الهاكرز.. أفعى تقتل.. وتنجي !

الأربعاء، ٢٣ يناير ٢٠٠٨
بدور الدمخي

الشبكة العنكبوتية هكذا يطلق عليها كونها تشكل نسيجا من المعلومات والمعرفة، إلا أن أضرارها أصبحت أكثر من فوائدها التي يجب علينا نحن الشباب الاستفادة منها واستغلالها بما يعود علينا بالمنفعة. ولعل وجود ضعاف النفوس ولّد قلقا وخوفا لدى المستخدمين من الشباب والفتيات نتيجة الإختراقات والتهديدات وانتهاكهم لخصوصيات الغير. ولعل السؤال الذي يطرح نفسه كيف يقومون بمثل هذا الفعل؟ وكيف يحصلون على مبتغاهم من ضحايا الإنترنت؟ وما سبب هذه الأعمال التي تتنافى مع أخلاق الشباب الواعد وأجيال المستقبل؟ هذه التساؤلات وغيرها من الاستفهامات كان لابد من البحث عن إجابة لها من خلال تجارب هؤلاء:

وقام كل من الهاكرز يوسف الجارد وعبدالله الجارد وعبدالله الرخيمي بالإجابة عنها بصورة ميسرة تمكن القارئ من استيعابها..

يقول يوسف الجارد : كانت بدايتي مع برنامج المحادثة الكتابية الـMIRC سنة ١٩٩٨ حيث كانت لغة الكتابة الإنجليزية المعربة ولم نستطع وقتها إدخال اللغة العربية في هذا البرنامج وكنت اقضي من ٤ - ٥ ساعات في اليوم وكنت أقوم بعمل سكربتات حماية ضد المسيئين للبرنامج.

ويرى يوسف أن مراقبة الأهل لأبنائهم امر ضروري عن طريق وضع برنامج يحفظ كل مايكتب في جهاز الكمبيوتر مما يساعدهم في عملية المراقبة والمتابعة.

واذا ما رأى شبابا يتصفحون الإنترنت لإلحاق الضرر بالآخرين يقول عبدالله الجارد: نعم بل الكثير منهم لايهدف من الإنترنت إلا إلحاق الأضرار ومنها السرقة فعلى سبيل المثال كنت مشتركا في إحدى شركات الإنترنت، في بعض الأحيان، عندما أحاول إدخال الرقم السري لم يكن يعمل وبالاتصال بالشركة أكدوا لي أن الحساب يعمل وعند التحقق من الشركة الرئيسية في الولايات المتحدة الأميركية اتضح أن هناك شخصا قد سرق الرقم السري وبدأ باستخدام حسابي دون علمي مما كلفني مبالغ عالية. وعن الهدف من وراء هذه الأفعال يقول :إن الهدف للمتعة أو المصالح الشخصية وأحيانا لممارسة السلطة على الغير. ويضيف قائلا: من يقم بإلحاق الضرر بالآخرين يدع الهاكر ولكن ليس كل هاكر يقوم بإزعاج الآخرين فنحن هاكرز نقوم ببعض الأعمال الإيجابية وأحيانا للتسلية.

أما عبدالله الرخيمي فيوضح ما يقوم به الهاكرز قائلا: يقوم باختراق الأجهزة الأخرى والصفحات. ويحتاج الهاكر إلى مايدعى بالـIB Address وأن يكون الـPort مفتوحا ليتمكن من دخول الجهاز والعبث به أو يمكنه استخدام برنامج آخر لدخول الأجهزة عندها يمكنني وضع رقم سري خاص بي لدخول الجهاز في أي وقت أريد ولكن من الضروري فتح الـPort ويمكننا ذلك من خلال إرسال أو استقبال ملف من الضحية.

عملية الاختراق

يقول عبدالله الجارد :تعلمت الاختراق من قريب لي متمرس في هذه العملية حيث قمت بمراقبته ثم أدمنت الاختراق وقد بدأت ببرنامج يدعى Sub 7 ثم برنامج Prorat ثم أحضر اصدقائي لي الـ IB Addresses والـ port ثم بدأت بالاختراق.

خصوصية الانترنت

يعرض الدكتور صلاح الناجم المتخصص في علم لغة الحاسوب بحثا عن الخصوصية المرتبطة بشبكة الإنترنت حيث ورد في نص البحث : برزت إلى الساحة جرائم جديدة تتعلق بخصوصية المعلومات أهمها جريمة سرقة الشخصية Identity Theft ، حيث إن هذه الجريمة تكلف المستخدمين خسائر تقدر بقرابة ٤ بلايين دولار سنويا وتكلف الشركات قرابة ٣٣ بليون دولار سنويا. فلكل مستخدم خصوصية يجب أن تكون محمية باستخدام التقنيات والاحتياطات الأمنية Security Counter Measures.كما يجب أن يكون للمستخدم دور في عدم تعريض خصوصيته للخطر عن طريق زيادة الوعي وتجنب مخاطر ما يعرف بالهندسة الاجتماعية Social Engineering.

وذكر في البحث بعض الأحصاءات المخيفة منها: استنادا إلى تقرير حديث نشر في مجلة نيوزويك، يستطيع لصوص الشخصية الحصول على ٥٥ بليون دولار سنويا في الولايات المتحدة الأميركية فقط .

استنادا إلى وكالة التجارة الفيدرالية الأميركية، ٢٨ بالمائة من شكاوى الاحتيال تتعلق بسرقات بطاقات الائتمان.

استنادا إلى مجلة نيوزويك، تعتبر جريمة سرقة الشخصية أسرع الجرائم نموا في الولايات المتحدة الأميركية.

استنادا إلى مجموعة Gartner لأبحاث تكنولوجيا المعلومات ، تم اكتشاف جريمة واحدة من كل ٧٠٠ جريمة سرقة شخصية.

استنادا إلى مجموعة the Anti-Phishing Working Group يتزايد عدد جرائم الاحتيال الإلكتروني Phishing عن طريق البريد الإلكتروني بمقدار ٤٠ إلى ٥٠ بالمائة شهريا.

ومثلما تعاون عبدالله الجارد وعبدالله الرخيمي ويوسف الجارد على تعلم الاختراق فالدكتور صلاح الناجم ابدى تعليقه على هذه الأنواع من الاختراقات قائلا: تجدر الإشارة هنا إلى أن الاتجاه الآن في مجال السرقة الجماعية. بدلا من سرقة الشخصيات بشكل مفرد. حيث يصل الآن عدد الشخصيات المسروقة إلى الملايين في العملية الواحدة. ومن قبل شهور اكتشفت مؤسسة تعنى بشؤون أمن المعلومات أن أحد أجهزة الحاسوب المركزية Servers في الولايات المتحدة الأميركية كان يستخدم في تخزين كلمات سر خاصة بحسابات ٥٠ بنكا إضافة إلى حسابات eBay و PayPal. كما كان هذا السيرفر يضم أرقام بطاقات ائتمان. كل هذه المعلومات تمت سرقتها عن طريق فايروس Trojan.

ويتابع قائلا: في يونيو ٢٠٠٥ استطاع مجرمون متخصصون في سرقة الشخصية اختراق أنظمة شركة أميركية متخصصة بمعالجة معاملات بطاقات الائتمان وسرقة أرقام ٤٠ مليون بطاقة ائتمان (Discover, Visa, MasterCard and American Express) نتيجة لثغرة أمنية في الحاسوب المركزي Server لديهم.

مثلما أن السرقة أصبحت جماعية، فان توزيع المعلومات المسروقة صار جماعيا. مايجب الالتفات إليه هنا هو أن المجرمين الآن بعد القيام بسرقة الشخصية، يبدأون ببيع تلك المعلومات المسروقة بشكل واسع عن طريق :

غرف المحادثة Chat Rooms ،غرف الرسائل الآنية Instant Messaging ،الويب

وعلى سبيل المثال، إحدى منظمات الاختراق Hacking الإجرامية وضعت إعلانا على الانترنت يعرض ٣٠٠ بطاقة ائتمان مسروقة مع أرقامها السرية المطبوعة خلف البطاقة بسعر ٢٠٠ دولار. كما يقول الإعلان انك تستطيع الحصول على ٣٠٠ بطاقة بدن الأرقام السرية بسعر ٥٠ دولارا. وقال: هنالك عدد من المخاطر التي تهدد خصوصية كل مستخدم للإنترنت. هذه المخاطر تتزايد وتتطور أشكالها وآثارها ووسائلها في الوقت الذي تقل فيه إمكانية اكتشاف فاعليها. لذلك فإن خصوصية مستخدم الإنترنت يجب أن تكون محمية باستخدام التقنيات والاحتياطات الأمنية Security Counter Measures.إلا أن دور العامل البشري في حماية الخصوصية لا يقل أهمية عن دور التقنيات والاحتياطات الأمنية المتمثلة في برمجيات وأجهزة أمن المعلومات. بل إن هذا العامل قد يقلل من فعالية تلك البرمجيات والأجهزة إذا ما كان المستخدم مهملا أو صاحب دور سلبي.

عبد الله الجارد

عبدالله الرخيمي

الهاكرز واقتحام للخصوصية الفردية والجماعية

الشبكة العنكبوتية وتهديد المستخدمين