الفصل الخامس

المخترقون (الهاكرز)

Chapter five

Hackers

المخترقون (الهاكرز)

تعريف المخترق أو الهاكر

هو الشخص الذي يتملك القدرة على كتابة البرامج وتصميمها و تحليل النظم، لديه الخبرة الكافية بلغات البرمجة وانظمة التشغيل، يتقن استخدام البرامج والإبحار والتجول بمواقع الشبكة العنكبوتية (الاننرنت)، يؤمن بوجود أشخاص آخرين يستطيعون القرصنة يمتاز بالسرعة في كتابة البرامج، يعتبر ذكي وعبقري بالوصول الى اجهزة الافراد والمؤسسات والولوج بمواقع الانترنت والتحايل على انظمة التشغيل وانتحال الشخصيات كما يعرف بخبث النيات.

أنواع الهاكزر

Cracker

المخترق الذي يستخدم البرامج او التقنيات في محاولات لاختراق الأنظمة او الأجهزه للحصول على معلومات سرية والتخريب وحذف أو إضافة معلومات، كان هذا الاسم يطلق على كل من يحاول إزالة أو فك الحماية التي تضيفها شركات إنتاج البرمجيات على برامجها لمنع عمليات النسخ غير القانوني، أما الأن تم تصنيف هذا النوع من المخترقين في فئه خاصة سميت بالقراصنة (Pirates).

Phreak

المخترق الذي يحاول التسلل عبر شبكات الهاتف اعتماداً على أساليب تقنية غير قانونية أو التحكم بهذه الشبكات ويستخدم أدوات خاصة مثل مولدات النغمات الهاتفية لذا قامت شركات الهاتف باستخدام المقاسم أو البدالات الرقمية عوضا عن الكهروميكانيكية القديمة.

مؤلفوا الفيروسات Crackers

يقوم هذا النوع من المخترقين بتصميم الفيروسات بغرض التخريب وتدمير الاجهزه يعتبر المحللون النفسيون أن من ينتمي إلى هذا النوع من المبرمجين مصاب بمرض عقلي أو نفسي يدفعه إلى هذه العمليات التخريبية التي لا يجني منها أي فائدة شخصية، يعتبر هذا النوع من أخطر الانواع .

Cypherpunks

يحاول هذا النوع من المخترقين الحصول على أدوات وخوارزميات التشفير المعقدة والقوية وتوزيعها بصورة مجانية حيث تسمح هذه الأدوات بإجراء عمليات تشفير لا يمكن فكها إلا باستخدام أجهزه كمبيوتر فائقة.

Cyberpunk

تطلق هذه التسمية على كل من يستخدم مزيجا من الطرق السابق ذكرها للقيام بعمليات غير قانونية.

Anarchists

هذا النوع هو الذي يروج معلومات مخالفة للقانون او مشبوهة مثل طرق ترويج صناعة المخدرات أو المواد المتفجرة أو قرصنة القنوات الفضائية.

أنواع المدمرين(الكراكز)

هم المخربين لأنظمة الكمبيوتر ينقسمون إلى قسمين:

- **المحترفون** : هم إما إن يكونوا ممن يحملون درجات جامعية عليا بتخصص الكمبيوتر والهندسة المعلوماتية ويعملون بمجال تحليل النظم والبرمجة، يكونوا على دراية ببرامج التشغيل ومعرفة عميقة بخباياها والثغرات الموجودة فيها.

تنتشر هذه الفئة غالبا بأمريكا وأوروبا، لكنها أخذت بالانتشار في المنطقة العربية **لايعني هذا أن كل من يحمل شهادة عليا بالبرمجة هو من المدمرين(الكراكز)**، لكنه إذا أقتحم الأنظمة عنوة مستخدما أسلحته البرمجية العلمية في ذلك فهو بطبيعة الحال احد المحترفين.

- **الهواة:** إما أن يكون احدهم حاملا لدرجة علمية تسانده في الإطلاع على كتب بلغات أخرى غير لغته كالأدب الإنجليزي أو لديه هواية في تعلم البرمجة ونظم التشغيل دءوب على استخدام البرامج والتطبيقات الجاهزة لكنه يطورها حسبما تقتضيه حاجته ربما يتمكن من فك شفرتها البرمجية ليتم من نسخها وتوزيعها بالمجان.

هذا الصنف ظهر كثيرا في العامين الآخرين على مستوى المعمورة و مما ساهم في انتشاره العوامل الآتية:-

- انتشار البرامج المساعدة وكثرتها وسهولة التعامل معها.
- ارتفاع أسعار البرامج وتطبيقات الكمبيوتر الأصلية التي تنتجها الشركات مما حفز الهواة على إيجاد سبل أخرى لشراء البرامج الأصلية بأسعار أقل بكثير مما وضع ثمنا لها من قبل الشركات المنتجة.

ينقسم الهواة إلى قسمين:

١- **الخبير:** هو شخص يدخل للأجهزة دون إلحاق الضرر بها، لكنه يميل إلى السيطرة على الجهاز و يتحكم به عن بعد مثل تحريك الفأرة (Mouse) وفتح مشغل الأقراص ذلك بقصد السيطرة لا أكثر .
٢- **المبتدأ:** أخطر أنواع الكراكرز جميعهم لأنه يحب أن يجرب برامج الهجوم دون أن يعرف طرق تطبيقها فيستخدمها بشكل عشوائي لذلك يقوم أحيانا بالتدمير والتخريب دون آن يدري ما يفعله.

الكراكرز بالدول العربية

للأسف الشديد كثير من الناس بالدول العربية يرون بان الكراكرز هم أبطال بالرغم أن العالم كله قد غير نظرته لهم فمنذ دخول خدمة الانترنت للدول العربية في العام ١٩٩٦ تقريبا والناس يبحثون عن طرق قرصنه جديدة، ذكرت آخر الإحصائيات بان هناك أكثر من ٨٠ % من المستخدمين العرب تحتوي أجهزتهم على ملفات الباتش، هي ملفات تسهل عمل الكراكرز .

الكراكرز بدول الخليج العربي

انتشرت ثقافة الكراكرز كثيرا بدول الخليج العربي خصوصا بالسعودية على الرغم من الدخول المتأخر لخدمة الانترنت حيث كان في (يناير ١٩٩٩) حيث كثرت الشكاوى من عدة أفراد و شركات و قد بين الاستبيان الذي أجرته مجلتين عربيتين متخصصتين هما **بي سي و انترنت العالم العربي** إن بعض الأجهزة بالدول الخليجية تتعرض لمحاولات اختراق مرة واحدة على الأقل يوميا.

مواقف و احداث مع المخترقين و المدميرين

- أحد الهاكرز دخل على الجهاز الشخصي لإحدى الفتيات، أخذ يشاهد ما يحتويه من صور وملفات ولفت انتباهه ان الكاميرا موصلة بالجهاز فأصدر أمر التصوير فأخذ يشاهدها وهي تستخدم الكمبيوتر ثم أرسل لها (رسالة يخبرها فيها انها جميلة جداً).
- أحد الهاكرز دخل إلى جهاز فتاة يهودية، أخذ يحاورها حتى انه بعد ذلك اكتشف انها بنت مسئول كبير في إسرائيل، عندما عرف بذلك ظل لمدة شهراً لا يدخل الانترنت خوفا من القبض عليه.
- أحد الهاكرز المحترفين اعتاد ان يدخل على مواقع البنوك عبر الانترنت يتسلل بكل سلاسة إلى الأرصدة والحسابات فيأخذ دولار واحد من كل غني ويضع مجموع الدولارات في رصيد أقل الناس حساباً.
- اعتاد الهاكرز على محاولة اختراق المواقع الكبيرة مثل موقع الياهوو وموقع مايكروسوفت لكنهم دائماً ما يفشلون في مراميهم هذه بسبب الجدران النارية التي تضعها هذه الشركات والإجراءات الضخمة التي تتبعها لمنع أي هاكرز من دخول النظام، مع هذا ينجح الهاكر في اختراق النظام لكن خلال أقل من خمس دقائق يستطيع موظفوها من إعادة الأمور إلى مجراها.

الآن تحولت الحروب من ساحات المعارك إلى ساحات الانترنت والكمبيوتر، أصبح الهاكرز من أقوى وأعتى الجنود الذين تستخدمهم الحكومات، خاصة (المخابرات) حيث يستطيعون التسلل بخفية إلى أجهزة و أنظمة العدو وسرقة معلومات لا تقدر بثمن، كذلك تدمير المواقع وغير ذلك.

الفرق بين الهاكرز (المخترقين) والكراكز (المدمرين)

الهاكرز (المخترق): هو الشخص الذي يستمتع بتدمير البيانات، لدية معرفه بأنظمة التشغيل يكون في الغاب مبرمج، على سبيل المثال يحصل على المعلومات والمعرفة من خلال خبرتهم بأنظمة التشغيل ولغات البرمجة، يكتشف الثغرات في أنظمة التشغيل وأسبابها، هو باستمرار يبحث مطولاً عن المعلومة، يشارك بما يكتشف دائماً بهدف تدمير البيانات.

المدمر(الكراكز): هو الشخص الذي يدمر أمن وسلامة الأنظمة عن طريق أهداف خبيثة النية ليس لديه الصلاحية وغير مخول، ليس لديه صلاحية الوصول ويدمر المعلومات وينتهك الحقوق الشرعية وخدمات المستخدمين وخصوصياتهم من أجل أهدافه، بسهولة يمكن التعرف عليه بسبب أعماله الماكرة.

أشهر المدمرين (الكراكز) في العالم

كيف متنك المعروف بكندور (condor) Kevin mitnik

عرف عالمياً بالكراكز، نجح منذ سنواته الأولى باختراق المواقع الأجنبية العسكرية بالإضافة لمواقع الشركات المالية والشركات المنتجة للبرمجيات والشركات التقنية الأخرى حيث كان في سن المراهقة، قام باختراق قاعدة الطيران الحربي لأمريكا الشمالية.

كيفن بولسن Kevin poulsen

اتبع أسلوب متنك و سار على خطاه، اشتهر بقدراته العالية وسيطرته على أنظمة شبكات الهاتف التابعة لشركة باسفك بل، يعد الوحيد الذي استخدم موهبته من اجل الربح حيث قام بتبديل خطوط الهاتف والتجسس على المكالمات الهاتفية والاستفادة من ذلك مالياً، اخترق جميع أنواع المواقع أشهرها مواقع الدفاع الحربي، أخر 5 سنين من حياته العملية في هذا المجال تم اعتقاله وزجه في السجن 1996.

بترسون Justin Tanner Peterson

اشتهر بترسون والمعروف بالعميل، كان يعمل في الخفاء اخترق وكالة ائتمان بارزة، تم القبض علية على معاونيه، منهم كيفن باولسون، بعدها ابرم صفقة مع وكالة الاستخبارات الأمريكية ليعمل بموجبها عميلاً لصالحهم، ترتب على ذلك أطلاق سراحه مما مكنه من الهرب و لاذ بالفرار وانخرط في سلسلة من الجرائم التي انتهت أخرها بالفشل، كانت هذه الجريمة محاولة سرقة الأموال ذلك عن طريق سرقة أرقام الحسابات الخاصة بأفراد وتحويل أرصدة حساباتهم لصالحه.

أشهر هؤلاء الهكرة الهاكر الأكبر متنيك

أُطلق حديثاً سراح كيفن ميتنك "الهاكر" الذي أقض مضاجع عدة مدن أمريكية باختراق أنظمة الكمبيوتر بعد أن أمضى في السجن مدة تقارب خمس سنوات، على الرغم من أن ميتنك البالغ من العمر 36 عاماً استعاد حريته إلا أنه لم يتمكن قبل مرور 3 سنوات من استخدام أجهزة الكمبيوتر بدون إذن من الضابط المشرف على مراقبته، بالإضافة لذلك الشروط التي وضعت لإطلاق سراحه سوف تحد من إمكانية حصوله على وظيفة مناسبة إذ أن معظم الشركات و المؤسسات تشترط إجادة استخدام الكمبيوتر لتعيين الموظفين، تقتضي شروط إطلاق سراح الهاكر الأكبر أن يمتنع عن استخدام البريد الإلكتروني، هو ما يعني أن عليه استخدام وسائل الاتصال التقليدية مثل الهاتف العادي للاتصال بأصدقائه و أفراد عائلته.

أدلى ميتنك ببيان طويل أمام حشد من الصحفيين خارج السجن هاجم فيه الذين قدموه للمحاكمة وجون ماركوف محرر صحيفة نيويروك تايمز بسبب تغطيته غير العادلة للقضية.

قال في بيانه "لقد تم التلاعب بأفعالي وحياتي منذ كنت في السابعة عشرة من عمري"، صورتها الصحافة بشكل خاطئ (القصة موجودة على موقع www.freekevin.com على شبكة الإنترنت)، قضيتي مجرد قضية حب استطلاع فقد كنت راغباً في معرفة كل ما يمكن عن كيفية عمل شبكات الهاتف ومدخلات ومخرجات الأنظمة في شبكات الكمبيوتر، لا يوجد أي دليل من أي نوع في هذه القضية ولم يكن لدي نية في أن احتال على أي شخص".

وصف رجال السلطات التنفيذية و القضائية ميتنك بأنه شخص خطير أحس بطعم القوة من خلال جهاز الكمبيوتر، كان لدى ميتنك هاجس قوي يدفعه للدخول إلى أنظمة الكمبيوتر لسرقة الملفات والتلاعب بالبرمجيات، على سبيل الاستعراض منذ أن كان يعيش في منطقة لوس أنجلوس في سن المراهقة حسب ما قال كريستوفر بينتر مساعد المدعى العام الذي تولى الادعاء في القضية عام 1995.

قال بنتر إن أول اصطدام له مع القانون كان عام 1981 وهو في السابعة عشر من عمره حيث ألقي القبض عليه بسبب السطو على محتويات أجهزة كمبيوتر شركة Pacific Bell في لوس أنجلس و حوكم على تلك الفعلة كحدث و حُكم عليه بالخضوع للمراقبة، بعد عام من تلك الحادثة ألقي القبض عليه مجدداً و هو متلبس باقتحام نظام الكمبيوتر في جامعة Sothern California سجن جراء تلك الفعلة لمدة ستة أشهر.

ألقي القبض عليه عدة مرات إلا أنه بعد إلقاء القبض عليه عام 1988 بسبب أعمال "الهكر" تمكن محاميه من إقناع القاضي أن حالته شبيهة بحالة مدمني المخدرات أو مدمني القمار و حكم عليه لذلك بالسجن لمدة عام في سجن لومبوك الفيدرالي المخصص لمرتكبي الجنح والجنايات البسيطة خضع بعد إطلاع سراحه لعلاج نفسي يشبه العلاج المكون من اثنتي عشرة خطوة المطبق على مدمني المشروبات الكحولية.

لكن ميتنك سرعان ما خرق شروط إطلاق سراحه، أصدرت على إثر ذلك مذكرة توقيف بحقه اختفى من العام 1992 عن الأنظار وتحول إلى العمل سراً.

شك رجال مكتب التحقيقات الفيدرالي لثلاثة أعوام في أن ميتنك ظل يمارس عمله المفضل في اختراق أنظمة الشركات التي تعمل في صناعة البرمجيات ومزودي خدمة الإنترنت والمؤسسات التعليمية بما في ذلك كل من Nokia, Motorola, Colorado Supernet, Netcom NEC, Novell, Fujistu, USC وصن ويمايكروسيستمز.

نجح ميتنك في التهرب من السلطات حتى العام 1995 حين اخترق ملفات الكمبيوتر التي تعود للباحث تسيموتو شيمومورا الذي يعمل مستشاراً لمكتب التحقيقات الفيدرالي والقوى الجوية ووكالة الأمن

القومي الأمريكية ومطوراً برامج الكمبيوتر الخاصة بحماية نظم شبكات الكمبيوتر من الاختراق تموله الحكومة الاتحادية.

تمكن شيمومورا، خبير بشؤون الأمن من اقتفاء أثر ميتنيك في مدينة راليا كارولينا الشمالية بعد شهرين من حادثة الاختراق.

ألقي القبض على ميتنك في فبراير 1995 واحتجز على ألا يطلق سراحه بكفالة مالية، قضى حوالي أربع سنوات في مركز احتجاز Metropolitian Detention Center في لوس أنجلوس منتظراً محاكمته أمام محكمة فيدرالية، اعترف في السادس والعشرين من مارس أنه مذنب في سبع من التهم الموجهة إليه بشأن اعتراض اتصالات سلكية بشكل غير قانوني والتحايل على الأنظمة باستخدام الكمبيوتر، حكمت المحكمة الفيدرالية عليه بالسجن لمدة ستة أشهر في سجن لومبوك الفيدرالي تحت إجراءات أمن متوسطة.

كان شيمومورا والسلطات الفيدرالية سعيدين بالقبض على ميتنك الذي قام كثير من أنصاره بالدفاع عنه بعدة طرق منها افتتاح موقع Kevin Free على شبكة الإنترنت.

قال رونالد راندلولف المحامي المعين للدفاع عن ميتنك إن القبض عليه قد يؤدي إلى نتائج عكسية يؤدي لظهور نوع جديدة من "الهكرة".

قال راندولف: " إن الحكومة لم تميز في المحاكمة بين إرهابيي الكمبيوتر وبين المتحايل بالكمبيوتر، أنه لن يستطيع أحد تقدير الفرق بين الاثنين إلا الأجيال التي ستأتي بعد عقود".

انتقد راندولف السلطات لتضخيمها قدرات ميتنك و قال: " لم يسلب الرجل أياً من مالكي الأجهزة حقهم في استخدام أجهزتهم كل ما فعله أنه تلصص عليها، لم يستطع المدعون أن يعترفوا بأنهم يحاكمون متلصصاً فاتبعّوا الأسطورة التي خلقوها"، إلا أن بينتر مساعد المدعي العام الذي تولى الادعاء في القضية قال إن ميتنك كان أكثر من متلصص على ملفات الآخرين، قال: "لم نعالج هذا القضية لنجعل من ميتنك مثالاً بل لأن سلوكه اقتضى من المجتمع أن يحاكمه فهو أحد أخطر "الهكرة" القادرين على اختراق أنظمة الكمبيوتر كما هو ثابت من سوابقه".

الطريف في الأمر أن شيمومورا و ماركوف محرر جريدة تايمز ألفا كتابا عن ميتنك بعنوان Takedown.