الأمن الالكتروني

الأمن الإلكتروني

تقوم الأجهزة الأمنية لمختلف البلدان بالبحث عن العباقرة في مجال الحاسوب بهدف الصراع ضد الإرهابيين والمجرمين. حتى إن ممثلي أجهزة الأمن في الولايات المتحدة الأمريكية شاركوا خلال الصيف الماضي باجتماع دولي لقراصنة الانترنيت في مدينة لآس فيغاس. إن التهديد باستخدام الشبكة العنكبوتية أصبح أكثر فأكثر امرا واقعيا.

فـأي مـن المؤسسـات والتشـكيلات تقـع فـي "منطقـة الخطر" وعليها الدفاع ضد الهجمات الالكترونية؟ ومن يهدد امن الدول وسلامة المواطنين باستخدام الانترنيت عـدا الإرهـابيين؟ وهـل تمتلـك البلـدان المختلفـة اختصاصيين جاهزين للحرب في الانترنيت؟ عن هذه الأسئلة وغيرها يجيب ضيوف برنامجنا.

معلومات عامة حول الموضوع:

ماالذي يمكن إن يقوم به القراصنة؟

الكوارث تتوالى في المؤسسات الصناعية الكبرى، وحركة المرور متوقفة. وأجهزة التحكم الإلكترونية معطلة. لا معلوماتٍ ولا اتصالات. الجيش والأسطول مشلولان. مجرمون مجهولون يستولون على إدارات السيطرة والتحكم في البني العسكرية الدفاعية دون إن يطلقوا رصاصة واحدة. ويوجهون الصواريخ النووية على هواهم.

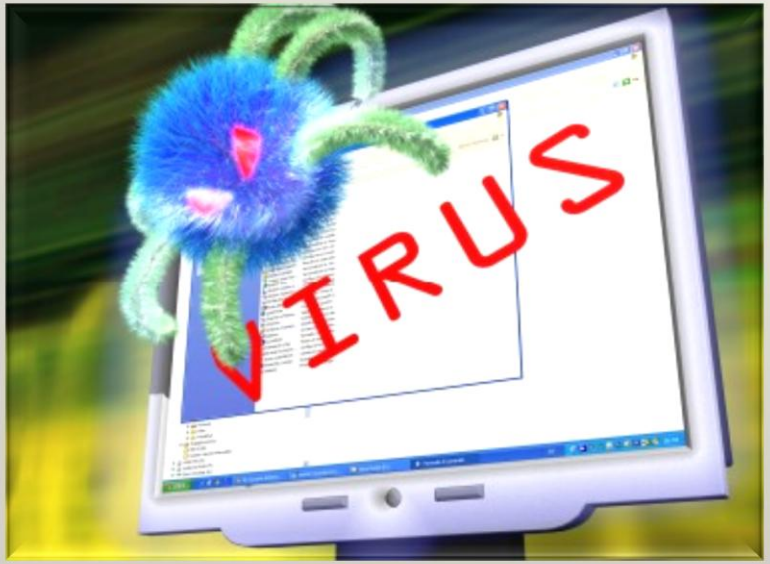
هذا ليس فيلما من أفلام هوليود. كلا. فإن كارثة كهذه يمكن إن تحصل، الآن، في أية لحظة. سلاح الهجوم جاهز، وتُجرى عليه تحسينات متواصلة. انه الحاسوب، الكمبيوتر... وجنود هذه الحرب الإلكترونية هم "الهاكرز".

هذه المفردة باتت مرادفة لكلمات مجرم الحاسوب... مخترق الكمبيوتر. إلا إن لها معنى ايجابيا بين الهاكرزأنفسهم. ويقصدون بها مصمم برامج الكمبيوتر.

ما يفعله ويبدعه الهاكر يتوقف على الجهة التي تدفع له. فهو يمكن إن يضع برامج تطبيقية نافعة ويمكن إن يضع برامج تجسسية. والحقيقة فإن مخترق الكمبيوترات لا يختلف بشئ عن اللص العادي، والفارق الوحيد انه لا يفتح قفل الباب بل يدخل بوقاحة كمبيوترات الغير، ويسرق المعلومات بدلا من الحاجيات.

كبار المجرمين في عالم المال والأعمال يجندون الهاكر اليوم لسرقة أموال منافسيهم أو إلحاق الضرر بهم. وتنتشر أكثر فأكثر سرقة البنوك من خلال الشبكة العنكبوتية، ما يسمى انترنت بانكينغ. وقد ظهر رأسا جمهور كبير جدا من الراغبين في الإثراء من سرقة واختطاف المعلومات المصرفية. الهاكر الخبيث، مصمم برامج التجسس على البنوك، يضع يده على شفرة كود دخول أو وصول شخص أو عدة أشخاص إلى الحسابات المصرفية الشخصية ويحوّل المبالغ منها إلى الحسابات والعناوين التي يريدها.

وهناك اتجاه أحدث. الهاكر يستولي على موارد الإنترنت الحيوية بالنسبة للشركة المنافسة. ويمكن إن تكون تلك الموارد أو المصادر بشكل موقع الكتروني لمتجر يبيع من خلال الإنترنت أو دار نشر أو كازينو إلكتروني. يقوم الهاكر بمهاجمة الموقع فيعطله. ويبعث رسالة إلى صاحبه يطالبه فيها بكلفة الهجوم، وإلا فإن الهجوم سيتكرر. ذلك في الحقيقة نوع من أنواع الابتزاز المعهود، ولكن على النطاق الدولي.



هجمات الفيروسات يمكن إن تضر بأناس لا علاقة لهم بالتقنيات الرقمية. فالمعلومات المتعلقة بالرواتب والأجور والمعاشات والمعونات الاجتماعية والمرافق والخدمات تحفظ في أجهزة الحاسوب. ولذا فإن إي عطل في الشبكة الموضعية أو المحلية لدائرة حكومية يمكن إن يضر بمئات الآلاف من الناس.

عمل الطالبة:قمزة علي القريصي

الصف:الحادي عشر.