بداية الاختراق

لا يمكن فعليا تحديد الفترة الزمنية لأول عملية اختراق، وذلك لأن مفهوم الاختراق قديما لم يكن يعني مجرد اختراق شبكة حاسوب أو موقع إلكتروني، وإنما كان اختراق أي جهاز لتحقيق هدف خاص يسمى اختراقا، وعلى هذا الأساس يمكن القول إن عام 1903 شهد أول عملية اختراق في التاريخ، تطورت الاختراقات بعدها لتصل إلى حد الحروب الإلكترونية.
في عام 1903 كان الفيزيائي جون أمبروز فلمنج يستعد لعرض إحدى العجائب التكنولوجية المستجدة وهي نظام تلغراف لاسلكي بعيد المدى ابتكره الإيطالي جوليلمو ماركوني، في محاولة لإثبات أن رسائل شفرة مورس يمكن إرسالها لاسلكيا عبر مسافات طويلة، وكان ذلك أمام جمهور غفير في قاعة محاضرات المعهد الملكي الشهيرة بلندن.
وقبل بدء العرض بدأ الجهاز ينقر مكونا رسالة، كانت في البداية كلمة واحدة ثم تحولت إلى قصيدة ساخرة بشكل غير لائق تتهم ماركوني "بخداع الجمهور"، فقد تم اختراق عرض ماركوني وكان المخترق هو الساحر والمخترع البريطاني نيفيل ماسكيلين الذي قال لصحيفة تايمز إن هدفه كان كشف الثغرات الأمنية من أجل الصالح العام.
في عام 1932 تمكن خبراء التشفير البولنديون ماريان ريجيوسكي وهنري زيجلاسكي وجيرزي روزيكي من فك شفرة جهاز إنيغما الذي استخدمه بشكل خاص الألمان خلال الحرب العالمية الثانية لإرسال واستقبال رسائل سرية.
في عام 1971 ابتكر جون درابر -الملقب بكابتن كرنتش- وصديقه جو إنغريسيا الصندوق الأزرق الذي استخدماه للتحايل على نظام الهاتف وإجراء مكالمات هاتفية بعيدة المدى مجانا.

- **سيتي بنك كان ضحية إحدى أكبر عمليات القرصنة الإلكترونية (غيتي)**

الثمانينيات والتسعينيات

- **ونقفز إلى عام 1981 حيث تشكلت مجموعة قراصنة "نادي فوضى الحاسوب" في ألمانيا، ومجموعة "أسياد البرامج" (وير لوردز) في أميركا التي تتألف من العديد من المتسللين المراهقين ومخترقي الهاتف والمبرمجين والعديد من قراصنة الحاسوب الذين يعملون في الخفاء.**

- **في عام 1988 ظهرت "دودة موريس" -إحدى أوائل ديدان الحواسيب المعروفة التي أثرت في البنية التحتية للإنترنت وانتشرت في الحواسيب وعلى نطاق واسع داخل الولايات المتحدة، واستغلت الدودة نقطة ضعف في نظام يونيكس " ناون1" واستنسخت ذاتها بانتظام وتسببت بإبطاء أداء الحواسيب لدرجة عدم القدرة على استخدامها.**

وعند اعتقال مطور هذه الدودة روبرت تابان موريس أصبح أول قرصان يدان تحت قانون "احتيال الحاسوب وإساءة الاستخدام"، وهو الآن أحد القراصنة الأخلاقيين (أصحاب القبعات البيضاء) حيث يعمل بروفيسورا في معهد ماساتشوستس التكنولوجي.
وفي صيف عام 1994 تمكن قرصان روسي يدعى فلاديمير ليفين من اختراق بنك "سيتي بنك" الأميركي وتحويل عشرة ملايين دولار من حسابات عملاء إلى حساباته الشخصية في فنلندا وإسرائيل مستخدما حاسوبه المحمول. حكم عليه بعد اعتقاله بالسجن ثلاث سنوات، واستعادت السلطات كافة المبلغ المسروق باستثناء أربعمائة ألف دولار.

-

- **أنونيموس تبنت مسؤولية العديد من الهجمات التي استهدفت مواقع إنترنت إسرائيلية (غيتي)**

اختراقات القرن الـ 21
في ديسمبر/كانون الأول 2006 أجبرت ناسا على حجب رسائل البريد الإلكتروني التي تأتي مع مرفقات قبل إطلاق المركبات الفضائية خشية اختراقها، وذكرت مجلة "بيزنس ويك" الأميركية أن خطط إطلاق مركبات الفضاء الأميركية الأخيرة حصل عليها مخترقون أجانب غير معروفين.
في عام 2007 تعرضت شبكات حاسوب الحكومة الإستونية لهجوم من نوع الحرمان من الخدمة من طرف مجهولين، وذلك بعد جدال مع روسيا بشأن إزالة نصب تذكاري، وتعطلت في الهجوم بعض الخدمات الحكومية الإلكترونية والخدمة المصرفية عبر الإنترنت، وفي

ذلك العام اخترق حساب بريد إلكتروني غير سري لوزير الدفاع الأميركي من طرف مجهولين ضمن سلسلة كبيرة من الهجمات للوصول إلى شبكات حاسوب البنتاغون.
وفي صيف عام 2008 اخترقت قاعدة بيانات حملات المرشحين الجمهوري والديمقراطي في الولايات المتحدة من قبل مجهولين قاموا بتحميل تلك البيانات، وفي أغسطس/آب اخترقت شبكة حواسيب في جورجيا من طرف مخترقين مجهولين خلال فترة صراعها مع روسيا.
وفي يناير/كانون الثاني 2009 وخلال العدوان الإسرائيلي على قطاع غزة تعرضت بنية الإنترنت التحتية في إسرائيل لهجمات إلكترونية عديدة تركزت على مواقع إلكترونية حكومية، ونفذت الهجمات باستخدام نحو خمسة ملايين حاسوب على الأقل وفقا لمجة "ناتو ريفيو" الإلكترونية، وتبنت مجموعة القراصنة المجهولين (أنونيموس) الكثير من تلك الهجمات.

شبكة حواسيب سوني بيكتشرز تعرضت لهجمة إلكترونية مدمرة (أسوشيتد برس)
حرب إلكترونية
في يناير/كانون الثاني 2010 عطلت جماعة تطلق على نفسها اسم "الجيش الإيراني السيبراني" خدمة البحث على الإنترنت لمحرك البحث الصيني الشائع "بايدو"، وكان يتم تحويل مستخدمي محرك البحث إلى رسالة سياسية إيرانية، وكانت الجماعة ذاتها اخترقت "تويتر" في ديسمبر/كانون الثاني 2009 مع توجيه رسالة مشابهة.
وفي أكتوبر/تشرين الأول 2009 اكتشف فيروس "ستكسنت" وهو برمجية خبيثة معقدة مصممة لتعطيل أنظمة التحكم الصناعية من إنتاج سيمنز كالتي تستخدمها إيران وإندونيسيا إلى جانب دول أخرى، الأمر الذي أثار تكهنات بأنها سلاح إلكتروني حكومي استهدف برنامج إيران النووي.
في يناير/كانون الثاني 2011 أعلنت الحكومة الكندية تعرض وكالاتها لهجوم إلكتروني ضخم من بينها وكالة البحث والتطوير الدفاعي الكندية، وأجبرت الهجمات وزارة المالية ومجلس الخزانة الكنديين على فصل اتصالهما بالإنترنت.
وفي يوليو/تموز 2011 أعلن نائب وزير الدفاع الأميركي أن قراصنة إنترنت سرقوا 24 ألف ملف من وزارة الدفاع في عملية واحدة خلال مارس/آذار، مضيفا أن الوزارة تعتقد أن وراء الهجوم دولة وليس أفرادا أو مجموعة قراصنة.
في أكتوبر/ تشرين الأول 2012 اكتشفت شركة أمن المعلومات الروسية "كاسبرسكي" هجوما إلكترونيا عالميا حمل اسم "أكتوبر الأحمر"، وقالت إنه يجري منذ عام 2007 على الأقل ويعمل على جمع معلومات من سفارات وشركات أبحاث ومؤسسات عسكرية وشركات طاقة وغيرها، مشيرة إلى أن أهداف الهجوم الرئيسية هي دول في أوروبا الشرقية ودول الاتحاد السوفياتي السابق وآسيا الوسطى، وبعض دول أوروبا الغربية وشمال أميركا.
وفي أواخر نوفمبر/تشرين الثاني 2014 تعرضت شبكة حواسيب شركة سوني بيكتشرز اليابانية في الولايات المتحدة لهجوم إلكتروني عنيف نتجت عنه سرقة عدد من الأفلام السينمائية الحديثة التي لم يكن بعضها قد عرض بعد، وتسريب مئات آلاف رسائل البريد الإلكتروني والبيانات الشخصية لحسابات معروفة، ووصفت بعض تلك الرسائل بالمحرجة، وبشكل عام تكبدت الشركة نتيجة هذا الهجوم -الذي نسب إلى كوريا الشمالية أو متعاطفين معها- خسائر قدرت بنحو مائة مليون دولار.

اساليب الاختراق

يستخدم قراصنة الإنترنت أساليب عديدة لاختراق أو تعطيل شبكات الحاسوب المستهدفة، وقد يكون ضرر بعض هذه الأساليب محدودا يقتصر على سرقة معلومات محددة من حاسوب مستهدف، وقد يكون مدمرا يؤدي إلى تعطيل شبكة بأكملها وتسريب بيانات مستخدميها وبريدهم الإلكتروني
ومن أبرز أساليب القراصنة لتعطيل شبكات الحاسوب ما يعرف بهجوم الحرمان من الخدمة (Denial-of-service) أو الحرمان من الخدمة الموزع (DDoS) وهي هجمات تستهدف عادة مؤسسات حكومية أو شركات كبرى كالبنوك مثلا، وهدفها جعل جهاز أو شبكة حاسوب غير متاحة للمستخدمين المستهدفين، أي حرمانهم من الخدمة التي تستضيفها خوادم الشبكة.

ولا تقتصر هجمات الحرمان من الخدمة على الأساليب المعتمدة على الحاسوب، بل قد تتحول إلى هجمات فيزيائية حقيقية ضد البنية التحتية مثل قطع أسلاك الاتصالات في قاع البحر، والذي قد يؤدي إلى شلل في خدمات الإنترنت في بعض المناطق أو الدول.

ووقعت أحدث هجمات الحرمان من الخدمة في عطلة عيد الميلاد الماضي، حيث استهدفت مجموعة قراصنة تطلق على نفسها اسم "ليزارد سكواد" خوادم شبكتي "بلايستيشن نتوورك" التابعة لسوني، و"إكس بوكس لايف" التابعة لمايكروسوفت، وتم تعطيل الشبكتين وحرمان مستخدميهما من خدماتهما لعدة أيام.

خبير أمني في مايكروسوفت يستعرض خارطة توضح الاهتمام العالمي بشبكات "البوتنت" الخبيثة (رويترز)
بوتنت (Botnet)
وهي كلمة مركبة من "روبوت" و"نتوورك"، وتعني بالتالي "روبوت الشبكة"، وهي إحدى أبرز الوسائل المستخدمة في هجمات الحرمان من الخدمة الموزعة.
و"بوتنت" عبارة عن مجموعة البرمجيات الخبيثة المتصلة بالإنترنت التي تتواصل مع برامج أخرى شبيهة، بهدف أداء مهام معينة، وقد تكون المهمة عادية مثل التحكم بقناة الدردشة على الإنترنت(IRC)، أو خبيثة مثل استخدامها لإرسال بريد إلكتروني غير مرغوب فيه (سبام)، أو المشاركة في هجمات الحرمان من الخدمة الموزعة، لكنها عادة ما ترمز إلى الجانب الخبيث.
الاصطياد بالرمح(Spear phishing)
وهو نوع من أنواع هجمات الاصطياد التي تركز على مستخدم واحد أو دائرة داخل منظمة، يتم شنها من خلال انتحال هوية جهة جديرة بالثقة لطلب معلومات سرية، مثل أسماء تسجيل الدخول وكلمات المرور.

وغالبا ما تظهر هذه الهجمات على شكل رسالة إلكترونية من الموارد البشرية للشركة أو أقسام الدعم الفني فيها، وقد تطلب من الموظفين تحديث اسم المستخدم وكلمات المرور الخاصة بهم، وبمجرد حصول المخترق على تلك البيانات فإنه يستطيع الولوج إلى مصادر الشبكة.
وهناك نوع آخر من هجمات الاصطياد بالرمح التي تطلب من المستخدمين النقر على رابط، وعند النقر عليه يؤدي إلى نشر برمجية تجسس خبيثة يمكنها سرقة البيانات.
دودة الحاسوب (Computer Worm)
وهي برامج حاسوب خبيثة صغيرة قائمة بذاتها قادرة على استنساخ برمجيتها من أجل الانتشار إلى حواسيب أخرى، وعادة تستخدم شبكة حاسوب لنشر نفسها معتمدة على أخطاء أمنية في الحاسوب المستهدف للوصول إليه.
وعلى عكس فيروس الحاسوب، لا تحتاج الدودة لأن ترفق نفسها ببرنامج موجود كي تنتشر.
وهي تسبب عادة بعض الضرر للشبكة حتى لو كان ذلك باستهلاك عرض النطاق الترددي، في حين أن الفيروسات تعمل دائما تقريبا على إفساد أو تعديل الملفات المستهدفة.
وقد تستغل الدودة للقيام بأعمار تخريبية أو لسرقة بيانات خاصة ببعض المستخدمين أثناء تصفحهم الإنترنت، أو إلحاق الضرر بهم أو بالمتصلين بهم. وعادة يصعب التخلص منها نظرا لسرعة انتشارها وقدرتها على التلون والتناسخ والمراوغة.

ومن أمثلة هذه الدودة "دودة موريس"، التي تعتبر أول دودة حاسوب تنتشر عبر الإنترنت أطلقها طالب جامعي أميركي عام 1988 لمعرفة "مدى ضخامة الإنترنت" ،ورغم أن هدفه لم يكن خبيثا، فإن الشفرة ضمت عيوبا تسببت في مشاكل في استقرار الأنظمة المصابة لدرجة جعلها غير قابلة للاستخدام، وكانت النتيجة تعطيل نحو ستة آلاف حاسوب يونيكس في الولايات المتحدة، وأضرارا تراوحت بين عشرة ملايين ومائة مليون دولار.

دودة حاسوب "كود رد" انتشرت عام 2001 (غيتي-أرشيف)
حصان طروادة (Trojan Horse)
وهي شفرة برمجية صغيرة، وهي ليست فيروسا أو دودة حاسوب، لأنها لا تكرر ذاتها على النظام المحلي أو عبر شبكة الحاسوب، وإنما يتم إرفاقها مثلا برسالة بريد إلكتروني أو مع برنامج ذي شعبية عالية، وتقوم ببعض المهام الخفية لمنح المخترق حقوقا مميزة على النظام، في حين تتنكر كأنها برنامج سليم.
بمعنى آخر، تفتح شفرة حصان طروادة " باباخلفيا" في الحواسيب المستهدفة لتحولها إلى مسرح للمتسللين الذين يسعون للحصول على وصول غير مصرح به إلى الجهاز المستهدف، أي اختراقه، بهدف سرقة البيانات أو حذفها أو إرسال رسائل بريد إلكتروني باسم المستخدم أو حتى السيطرة على الشبكة بأكملها.

من أمثله أحصنة طروادة "ستورم" الذي ظهر عام 2007، واخترق آلاف الحواسيب، وكان يأتي على شكل ملف مرفق برسالة بريد إلكتروني عنوانها ملف مثل "230 قتيلا في عاصفة تضرب أوروبا"، وبمجرد فتح الملف المرفق يزرع حصان طروادة خدمة تدعى "وينكوم 32" تنتقل إلى حواسيب أخرى عبر الشبكة ليتحول كل حاسوب إلى "بوت" -الذي تم ذكره سابقا- في خدمة هدف خبيث.
ومن البرمجيات الخبيثة أيضا:
رانسوم وير: نوع من البرمجيات الخبيثة التي تقيد الوصول إلى نظام الحاسوب الذي تصيبه، وتطالب بـ"فدية" تدفع لصانعالبرمجية لإزالة هذا القيد.
آدوير: برمجية خبيثة تولد إعلانات بشكل تلقائي على جهاز المستخدم أثناء تصفح الإنترنت من أجل تحقيق ربح مادي لصانعها
سبايوير: برمجية خبيثة تساعد في جمع معلومات عن شخص أو منظمة دون علمهم، وترسل تلك المعلومات إلى طرف آخر دون موافقة المستخدم، أو تؤكد سيطرتها على جهاز حاسوب دون علم صاحبه.
المصدر : الجزيرة
كلمات مفتاحية: هجمات الحرمان من الخدمة دودة حاسوب حصان طروادة فيروس بوتنت برمجية خبيثة

اشهر القراصنة

رغم أن قراصنة الإنترنت ينتشرون حول العالم بشكر كبير ويعملون في أحيان كثيرة بصفة فردية، إما لتحقيق مكاسب مادية وأهداف خاصة، أو من أجل مصلحة عامة، فهناك في المقابل قراصنة يتكاتفون معا ليشكلوا باتحادهم مجموعات قرصنة على درجة كبيرة من الخطورة، وقد تكون دوافعهم ذاتية وربما تحركهم توجهات سياسية أو جهات حكومية.

وتعد مجموعة "أنونيموس" (المجهولين) أشهر هذه المجموعات، وهي تتألف من عدد كبير جدا من القراصنة المنتشرين حول العالم، والتي أصبحت ذات ثقل كبير في ما يسمى "الحرب الإلكترونية"، ونفذت العديد من الهجمات المؤثرة.

ومن أبرز هجماتها تسريب آلاف رسائلالبريد الإلكتروني الخاصة بالرئيس السوري بشار الأسد، ومهاجمة مواقع حكومية أميركية وبريطانية وأخرى للناتو، إلى جانب مهاجمتها مواقع إلكترونية حكومية إسرائيلية في كل مرة تشن فيها إسرائيل عدوانا عسكريا على قطاع غزة.

موقع إذاعة "بي بي سي" على تويتر كان ضمن المواقع التي اخترقها قراصنة الأسد (أسوشيتد برس)
الجيش الإلكتروني السوري
مجموعة من القراصنة اكتسبت حضورا على الساحة الدولية بعد بزوغ نجم الثورة السورية، لكن هؤلاء القراصنة يدينون بالولاء للحكومة السورية، ويستهدفون أي مواقع إلكترونية لا تتفق مع آرائهم، أو يرون أنها معادية للنظام في سوريا، أو أنها تدعم الثورة الشعبية.

وينسب للمجموعة نجاحها في اختراق عشرات المواقع الإلكترونية الإخبارية الشهيرة مثل موقع الجزيرة نت ووكالة أسوشيتد برس الأميركية ووكالة رويترز وصحيفة فايننشال تايمز البريطانيتين، وموقع منظمة هيومن رايتس ووتش الأميركية، وحتى موقع شركة البرمجيات مايكروسوفت، وغيرهاالكثير.
ويعتبر الجيش الإلكترونيالسوري أول جيش افتراضي في العالم العربي يشن بشكل صريح هجمات إلكترونية على خصومه.
الجيش الإيراني الإلكتروني
مجموعة قراصنة تشكل الذراع الهجومية في قوة إيران الإلكترونية، حيث تمكنت هذه المجموعة من شن عدد من الهجمات الناجحة، منها اختراق موقع التدوين الأميركي المصغر "تويتر" في ديسمبر/كانون الأول 2009، وعرض رسالة ذات توجهات سياسية جاء فيها

"تعتقد الولايات المتحدة أنها تتحكم وتدير الإنترنت لكنها لا تفعل، نحن من يتحكم ويدير الإنترنتبقوتنا".
كما اخترقت المجموعة ذاتها في يناير/كانون الثاني 2010 خدمة البحث على الإنترنت لمحرك البحث الصيني الشائع "بايدو"، فكان يتم تحويل مستخدمي محرك البحث إلى رسالة سياسية إيرانية.
وحدة جيش التحرير الشعبي الصيني 61486
وهي وحدة تابعة لجيش التحرير الشعبي الصيني ومقرها شنغهاي، يعتقد أنها مصدر العديد من هجمات الاختراق ضد شبكات حواسيب ومواقع إلكترونية، في إطار محاولات الصين سرقة أسرار تجارية وعسكرية من أهداف أجنبية.

وفي عام 2014، اتهم تقريرلشركة "كراودسترايك" الأميركية لأمن المعلومات هذه الوحدة باستهداف قطاعات الفضاء والاتصالات الأميركية وتطبيقات حاسوب إنتاجية معروفة، مثل "أدوبي ريدر" و"مايكروسوفت أوفيس" بهدف نشر برامج خبيثة عبر هجمات على البريد الإلكتروني
ليزارد سكواد
وهي مجموعة قراصنة عرفت باستهدافها خدمتي "بلايستيشن نتوورك" و"إكس بوكس لايف" الإلكترونيتين خلال عطلة عيد الميلاد 2014، وتسبب هجومها -وهو من نوع "الحرمان من الخدمة الموزع"- في حرمان الملايين من هواة ألعاب بلايستيشن وإكس بوكس من استخدام الخدمة على الإنترنت لعدة أيام.
وكانت المجموعة قالت إن هجومها كان من أجل "التسلية"، لكن يبدو أنه تحول لاحقا إلى فرصة لترويج خدمة مدفوعة الثمن من خلال أداة تتيح لمن يرغب في تعطيل أي موقع إلكتروني لفترة من الزمن.

مجموعة من أصدقاء معتقلين في مجموعة ردهاك التركية يطالبون بالعدالة لهم (غيتي)
مجموعات أخرى
إلى جانب المجموعات السابقة، هناك العديد من مجموعات القراصنة، منها ما ظهر ثم اندثر، ومنها ما استمر لكن بشكل أقل بروزا من الفترة التي اشتهر فيها، ومن هذه المجموعات:
ردهاك
وهي مجموعة قراصنة مقرهاتركيا تأسست عام 1997، تشن عادة هجمات ضد مواقع إلكترونية تابعة للحكومة التركية وتسرب وثائقسرية للحكومة التركية.
هنكر يونيون
وهي مجموعة معروفة بنشاطها في القرصنة، مقرهاالصين، أطلق أعضاؤها سلسلة من الهجمات على مواقع إلكترونية -أغلبها حكومية- داخل الولايات المتحدة.
نادي فوضى الحاسوب
تشكل في برلين سنة 1981، وله قواعد في ألمانيا ومناطق أخرى من العالم، واشتهر باختراقه خدمة للفيديو التفاعلي تتبع مكتب البريد الألماني، وكذلك اختراقه بنكا في هامبورغ وسرقة 134 ألف مارك ألماني قبل أن يعيد المبلغ كاملا في اليوم التالي، معلنا أن هدفه كان إثبات ضعف الأمن في شبكة الحاسوب.
المصدر : الجزيرة
كلمات مفتاحية: أنونيموس قراصنة إنترنتهاكر اختراق الجيش الإلكتروني السوري ليزارد سكواد

انواع القراصنة

يطلق مصطلح "هاكر" (قرصان إنترنت) لوصف الشخص ذي المعرفة العميقة بالحواسيب وشبكاتها والذي يملك مهارة عالية في لغات البرمجية وأنظمة التشغيل بحيث يستطيع بمهارته استغلال نقاط الضعف في أي شبكة حاسوب لاختراقها، وكانتالكلمة في الأصل تحمل معنى إيجابيا قبل أن تتحول إلى المعنى السلبي الذي تركز عليه وسائل الإعلام حاليا.
ويُقسّم قراصنة الإنترنت عادة إلى قسمين: القراصنة الأخلاقيون (القبعات البيض) والقراصنة المجرمون (القبعات السود) ويضاف إليهم أحيانا قسم ثالث هم أصحاب القبعات الرمادية.
القبعات البيض
هم القراصنة الذين يعملون في المؤسسات الحكومية وشركات أمن المعلومات أو حتى منفردين لاكتشاف ثغرات البرامج والأجهزة والشبكات، والإبلاغ عنها من أجل سدها ومنع استغلالها من قبل المخترقين المجرمين.

وأشهر شخصية على مستوى العالم من هذا النوع هو الهاكر كيفن ميتنيك الذي اعتبرته وزارة العدل الأميركية في يوم ما "أكثر مجرم حاسوب مطلوب في تاريخ الولايات المتحدة" واعتقل وسجن أكثر من مرة قبل أن يتحول إلى هاكر أخلاقي ويصبح مستشارا ومتحدثا عاما في أمن الحاسوب ومديرا لشركة "ميتنيك للاستشارات الأمنية".

لامو تعاون مع الجيش الأميركي لاعتقال مطلوب بتهمة تسريب بيانات سرية لويكيليكس (رويترز)
وهناك القرصان أدريان لامو (المعروف باسم الهاكر المشرد) الذي كان يستخدم المقاهي والمكتبات ومقاهي الإنترنت أماكن لتنفيذ اختراقاته لمواقع إلكترونية لشركات شهيرة مثل نيويورك تايمز ومايكروسوفت وياهو، لكنه تحول أخيرا إلى هاكر أخلاقي ويعمل مستشارا بأمن الحاسوب وساعد في تسليم سلطات الجيش الأميركي برادلي مانينغ المتهم بأنه مصدر تسريب فيديو غارة جوية على بغداد إلى موقع نشر الوثائق السرية الشهير ويكيليكس في يوليو/تموز 2007.
ومن القراصنة البيض أيضا "ستيف وزنياك" الشريك المؤسس لشركة أبل الشهيرة، ولينوس تورفالدس مطور نظام التشغيل مفتوح المصدر "لينوكس"، وتيم بيرنرز-لي العقل المبدع وراء تطوير الشبكة العنكبوتية العالمية، وجوليان أسانج مؤسس موقع ويكيليكس.
القبعات السود
وهم النوع الشائع الذي تركز عليه عادة وسائل الإعلام، ويخترقون أمن الحاسوب من أجل مكاسب شخصية مثل سرقة بيانات بطاقات الائتمان أو البيانات الشخصية من أجل بيعها، أو حتى من أجل المتعة الذاتية مثل صنع روبوتات برمجية (بوتنت) يمكن استخدامها لشن هجمات الحرمان من الخدمة الموزعة ضد مواقع إلكترونية معينة.

مكينون تسبب بأضرار لأنظمة الجيش الأميركي قدرت بسبعمائة ألف دولار (رويترز)
ومن أشهر هؤلاء القراصنة البريطاني غاري مكينون المتهم بتنفيذ أكبر عمليات اختراق ضد شبكات حواسيب حكومة الولايات المتحدة من بينها أنظمة حواسيب الجيش والقوات الجوية والبحرية وإدارة الطيران والفضاء (ناسا) وتسبب بأضرار لأنظمة الجيش قدرت بسبعمائة ألف دولار.
وإلى جانب مكينون، هناك جونثان جيمز (المعروف باسم كومريد) الذي اخترق وهو في الـ 15 عاما من عمره شبكة ناسا ووزارة الدفاع الأميركية.
وجورج هوتز الذي يعرف بكونه مخترق منصة ألعاب سوني بلايستيشن 3 عام 2011. وكيفين بولسون (المعروف باسم دارك دانتي) وهو أحد قراصنة الثمانينيات ذوي القبعات السود، واكتسب سمعته تلك لاختراقه خطوط الهاتف لمحطة إذاعة في لوس أنجلوس للفوز بجائزة كانت عبارة عن سيارة بورش 911 جديدة من ضمن جوائز أخرى.
وهناك ألبرت غونزاليس الذي اتهم بأنه العقل المدبر في أكبر سرقة لأجهزة الصراف الآلي وبطاقات الائتمان بالتاريخ، حيث يعتقد أنه وجماعته من القراصنة باعوا خلال الفترة من 2005 إلى 2007 أكثر من 170 مليونا من أرقام بطاقات الصراف الآلي وبطاقات الائتمان.

والروسي فلاديمير ليفين الذي تمكن عام 1994 مستخدما حاسوبه المحمول في شقته بمدينة سانت بطرسبرغ من تحويل عشرة ملايين دولار من حسابات عملاء في بنك "سيتي بانك" إلى حساباته الشخصية حول العالم، وبعد اعتقاله تمت استعادة المال المسروق باستثناء أربعمائة ألف دولار.
وهناك روبرت تابان موريس الذي أطلق في الثاني من نوفمبر/تشرين الثاني 1988 دودة حاسوب (برمجية خبيثة) عطلت نحو عُشر الإنترنت وأكثر من ستة آلاف نظام حاسوب، وقدرت قيمة الخسائر المالية لهذه العملية بنحو 15 مليون دولار.
القبعات الرمادية
وهم القراصنة الذين يقومون بأعمال قانونية أحياناً، أو بمساعدة أمنية كما يملي عليهم ضميرهم أحياناً، أو باختراق مؤذ في أحيان أخرى، وهم لذلك مزيج من القراصنة ذوي القبعات البيض وذوي القبعات السود، وهم عادة لا يخترقون لأغراض خبيثة أو لمصلحة شخصية، بل لزيادة خبراتهم في الاختراق واكتشاف الثغرات الأمنية.

المصدر : الجزيرة

جمع و ترتيب

ترجمان عربى

https://www.facebook.com/mohuomha.mo