد وُجد كيفن مذنباً في استخدامه الحاسب سنوات طويلة، للاحتيال وحصوله على كلمات العبور، للعديد من حاسبات الشركات بشكل مخالف للقانون. وهي المرة الخامسة التي يدان فيها كيفن في مثل هذه الجرائم، وحُكم عليه بالسجن لمدة سنة واحدة وستة شهور معالجة من إدمان اختراق الشبكات. وهو حكم أثار اهتمام الرأي العام لغرابته.

أمضى كيفن عقوبة السجن، لكنه لم يلتزم بالحكم الآخر، وهو الخضوع للمعالجة من إدمان اختراق الشبكات، وانتقل إلى لاس فيجاس وعمل مبرمجاً بسيطاً في إحدى الشركات المتخصصة في القوائم البريدية الإلكترونية.

ولكن كيفن لم يحتمل البعد عن سان فرانسيسكو، عاد إليها مرة أخرى بعد وفاة شقيقه وعمل مع والده في أعمال البناء، ثم انتقل للعمل مع صديق والده في وكالة تحقيق. وبعد مدة قليلة اكتُشِفتْ عمليةُ استخدام غير شرعية لقواعد البيانات التي تملك الوكالة حق الوصول إليها. ووجّه الاتهام إلى كيفن الذي قام مكتب التحقيقات الفدرالي بتفتيش منزله للبحث عن أدلة تدينه. وفي عام ١٩٩٢ أصدر القاضي أمراً باعتقاله بتهمتي الدخول غير الشرعي إلى حاسب إحدى شركات الهاتف، وعدم الالتزام بالبقاء في المدينة ومغادرتها قبل انتهاء فترة الستة شهور التي فرضتها المحكمة لعلاجه من الإدمان. ولم يتم اعتقاله لأنه اختفى فجأة دون أن يترك أثراً.

وفي عام ١٩٩٢ استطاع كيفن الهرب من الشرطة بعد أن شكَّتْ في طلب كان قد تلقاه قسم

الآليات بكاليفورنيا في اتصال عبر الحاسب، للحصول على نسخ من شهادات رخص السواقة للمتعاونين مع الشرطة، محاولاً إيهام المسؤولين بأنه مخول قانونياً بالاطلاع على الوثائق، وتم إرسال عناصر من الأمن إلى المحل المطلوب إرسال النسخ إليه، لمعرفة الشخص الذي طلب مثل هذه المعلومات المثيرة للريبة والشكوك وهدفه من طلبها.

وأفلت منهم كيفن، ولكن الأوراق سقطت منه في أثناء هربه. وجعلت هذه الحادثة والنجاح في الهرب من كيفن لصاً ذكياً، مثل أرسين لوبين تماماً، ومثيراً لإعجاب الكثيرين، لدرجة أن صحفياً يدعى ماركوف تخصص في تتبع أخبار كيفن، صغيرها وكبيرها، بالقدر الذي دفع مكتب التحقيقات الفدرالي إلى تعيينه مستشاراً لها في عمليات مطاردة كيفن.

وفي حادثة كانت قاصمة الظهر، وقع النسر الكاسر في شر أعماله. ففي إجازة أعياد الميلاد لعام ١٩٩٤، تمكن كيفن من سرقة مئات الملفات والبرامج من الحاسب المنزلي المتصل بشبكة العمل الواسعة لشيمومورا، أحد خبراء أمن الشبكات والبرمجة الذي يعمل مستشاراً، لمكتب التحقيقات الفدرالي، والقوى الجوية، ووكالة الأمن القومي الأمريكي، ومطور برامج لحماية نظم الحاسب من الاختراق. وكانت الملفات المسروقة مفيدة لكل من يريد تعلم أساليب اختراق شبكات الحاسب والهاتف النقّال.

لقد دخل كيفن إلى عرين الأسد، ولم ينتبه إلى أن شيمومورا قد ركّب نظام مراقبة ينذر عند الاشتباه بوقوع اختراق لشبكة الحاسب التي تتصل بها حواسبه المنزلية. فعندما بدأ الهجوم على حاسب شيمومورا المنزلي أرسل آليا مجموعة من السجلات، تتضمن كل ما دار من أحداث إلى حاسب آخر موجود في مركز الشبكة، مما جعل المشرفين يدركون وقوع اختراق لحاسب شيمومورا المنزلي، وتمكنوا من طرد المعتدي. وبعد دراسة الهجوم اكتشف شيمومورا أن المخترق قد خدع حاسبه، واتضح له أنه مخول بالدخول عليه. ولم يتمكن شيمومورا من تتبع مصدر الاتصال والوصول إلى نتيجة، وبدا له كأن الهجوم قادم من إحدى جامعات شيكاغو.

لقد أشعلت هذه الحادثة نيران غضب شيمومورا وحنقه، ودفعته إلى توجيه طاقاته وخبرته المتميزة للتعاون مع مكتب التحقيقات الفدرالي لإيقاع من تجرأ على دخول العرين.

ونجح شيمومورا بمساعدة المحققين، ومن خلال نظام المراقبة الذي بذل جهداً جباراً في تحسينه، من تتبُّع أثر المعتدي، وهو يبحر طليقاً في سماء الإنترنت، ورصده وهو يعبث دون هوادة بمقاسم شركة الهاتف، ويسرق ملفات من شركات موتورولا وأبل وغيرها، وينسخ عشرين (٢٠) ألف بطاقة ائتمان من إحدى شبكات الحاسب التجارية.

وقع النسر في الشبكة، وحامت الشكوك في كل هذه الجرائم حول كيفن ميتنك الهارب والمختبئ منذ عام ١٩٩٢، وكشفت عن أنه يقوم بعملياته الإجرامية، عبر شبكة هواتف نقّالة من مدينة رالي بشمال كاليفورنيا.

وفي مدينة رالي التي ذهب إليها شيمومورا في ١٣ فبراير ١٩٩٥، قام بمساعدة المحققين الفدراليين وخبراء شركة الهاتف المحلية، باستخدام جهاز مسح لترددات الهاتف النقّال، لتحديد مكان كيفن بمنتهى الدقة. وفي ١٥ فبراير ١٩٩٥، وصلوا إلى شقة في ضواحي مدينة رالي، وتم اعتقال النسر، ووضع في السجن دون محاكمة، حتى صدر عليه حكم بالسجن لمدة ٢٢ شهرا في ٢٧ يونيو عام ١٩٩٧، وكان حينها قد أمضى مدة الحكم وزاد عليها أربعة شهور أخرى، ومع ذلك لم يطلق سراحه على أساس أنه خطر جداً، ويمكن أن يهدد الأمن القومي للبلاد، بفضل قدرته على اقتحام أكثر المواقع خطراً وأهمية عبر شبكات الحاسب والهاتف.

ولقد تمَّ الإفراج عنه في أوائل عام ٢٠٠٠، ومنذ ذلك الحين عمد كيفن ميتنيك إلى تغيير سلوكه، وقام بتأسيس شركة استشارات متخصصة في أمن المعلومات أسماها (Mitnick Security Consulting)، تقدم مجموعة شاملة من الخدمات، لمساعدة الشركات على حماية أصولها.

والطريف في الأمر أن موقع شركة ميتنك (الهاكرز الأعظم) تم اختراقه أكثر من مرة!

فهل بات ميتنك هدفًا مثيرًا للمخترقين، أم أراد زملاء مهنة الأمس أن يجرعوه مرارة الكأس التي سقاها للكثيرين؟! أم هو أثبات بأنه لا يوجد موقع في العالم غير معرض للإختراق إذ من الممكن اكتشاف الثغرات واستغلالها، فيما تكمن الصعوبة في تأمين المواقع الالكترونية بشكل كامل.

شكل ٦-٥: موقع شركة متينك وبجوارها صورته معلنا (لست مخترقاً)

٦-٣ كيفين بولسون

شكل ٦-٦: كيفين بولسون

هو من أوائل المخترقين الذين أتعبوا المباحث الفدرالية في تتبع خطاهم حتى الإيقاع بهم، وقد ألقي القبض على كيفن للمرة الأولى في ١٩٨٩، عندما كان عمره أربعة وعشرين عاما.

واتهم بالعديد من الاختراقات لشبكات الهاتف والكمبيوتر، غير أنه تمكن من الهرب وظل طريدًا للمباحث الاتحادية لأكثر من ١٧ شهرًا، وفي هذه الفترة قام بولسون بأشهر الاختراقات التي عُرف بها. إذ قامت محطة راديو لوس أنجلوس بإطلاق مسابقة، يحصل فيها المتصل رقم (١٠٢) على سيارة بورش ٩٤٤، فبدأ بولسون باختراق شبكة الهاتف، وفرض سيطرة كاملة على الشبكة الموصلة إلى المسابقة، وحجب كل المكالمات الآتية، لكي يضمن أن

يكون هو المتحدث رقم ١٠٢. ودفع نجاح بولسون المباحث الاتحادية إلى تكثيف البحث، لتشديد الخناق حوله، إلى أن ألقي القبض عليه في أبريل ١٩٩١م، نتيجة وصول خبر قيامه بالتسوق في محل عادي في ضواحي لوس أنجلوس. ووجهت التهم لبولسون في ١٩٩٤، وحكم عليه بالسجن لأربع سنوات، وكان هذا الحكم أكبر عقوبة تصدر على هاكر في هذا الوقت.

٦-٤ جستن تانر بيترسون

يقول جون نيتيل ومايكل سوتو: «اشتهر في عام ١٩٩١ شخصٌ يدعى جستن تانر بيترسون، الذي عُرف وقد ألقي القبض عليه فيما بعد بلقب (وكيل السرقة) لسرقته سيارة، إلا أن التحقيقات التي أجريت معه لاحقاً بينت أن هناك أموراً أكثر من سرقة السيارة بكثير، قد ارتكبها هذا (اللص الظريف). فقد تبين أنه يخترق أجهزة الكمبيوتر المعقدة، ويتسلل إلى مختلف الأنظمة، وأدين بناء على هذه الأمور، إلى جانب حيازته مواد بريدية لا تخصه، وأرقام بطاقات ائتمان لأشخاص آخرين. والطريف في الأمر أن ملف هذا المجرم قد أقفل بناء على تدخل كل من مكتب التحقيقات الفيدرالي الأمريكي، ومكتب المحامي العام الأمريكي، نظراً للرغبة في استخدام مهاراته الفذة في الكشف عن المجرمين الآخرين من طرازه. وأفرج عنه من السجن، وبقي تحت إشراف مكتب التحقيقات الاتحادي الأمريكي من شهر سبتمبر ١٩٩١ وحتى أكتوبر ١٩٩٣، حيث ساعدهم في قضيتين لمخترقين كبيرين مشهورين، هما كيفن ميتنك وكيفن بولسن. إلا أنه لما أعيد فتح ملفه الإجرامي توقع الكثير أن يصدر الحكم عليه بالسجن لمدة (٤٠) أربعين عاماً، ودفع غرامة مالية قدرها (١,٥) مليون دولار. لأن بيترسون أقر في اجتماع ضمّه و محاميه مع محامي الدفاع الأمريكي بأنه لا يزال يقوم بالجرائم الإلكترونية. إذ اقتحم خلال فترة بسيطة عدداً من أجهزة الحاسب الخاصة بالحكومة الاتحادية الأمريكية ومكاتب بطاقات الائتمان. وتجاوزًا لغلطة الإقرار بالذنب، طلب بيترسون استراحة قصيرة، وفر

خلالها من المحكمة التي كان يحاكم فيها، وتوارى عن الأنظار، لأكثر من سنة، إلى أن اعتقل على مقربة من مكتب التحقيقات الفدرالي الأمريكي في مدينة لوس أنجلوس في عام ١٩٩٥، واعترف بأنه (مذنب) بتحويل مبلغ (١٥٠,٠٠٠) دولار برقياً في بنك (هيلر فاينانشال)، حيث صدر حكم عليه بالسجن لمدة ثلاث سنوات، وبالمراقبة لمدة ثلاث سنوات أخرى، ودفع غرامة مالية قدرها(٣٨,٠٠٠) دولار.

أُطلق سراح جستين بيترسن عام ١٩٩٧م، فأعلن عقب خروجه، أنه توقف نهائياً عن العمليات غير المشروعة التي كان يقوم بها، وركز على تطوير مهاراته في مجال الويب. فعمل مطورًا لصفحات ويب ضمن (ويندوز نت)، وافتتح موقعاً شخصياً له.

٦-٥ جيسون ميوهايني يُعتقل في وكالة الفضاء الأمريكية (ناسا)

ورد في خبر من أونتاريو بكندا بتاريخ ١٥ أبريل ١٩٩٨، أن شاباً كندياً يبلغ من العمر ٢٢ عاماً، يواجه عشرات التهم في قضايا هجوم واختراق لأنظمة حاسب، وسرقة شيفرات أمن حاسبات في مرافق جوية مهمة جداً في الولايات المتحدة الأمريكية.

وذكرت الشرطة الملكية الكندية التي أجرت تحقيقاً لمدة أربعة عشر شهراً، أن أحد المتطفلين الهاكرز، تمكن من الدخول إلى أنظمة حاسب كل من المركز الوطني لإدارة الطيران والفضاء، والجمعية الوطنية لعلوم الجو والمحيطات، وشركة هيوز إحدى أضخم الشركات العاملة في مجال الطيران والفضاء. وقد ذكر أن خسائر إتلاف ملفات في واحدة من هذه القضايا قد بلغ خمسين ألف دولار أمريكي، وأن اختراقاً قد تمَّ لعدة أنظمة حاسب خاصة، أو تابعة لجامعات بكندا، والولايات المتحدة الأمريكية.

وقد وجهت لهذا الشاب المدعو جيسون ميوهايني، تهم التسبُّب بالأذى لقيامه عن عمد بإعاقة الاستخدام القانوني للبيانات واعتراضه، والتدخل فيه، وقدم للمحاكمة في ١٣ مايو من عام ١٩٩٨.

٦-٦ روبرت تابان موريس

تسبب روبرت موريس في إتلاف أكثر من ٦٠٠٠ جهاز كومبيوتر في نوفمبر ١٩٨٨، وأدت إلى خسارة قدرت بعدة ملايين من الدولارات، وكان ذلك بسبب فيروس قام باختراعه وعرف باسم (دودة موريس)، وانتشر على تلك الأجهزة عن طريق الشبكة فتم إتلاف جميع تلك الأجهزة، ولم يستطع أحد جعلها تعمل كحالتها الأولى. وقد تم القبض عليه، وحاول تبرير فعلته بأنه كان يريد اختبار مدى تحمل الشبكة وأجهزة الكومبيوتر، ولكن ذلك لم يكن سبباً مقنعاً لذا حكم عليه بالسجن لمدة ٣ سنوات تحت المراقبة، و ٤٠٠٠ ساعة في خدمة المجتمع وغرامة مالية كبيرة .

وفى يومنا هذا يعرض في متحف بوسطن للعلوم قرص كومبيوتر يحتوي على الفيروس، وهذا القرص هو نفسه الذي استخدمه روبرت في هجماته .

٦-٧ المخترق السعودي (sNiper_hEx)

ينظر كثيرون بعين الرضا والإعجاب لأحد المخترقين السعوديين، الملقب بـ(sNiper_hEx) واسمه الحقيقي خالد، لأن أعماله –كما يقولون– لم تنصب في الجانب المظلم من

الاختراقات، بل تكرّست في الهجوم –حسب رأيه– على الأعداء الصهاينة، ولعل شهرته زادت كثيراً حينما كتبت عنه بعض الصحف الأمريكية والإسرائيلية ونشر اسمه في المجلات والمواقع اليهودية للتحذير منه، ولأخذ الاحتياطات الأمنية اللازمة، إذ استطاع تدمير أكثر من (٤٠٠) موقع إسرائيلي ويهودي في فترة قصيرة. وذكر sNiper_hEx أنه عمل على تطوير برنامج (الدرة) بطريقة جديدة، لاستهداف المستخدمين الإسرائيليين بحيث تتم عمليات الهجوم على مزودات الويب الإسرائيلية بواسطة المستخدمين الإسرائيليين أنفسهم، وحتى لا يتمكنوا من صد الهجمات لاسيما بعد نجاح تجربته الأولى في إصابة أكثر من (٦٩) ألف جهاز في أربعة أيام.

والجدير بالذكر أن sNiper_hEx يأخذ على المخترقين العرب اختراقاتهم للعناوين البريدية والمواقع العربية، واستهداف المستخدمين ولاسيما المبتدئين منهم.

٦-٨ الهاكرز المراهقون

لم يكن الاختراق عملا خاصا بالبالغين أو المحترفين، بل غدا هواية للمراهقين الحالمين بتحقيق أمجاد شخصية، وقد برز عدد منهم، وقاموا بعمليات عديدة جلبت لهم كثيرا من الاهتمام.

٦-٨-١ ميشال سالس Michael Calce

مخترق مراهق عمره ١٥ سنة اكتسب سمعة سيئة منذ البداية بعد أن قام باختراق بعض المواقع التجارية العالمية، واستخدم اسماً مستعاراً (MafiaBoy) حيث اخترق (٧٥) جهاز كمبيوتر و (٥٢) شبكة، أثرت على شركة أمازون وإيباي وياهوو، وألقي القبض عليه فحكم عليه بالسجن لمدة ٨ أشهر وغرامة مالية صغيرة.

٦-٨-٢ مراهقان يتسللان إلى شبكة مقدم خدمة ألماني

استطاع اثنان من المراهقين الهاكرز الألمان تنفيذ هجوم ناجح، على مقدم خدمات الهاتف المباشر، وهي الخدمة المباشرة التي تديرها شركة الهاتف الوطنية الألمانية (T-Online)، وتمكنا من سرقة معلومات حول مئات أرقام الحسابات البنكية. وكان هذان المراهقان المتسللان البالغان من العمر ١٦ عاماً قد تفاخرا بأعمالهما الجريئة، ومآثرهما لمجلة تقنية الحاسب الألمانية، واصفين الأنظمة الأمنية للاتصالات الألمانية بالتخلف والبدائية المطلقة.

وقد حدث هذا الهجوم عقب قيام وزارة العدل الألمانية، باعتقال ثلاثة من المراهقين الإسرائيليين، لهم علاقة بسلسلة من الاختراقات، لشبكات حاسب مملوكة للحكومتين الأمريكية والإسرائيلية، بالإضافة إلى شبكات خاصة بشركات ومؤسسات تعليمية في الولايات المتحدة الأمريكية وخارجها.

ويمارس المتطفلون من المراهقين الألمان ألعاباً مجانية على الشبكة عند اختراقهم لأنظمة الحاسب والشبكات، وقد قام عدد منهم مؤخراً بسرقة بيانات مالية مهمة، ادَّعوا أنهم أتلفوها دون أن يستخدموها.

وعلَّق على ذلك أحد المسؤولين الألمان مشيراً إلى أن عمليات الاختراق والهجوم على الشبكات، أصبحت مشكلة دولية مع ازدياد حجم المعلومات التي توضع على الشبكة الدولية، وشبكات الحاسب الأخرى، وأن الاشتباه بقيام المراهقين بهذه الهجمات يزيد المخاوف من خطورة الأمر كثيراً، لأن في ذلك قابلية لوقوع معلومات حساسة في أيدي مراهقين باحثين عن الإثارة.

٦-٨-٣ مخترق مراهق يمنع من استخدام الحاسب

وجهت ولاية ماسيتشوتس تهماً بارتكاب جرائم اتحادية ضد مراهق، لقيامه بالهجوم

على حاسبات شركة اتصالات هاتفية بالولاية، تمكن خلاله من تعطيل برج المراقبة لإدارة طيران اتحادية، وقطع خدمات الهاتف الخاصة بالولاية، وهي أول قضية توجه فيها تهم اتحادية ضد حَدَثٍ لقيامه بجريمة حاسب آلي. وبناء على التماس قانوني خاص، أُخضع هذا المراهق للمراقبة مع تعليق العقوبة لمدة سنتين، لا يحق له خلالهما تملك أو استخدام جهاز مودم، أو أي وسائل اتصال عن بُعْد، مع أجهزة أو شبكات الحاسب بصورة مباشرة أو غير مباشرة، وأن يدفع تعويضاً لشركة الهاتف، وأن يكمل ٢٥٠ ساعة خدمة اجتماعية بالإضافة إلى مصادرة جميع أجهزة الحاسب التي استخدمت خلال فترة قيامه بنشاطه الإجرامي.

وقد علّق النائب العام الأمريكي دونالد ك. ستيرن على ذلك قائلاً: «إن شبكات الحاسب والهاتف هي قلب الخدمات الحيوية التي تقدمها الحكومة والقطاع الخاص، وهي البنية التحتية المهمة للدولة، وهي ليست لعبة لتسلية المراهقين لأن الهجوم على أي جهاز حاسب أو شبكة هاتف يمكن أن يشكل خطراً هائلاً على الجمهور، ولذا، فإن الحكومة ستحاكم المراهقين المتطفلين (الهاكرز) في القضايا المناسبة مثل هذه القضية».

٦-٩ عمليات اختراق متفرقة

هناك عدد من العمليات المميزة التي قام بها مخترقون (هاكرز)، وربما كان الباعث لتميزها هو الأثر النوعي الذي أحدثه، أو الطريقة التي تمت بها، ومن هذه العمليات:

٦-٩-١ هاكر نيوزيلندي يحذف ٥٠٠٠ موقعاً للإنترنت

في هجوم يعدُّ الأكبر من نوعه الذي تشهده نيوزيلندا على شبكة الإنترنت، قام أحد المتطفلين عام ١٩٩٨، بالدخول في خدمة مضيف في الولايات المتحدة الأمريكية تحمل مواقع

عنكبوتية مملوكة، لزبائن موفر خدمة إنترنت نيوزيلندي وقام بحذف ٥٠٠٠ موقع إلكتروني.

٦-٩-٢ هجوم على مواقع يابانية حكومية

أعلنت الحكومية اليابانية عن تعرض موقع وكالة العلوم والتقنية في اليابان على الإنترنت، لهجوم مزدوج تم فيه اختراق الصفحة الرئيسة، للموقع مرتين متتاليتين يومي الأربعاء والخميس ٢٦ و ٢٧ يناير ٢٠٠٠م، وقد سبقهما هجومين آخرين يوم الثلاثاء ٢٥ يناير ٢٠٠٠، على وكالة الإدارة والتنسيق ومكتب الإحصاء الياباني، وذكرت الحكومة اليابانية أنه الهجوم الأول من نوعه الذي تم على مواقع حكومية يابانية حتى التاريخ المذكور. وكان التركيز في هذا الهجوم على انتقاد الحكومة اليابانية، على محاولتها إنكار حدوث مجزرة "نانجينغ" التي راح ضحيتها ما يقرب من ثلاث مئة ألف من الصينيين عام ١٩٣٧، وهو أمر أثار حفيظة الصينيين الذين خرجت مجموعات منهم في مظاهرات احتجاجية على ذلك.

وقد قام المهاجمون باستبدال النصوص الموجودة على صفحات المواقع الرئيسة، بعبارات كتبت باللغتين الصينية والإنجليزية، تضمنت كلمات وشتائم بذيئة، فضلاً عن وصل أحد المواقع بموقع إنترنت إباحي، وكذلك شطب بيانات موقع الإحصاء بشكل كامل. ولكنه تمَّ استرجاع البيانات من نسخة احتياطية.

٦-٩-٣ عملية بعشرة ملايين دولار

حظي فلاديمير ليفين بشهرة واسعة بعد أن سرق عشرة ملايين دولار في عميلة مثيرة.

إذ اخترق ليفين شبكة (سيتي بنك) الأمريكي المشهور على مستوى العالم في عام ١٩٩٤م، وحصل على بعض الصلاحيات في الشبكة التي سهلت له الوصول إلى بعض الحسابات البنكية، وبمجرد الدخول إلى هذه الحسابات قام ليفين بتحويل (١٠,٧) مليون

دولار إلى حسابات أخرى في الولايات المتحدة، وفنلندا، وألمانيا، والكيان الصهيوني، وهولندا. وقد قام ليفين بتحول هذه المبالغ بمعاونة ثلاثة من العاملين، داخل البنك الذين تم تخويلهم بجمع المال المسروق.


شكل ٦-٧: فلاديمير ليفين

وحين حاول المتعاونون معه الاختفاء بالمال المسروق، تم القبض عليهم. وتسبب التحقيق معهم في التوصل إلى ليفين، والبدء في ملاحقته بينما كان يعمل في شركة لتقنية الحاسب في سانت بطرسبرج في روسيا. وألقي القبض عليه في مطار هيثرو بلندن في مارس ١٩٩٥م، ولم تبدأ محاكمته حتى سبتمبر ١٩٩٧م، وانتهت المحاكمة بالحكم عليه بالسجن لمدة ثلاث سنوات في فبراير ١٩٩٨.

٦-١٠ أشهر مجموعات الاختراق على الإنترنت

يوضح الجدول الآتي أسماء أشهر مجموعات الاختراق على الإنترنت، ونلحظ المجموعة المسماة S4udi-S3curity-T3rror التي يبدو من اسمها أنها مجموعة سعودية.

Hmei7	[elite top team#]	core-project	Prime Suspectz	S4udi-S3curity-T3rror
iskorpitx	Swan	1923Turk	eMP3R0r TEAM	NobodyCoder
Fatal Error	D.O.M	linuXploit_crew	spook	Kernel_Attack
chinahacker	Triad	Poizonb0x	THE FREEDOM	Sovalye
Ashiyane Digital Security Team	3n_byt3	PowerDream	Silver Lords	DATA ir Security Group
Mafia Hacking Team	HEXB00T3R	KHG	Persian Boys Hacking Team	SPYKIDS
DeltahackingSecurityTEAM	LaTinHacKTeam	XTech Inc	ISCN	reDMin
Red Eye	sinaritx	Hi-Tech Hate	nf3rN.4lL!	OutLaw
uykusuz001	ZoRRoKiN	S4t4n1c_S0uls	Vezir.04	dark-underground
Iran Black Hats Team	By_aGReSiF	BeLa	batistuta	m0sted

جدول ٦-١ أشهر مجموعات الاختراق

٦-١١ أشهر الجرائم الإلكترونية في العامين ٢٠١١/٢٠١٢

يعد العام المنصرم عاماً مفصلياً في تطور الجرائم الإلكترونية، وما تسببت به من خسائر مادية جسيمة على كافة الأصعدة وهنا سنستعرض أكبر عمليات الاختراق التي حدثت في عام ٢٠١١ ومطلع عام ٢٠١٢:

٦-١١-١ أكبر عملية تجسس

بهدف سرقة البيانات والتجسس، شُنَّت موجات عنيفة من الهجمات ضد الولايات المتحدة وبلدان أوروبية أخرى، ويرجح الكثيرون أن الصين هي مصدر هذه الهجمات، إذ تستخدم التجسس عبر الإنترنت للحاق بركب منافسيها الغربيين فضلا عن سعيها لتحقيق التوازن العسكري. وفي مقابلة نادرة على (SkyNews) صرّح رجل أعمال صيني بأنه يعمل مع الحكومة لاختراق الشركات المنافسة في الدول الغربية، وكشف عن صلات غامضة بين القراصنة والحكومة الصينية. وفي التقرير ذاته قال رجل شرطة: «نحن هنا لنرى ما إذا كان لديهم أي شيء يمكننا استغلاله، إذا كان هناك ما يدعو للاهتمام، فإننا سوف نحاول الحصول عليه، والقيام بالخطوات اللازمة». وقد ولدت الحصول على المعلومات واستغلال البيانات الحساسة «أعظم تحول للثروة في التاريخ»، بحسب وصف الجنرال كيث الكسندر.

فالحكومات ولاسيما الصين تسعى جاهدةً لتحقيق أهدافها المحددة في كتاب (الحرب غير المقيدة) انظر الشكل٦-٨. إذ إن واحدا من المكونات الرئيسة للكتاب هو (حرب الشبكة) والتي غالبا ما تكون ذات تكلفة هائلة وفق تقرير مكتب مكافحة الاستخبارات الذي يؤكد أن ما بين (٢ — ٤٠٠) مليار دولار هي مقدار الخسائر التي وقعت بسبب التجسس الإلكتروني.

شكل ٦-٨: صفحة الغلاف لكتاب (الحرب غير المقيدة)

٦-١١-٢ مواقع حكومية وعسكرية للبيع !!

ظهرت مؤخراً خدمات إلكترونية تقدم خدمة اختراق المواقع الحكومية والعسكرية باستغلال ثغرات حقن قواعد البيانات (SQL Injection) حيث إن المئات من المواقع مصابة بهذه الثغرة الخطيرة التي يمكن استغلالها والحصول على صلاحيات مدير النظام، ومن ثم يتم بيع هذه البيانات لمخترقين آخرين، وبإمكان من يملك ٥٠ دولاراً أن يستأجر هذه الخدمة ليتمكن من اختراق مواقع عسكرية كما تشير لائحة أسعار خدمات الاختراق الآتية:

شكل ٦-٩: لائحة أسعار خدمات الاختراق

لقد أثبتت ثغرة حقن قواعد البيانات (SQL Injection) بأنها الأغلى تكلفة، والثغرة الأكثر انتشارا في التاريخ. والموقع أعلاه يوضح كيف أن هذه الثغرة قد تستخدم من قبل المخترقين لجني الأرباح من خلال بيع ما يحصلون عليه من بيانات ومعلومات للمهتمين بها، إذ لم يعد اختراق الأنظمة لمجرد التحدي والمتعة وإنما لجني الأموال!

٦-١١-٣ سوني (SONY)

تم اختراق شبكة سوني الترفيهية والاستحواذ على بيانات أكثر من ١٠٠ مليون مشترك في شبكة سوني للموسيقا (Qriocity) وشبكة الألعاب (PSN) منها ١٢ مليون بيانات غير مشفرة والبيانات الائتمانية للمشتركين، وكان هذا الاختراق هو الأكبر نوعاً وكماً لعام ٢٠١١ مما كان له الأثر الأكبر على عدة أوجه.

قوائم الخسارة الكبيرة لأسهمها في سوق الأسهم كما يشير الرسم البياني الآتي:

شكل ٦-١٠: انخفاض سهم سوني في سوق الأسهم بعد عملية الاختراق

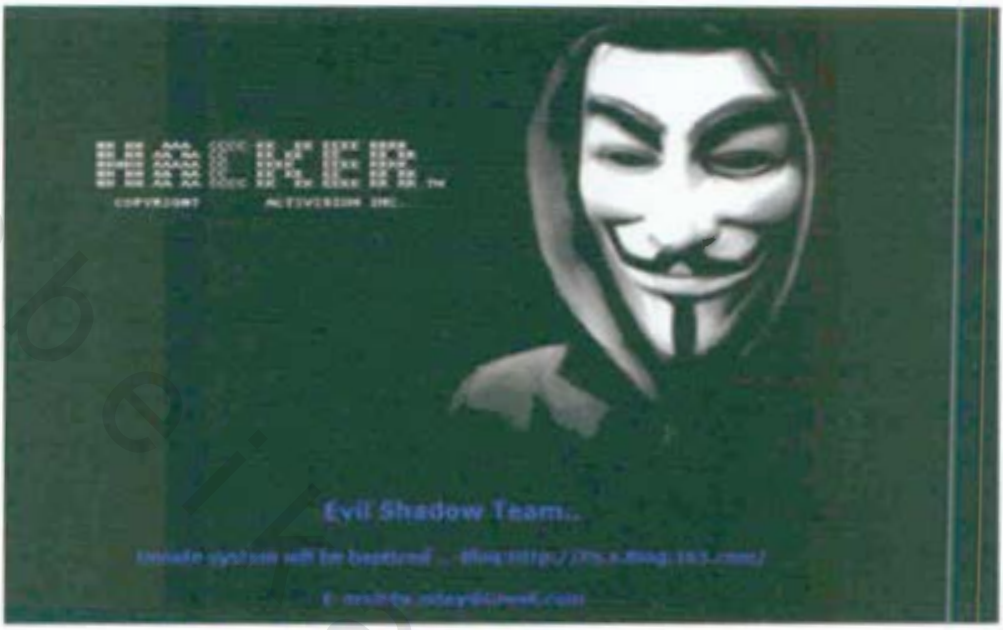
رفع هذا الاختراق من قيمة تأثير ثغرة حقن قواعد البيانات (SQL Injection) بحيث جعله الهدف الأول لمحاولي اختراق المواقع.

كان الهدف الأساس للهجوم ليس إحراج سوني وإنما إسقاطها تماماً، وهو ما تم بالفعل حيث بقيت شبكات الألعاب الاجتماعية معطلة قرابة الشهر.

قدرت الخسائر المادية بقرابة ١٠٠ مليون فضلا عن خسارة السمعة وولاء الزبائن.

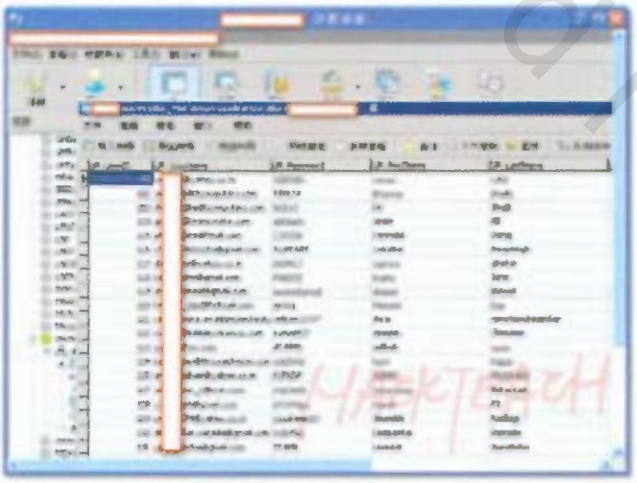
٦-١١-٤ اختراق متجر مايكروسوفت في الهند

قامت مجموعة من الهاكرز في منتصف فبراير ٢٠١٢، باختراق متجر مايكروسوفت لمستخدمي الهند، وقد تم وضع صورة للاختراق على الصفحة الرئيسة مما أدى إلى عدم قدرة المستخدمين الدخول إلى حساباتهم، انظر الشكل ٦-١١. ولم يقتصر الاختراق فقط على وضع الصورة، ومنع المستخدمين من دخول حساباتهم والتحميل، بل تمت عملية سرقة أسماء الحسابات مع كلمات المرور الخاصة بالمستخدمين.



شكل ٦-١١ الصفحة الرئيسة لموقع متجر مايكروسوفت الهند.

وما يلفت النظر ويسترعي الانتباه أن المجموعة استطاعت الحصول على كلمات المرور لأنها كانت محفوظة في قواعد البيانات بشكل غير مشفر كما يوضح الشكل (٦-١٢).



شكل ٦-١٢ قواعد البيانات لموقع متجر مايكروسوفت الهند.

٦-١١-٥ موقع الاستخبارات المركزية الأمريكية

أدى تعرض موقع الاستخبارات المركزية الأمريكية (CAA) الإلكتروني للقرصنة على يد أشخاص استخدموا راية مجموعة القرصنة الشهيرة (أنونيموس) إلى توقفه ما يزيد عن ٩ ساعات.

وزعمت وسائل إعلام أمريكية أن مجموعة (أنونيموس) أعلنت مسؤوليتها عن الأمر قائلة أنها تمكنت من الحصول على المعلومات الشخصية لـ٤٦ ألف شخص في ألاباما. غير أنه بعد عدة ساعات نشرت المجموعة على صفحتها على موقع (تويتر) ملاحظة أوضحت فيها أن إعلانها عن تعرض موقع الـ(CAA) للقرصنة لا يعني أنها هي التي نفذت الهجوم الإلكتروني. ويشار إلى أن مجموعة (أنونيموس) تستهدف الوكالات الفدرالية الأمريكية وصعدت من هجماتها في الأشهر الأخيرة، فقرصنت مواقع تابعة لوزارة العدل الأميركية ومكتب التحقيق الفدرالي (FBI) ومواقع تابعة لشركات ترفيه.

٦-١١-٦ سرقة نحو ٤٠٠ ألف بطاقة ائتمانية إسرائيلية

مع بداية عام ٢٠١٢ تكاثرت الأخبار عن حدوث اختراق كبير طغى عليه البعد السياسي أكثر من جانبه التقني والمعلوماتي، فقد نشر مؤخرا أن مخترقاً يدعى (Ox Omar) قام باختراق حسابات مصرفية وعشرات الآلاف من بطاقات الائتمان العائدة لإسرائيليين إضافة شركة طيران العال والبورصة الإسرائيلية، وادعت إسرائيل أنه المخترق سعودي مقيم في المكسيك ويسمى عمر حبيب وهو ما نفته وزارة الخارجية السعودية، وفقاً لتقرير نشرته صحيفة (عكاظ)، فندت فيه المزاعم التي تداولتها وسائل إعلام إسرائيلية فذكرت أنه بمراجعة سجلات الرعايا في السفارة السعودية في المكسيك لم يعثر على أحد بهذا الاسم.

وأشارت تقارير إلى تمكن المخترق السعودي من نشر تفاصيل ٤٠٠ ألف بطاقة ائتمانية يملكها إسرائيليون إلا أن الشركات الائتمانية قالت أن نحو ١٤ ألف بطاقة فقط تضررت.