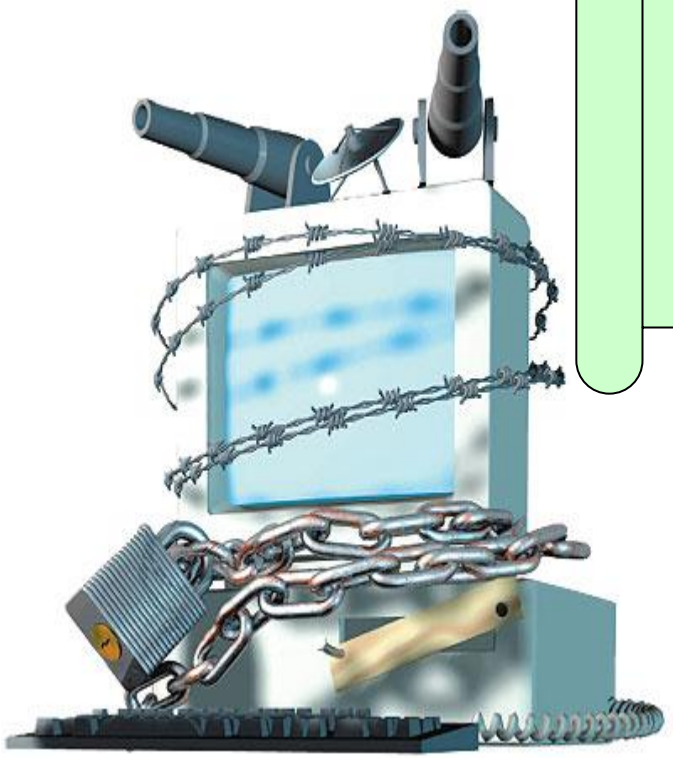
# الحماية الالكترونية(تقنيه المعلومات)

شهدت نهاية هذا العام العديد من الهجمات الالكترونية المتطورة.



# ومن احدثها

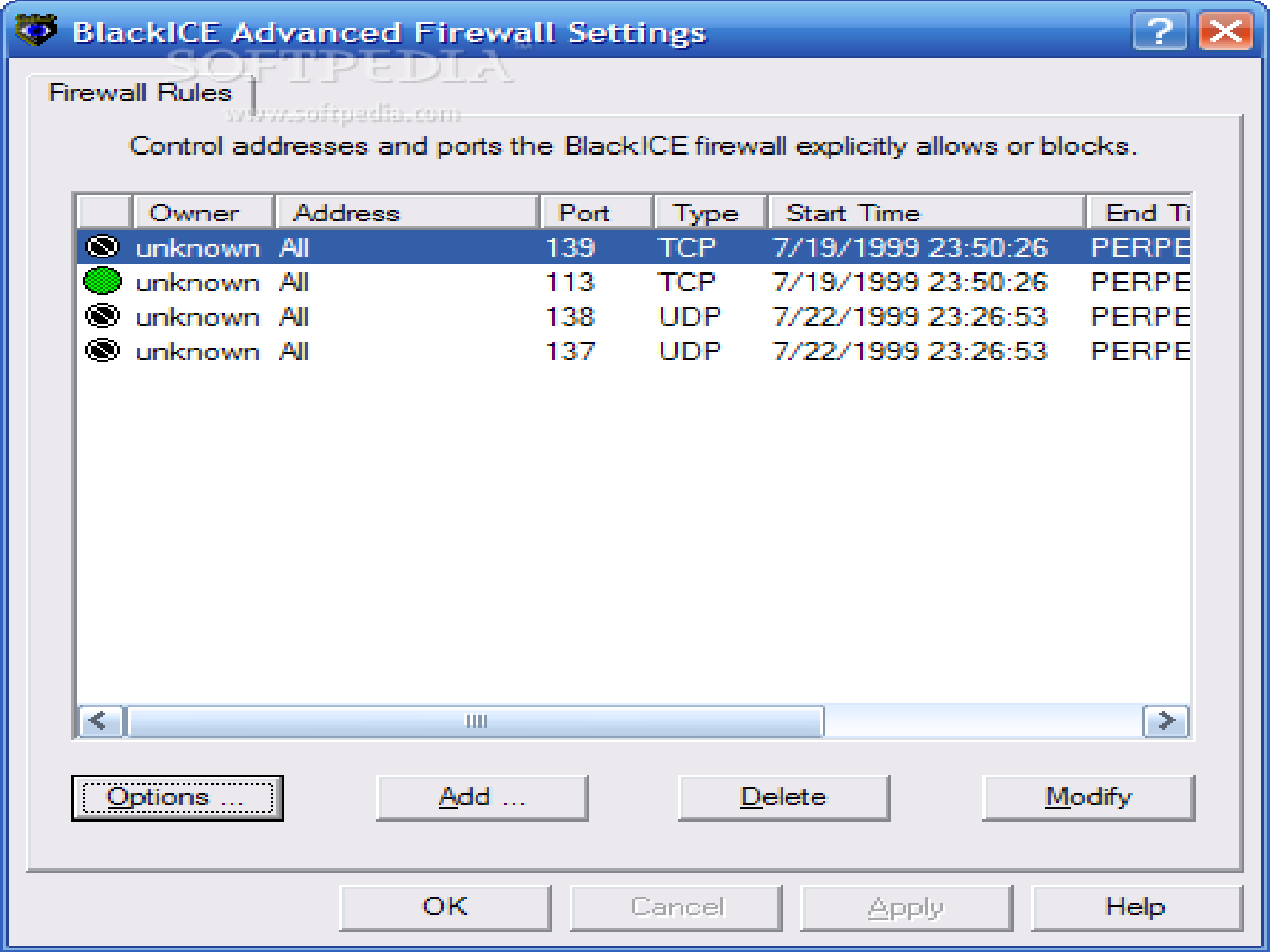
- *التي حصلت على أجهزة وزارة الدفاع الأميركية في نهاية شهر نوفمبر (تشرين الثاني) المنصرم، حيث تعرض المركز الخاص بعمليات العراق وأفغانستان إلى هجمات متخصصة بالشبكات الحربية أثرت فيها بشكل ملحوظ.
- *الذي أصاب كومبيوترات البنتاغون. ومنع البنتاغون جميع المستخدمين في مركزه الأميركي وفي العراق وأفغانستان من استخدام وحدات الذاكرة المحمولة «يو إس بي»، نظرا لسهولة انتقال البرنامج من كومبيوتر إلى آخر عبرها.

- معلومة:ومن المرجح أن تكون التقنيات المستخدمة في هذا النوع من الهجمات على مركز عسكري ذي نظام حماية معقد من الدرجة الأولى متطورة جدا، وأن تموه المجموعة المسؤولة عن الهجمات موقعها الجغرافي في فترات زمنية متتالية، وذلك حتى لا تستطيع الوزارة معرفة مكان عملها الفعلي، خصوصا إن كان أفراد المجموعة يستخدمون كومبيوترات متصلة بالإنترنت عبر هواتف جوالة في داخل آليات نقل متحركة طوال الوقت.

معلومة: هذا واستطاعت مجموعة من الـ«هاكرز» الروس في بداية الشهر الحالي ديسمبر (كانون الأول) اختراق موقع شبكة «سي بي إس» CBS الأميركية وإضافة برنامج يصيب جميع من يتصفح الموقع إن كان لا يستخدم نظم أمن متطورة. ويدل هذا الأمر على أن بوابات الإنترنت ليست آمنة على الإطلاق، مهما كانت درجة تطورها التقني. واستخدم الـ«هاكرز» ثغرات أمنية يطلق عليها اسم «آي فريم» iFrame، وحقنوا لغة قواعد البيانات «إس كيو إل إنجيكشين» SQL Injection التي تضيف أسطر إلى نص الصفحة البرمجي لإجراء عمليات محددة على قواعد بيانات الموقع.

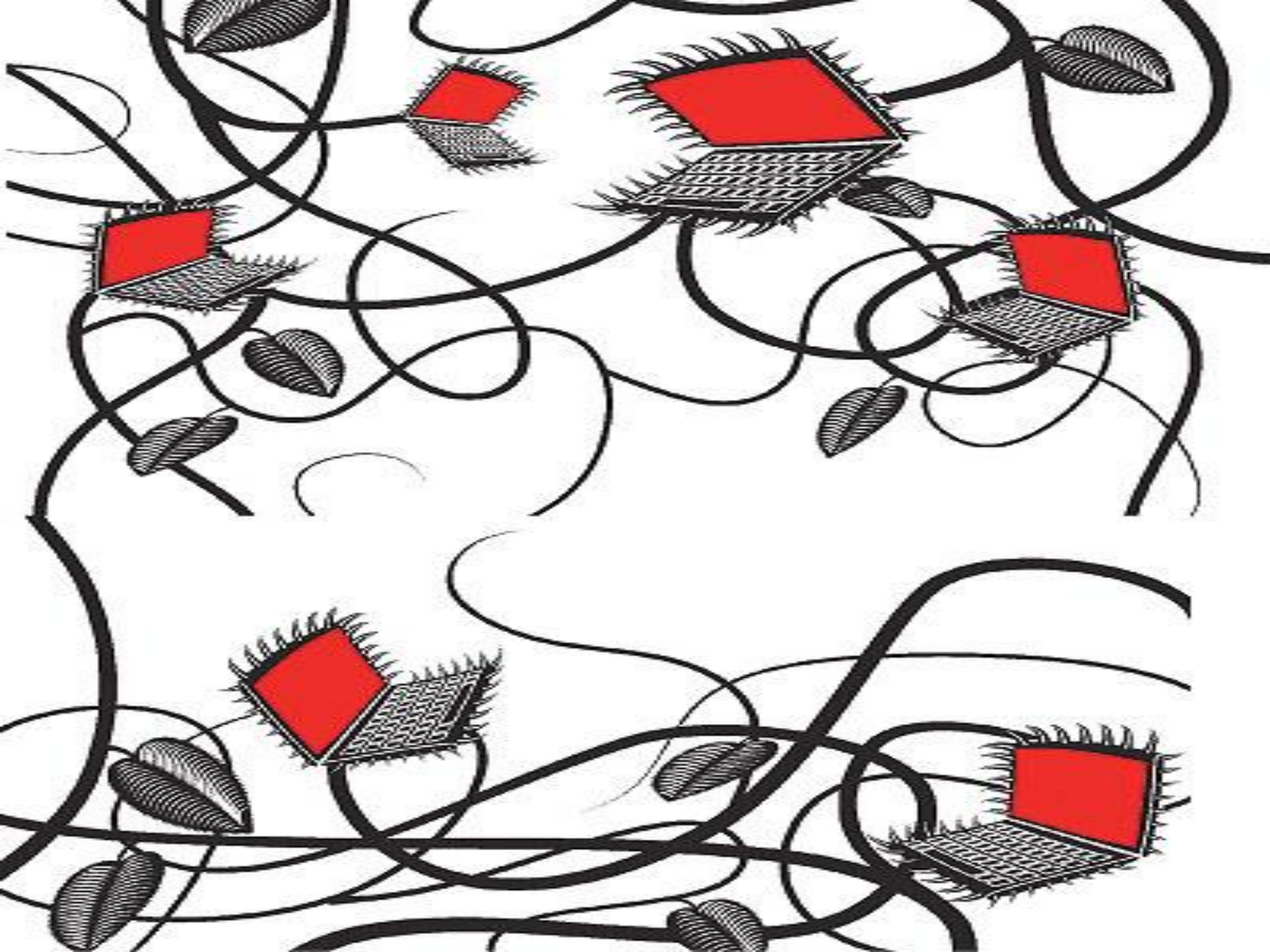
# ظهور المتسللين

- * نما مجتمع الكومبيوترات بشكل كبير في نهاية سبعينات وبداية ثمانينات القرن الماضي، وذلك بسبب ظهور الكومبيوتر الشخصي بعد تصغير التقنيات إلى أحجام يمكن وضعها في منازل المستخدمين. ومع ازدياد عدد مستخدمي الكومبيوترات الشخصية في تلك الفترة، ظهرت شريحة جديدة من المستخدمين اسمها «هاكرز» Hackers، أو المتسللين او مخترقي نظم الأمن (لا يجب خلط هذا المصطلح مع «القراصنة» Pirates الذين ينسخون البرامج والألعاب الإلكترونية بشكل غير قانوني). ويطلق هذا المصطلح على من يريد معرفة داخليات الكومبيوتر عوضا عن استخدامه بشكل عادي، وغالبا ما يكونوا من الأذكياء الذين لديهم شغف بالكومبيوترات والشبكات، وبعض الفضول والمزاح، الذين غالبا ما يسببون المتاعب لخبراء الشبكات والأمن، وحتى لمكتب المباحث الفيدرالية الأميركي «اف بي آي». وترك الكثير من الـ«هاكرز» بصماتهم في تاريخ الكومبيوتر، حتى أن بعضهم أصبح قدوة لجيل جديد يحتذى بهم. ومع تطور التقنيات في تسعينات القرن الماضي وأوائل هذا القرن، فإن طرق التحايل الـ«هاكرز» تواكب تلك التطورات بشكل مطرد .


BlackICE Advanced Firewall Settings
Firewall Rules
Control addresses and ports the BlackICE firewall explicitly allows or blocks.
Owner
Address
Port
Type
Start Time
End Ti
unknown All 139 TCP 7/19/1999 23:50:26 PERPE
unknown All 113 TCP 7/19/1999 23:50:26 PERPE
unknown All 138 UDP 7/22/1999 23:26:53 PERPE
unknown All 137 UDP 7/22/1999 23:26:53 PERPE
Options ...
Add ...
Delete
Modify
OK
Cancel
Apply
Help

# تقنيات تسلل

- *وعلى صعيد آخر، استطاع باحثون في جامعتي كاليفورنيا الأميركية وساربروكين الألمانية، تطوير تقنيات بسيطة يمكن لأي «هاكرز» تطويرها، تتعرف على الكلمات التي يطبعها المستخدم على لوحة المفاتيح في ظروف إضاءة صعبة، أو من مسافات بعيدة، والتنبؤ بالكلمات القريبة من تلك التي تعرف عليها البرنامج. وغالبا ما تكون الكلمات الحقيقية من ضمن الاقتراحات الخمسة الأولى. ويمكن لمن يريد سرقة المعلومات أن يضيف كاميرا صغيرة في سقف مركز معلومات مهم، أو في مقهى للإنترنت، أو حتى أن يدخل إلى كاميرا الكومبيوتر الشخصي، التي غالبا ما تكون مدمجة في الكومبيوترات المحمولة الحديثة، وسرقة ما يريد من أمام أعين المستخدم، ومن دون أن يعرف المستخدم ماذا يجري. ويمكن لهذه التقنية أيضا أن تعرض محتوى الشاشة من انعكاس الصورة من على النظارات والزجاج وإبريق الشاي وزجاجات المشروبات الغازية والملاعق، وحتى من على العين البشرية.



معلومة:تجدر الإشارة إلى ان الباحثين قد استطاعوا عرض محتوى الشاشة من على جدار أبيض اللون يبعد مترين عنها فقط. وأطلق الباحثون اسم «كلير شوت» Clear Shot على هذه التقنية المثيرة للاهتمام والجدل.

# اختراق وسرقة

- *ونجحت مجموعة من «هاكرز» الصين في إصابة أكثر من 10 آلاف جهاز خادم في غرب أوروبا والولايات المتحدة الأميركية، وتعديل نص الصفحات البرمجي بنص «جافا سكريبت» JavaScript خاص يحول المتصفحين إلى جهاز خادم من بين 6، الذي يحولهم بدوره إلى جهاز رئيسي موجود في الصين، ومن ثم تحميل مجموعة من الملفات والبرامج الضارة التي تسرق معلومات المستخدمين. وتجدر الإشارة إلى أن الجهاز الرئيسي يستغل الثغرات الأمنية الموجودة في متصفحات «إنترنت إكسبلورر» و«فايرفوكس» وتقنيات «آدوب فلاش» و«آكتيف إكس»، الأمر الذي يعني بأن جميع من تصفح تلك المواقع ولم يكن قد حدث برامجه هو عرضة لأن يكون مصابا ببرنامج ضار من دون أن يعلم بذلك.


TrustPort Internet Security 2012
Parfaitement protégé
TrustPort protège pleinement votre ordinateur
Aide
A propos
Paramètres généraux »
TRUSTPORT INTERNET SECURITY 2012
TrustPort Internet Security 2012
Analyse à la demande
Analyse: CSM58.tmp
Répertoire: C:\...ts and Settings\Administrateur\Local Settings\Temp\
Cible : Registre; C:\WINDOWS\system32; C:\Documents and Settings...
Sur l'ensemble des 416 fichiers analyés, 0 infections ont été trouvées et 0 d'entre elles ont été correctement résolues.
A propos
Manuel
Pause
Afficher Rapport
Annuler
MISES A JOUR
Configurer »
Dernière mise à jour antivirale: 20/07/2011 à 13:16:41
Version du programme: 2012 (12.0.0.4788)
Mettre à jour maintenant
Vérifier maintenant
Paramétrage Expert
Fermer

معلومة:يذكر أن رجلا كولومبيا يدعى ماريو بونيلا يبلغ من العمر 40 عاما، قد استطاع إضافة برنامج على كومبيوترات مراكز رجال الأعمال.

- تابع:في الفنادق الفاخرة وصالات الإنترنت، يسجل جميع ما يُكتب على لوحات المفاتيح. واستطاع «ماريو» الحصول على معلومات سرية خاصة بالعديد من رجال الأعمال وموظفي وزارة الدفاع الأميركية، ومن ثم استخدام هذه المعلومات لتحويل مبالغ من حسابات الضحايا إلى بطاقات ائتمانية وبطاقات مسبقة الدفع ومال، ومن ثم شراء الإلكترونيات والسفر المرفه إلى هونغ كونغ وفرنسا وجامايكا والولايات المتحدة الأميركية، وغيرها من البلدان. ووصلت قيمة المبالغ المسروقة إلى 1.4 مليون دولار أميركي من حوالي 600 ضحية. وألقي القبض على «ماريو» في الولايات المتحدة الأميركية في هذا العام، وحكم عليه بالسجن لتسعة أعوام ودفع مبلغ 347 ألف دولارا أميركيا، والإشراف على أعماله لثلاثة أعوام بعد إطلاق سراحه

# مكالمات مجانية

- *ويعتبر جون دريبير من أوائل الـ«هاكرز» في التاريخ، حيث استطاع اختراق نظام الهواتف باستخدام صفارة مجانية موجودة في عبوات رقائق الذرة، وذلك بتصفير نغمات معينة في الهواتف العمومية باستخدام الصفارة، والحصول على مكالمات مجانية عند الطلب. وعلم جون أن هذه الصفارات قادرة على إصدار نغمات بتردد 2600 هرتز، الترددات نفسها المستخدمة في الهواتف للدلالة على أن الخط غير مستخدم. وتعمل الطريقة بشكل بسيط ببساطة، حيث يتصل المستخدم برقم دولي، ويطلق صفارة بنغمة معينة بعدما يرن هاتف الجهة الثانية، الأمر الذي يخدع شبكة الاتصالات لتظن بأن المستخدم قد توقف عن الكلام وأن الخط غير مستخدم، وبالتالي عدم طلب المزيد من النقود من المستخدم. وألقي القبض على جون في عام 1972 بعد تحقيق شركة الاتصالات في حساباته وملاحظة نمط اتصال غير منطقي. وبرزت مجموعات جديدة من الـ«هاكرز» أطلقت على نفسها اسم «2600»، تيمنا بالتردد المستخدم، وحاولت العثور على طرق جديدة لإجراء المكالمات المجانية.


ADPHONE
CONTACTS
myADPHONE
?
X
تكلفة الدقيقة بالوحدات
Country Code
كود الدولة 20
Egypt
Phone Number
رقم الهاتف
Landline (12 Units/min.)
DIAL
My Status: Online
Units: 95
SETTINGS
Welcome!, Click 'Start Tutorial' To Learn All About ADPHONE
START TUTORIAL
عدد الوحدات
اضغط هنا للاتصال

معلومة:إلا أن جون كان قد أخبر الكثير من الأصدقاء عن اكتشافه قبل إلقاء القبض عليه، منهم ستيف ووزنياك الشريك المؤسس لشركة «آبل». وأتقن ووزنياك مع صديقه ستيف جوبز طريقة جون، وصنعوا جهازا أسموه «الصندوق الأزرق» Blue Box الذي يستطيع إطلاق نغمات هاتفية بالترددات اللازمة لخداع نظام الاتصالات. وبعد تجربة الجهاز بنجاح، قرر الثنائي المتاجرة بهذه الأجهزة، حيث إن استخدامها سهل جدا وسعرها منخفض، الأمر الذي ساهم بنشرها بسرعة بين العديد من المستخدمين. وتجدر الإشارة إلى أن هذا الصندوق أكثر تطورا من صفارة جون، حيث إنه يستطيع محاكاة جميع النغمات والترددات المستخدمة في نظم الاتصالات في ذلك الوقت. ومن القصص المشهورة المتعلقة بهذا الصندوق مكالمة ووزنياك للفاتيكان مدعيا أنه هنري كيسنجر وزير الخارجية الأميركي الأسبق!.

تابع:ومن الأفراد المعروفين في عالم الـ«هاكرز»، كيفين ميتنيك الذي نقش اسمه في التاريخ التقني في عام 1981 عندما كان عمره 17 عاما فقط، حيث استطاع الوصول إلى بدالة هاتف شركة الاتصالات «باسيفيك بيل» وتحويل المكالمات كيفما أراد. وتحول هذا المزاح إلى شكاوى المستخدمين الذين حصلوا على مكالمات لا يريدونها. وبالطبع، فإن الطرف المتلقي للشكاوى كان كيفين نفسه، حيث عالج الموضوع بالمزيد من المزاح والإزعاج. وتطورت الأمور بعد ذلك، حيث وصل كيفين إلى قاعدة بيانات الشركة وسرق معلومات الكثير من المشتركين، مثل فواتيرهم وكلمات السر الخاصة بهم، وحتى كتيب إرشادات نظام الشركة، وباتت جميع مكالمات كيفين مجانية. ولاحظ أحد خبراء الشركة نمطا غريبا في النظام، وراقبه واستطاع معرفة الهاتف العمومي الذي كان كيفين يستخدمه، وانتظره مع الشركة ليلقى القبض عليه بالجرم المشهود، وحكم عليه بالسجن لـ3 أشهر، وسنة من المراقبة. ومن المشاهير في هذا المجال أيضا كيفين بولسين الذي استطاع الوصول إلى بدالات الهواتف.

# هجمات على مراكز معروفة

- *واستطاع كيفين ميتنيك أيضا الوصول إلى كومبيوترات وزارة الدفاع الأميركية في عام 1983 عندما كان طالبا جامعيا، حيث استخدم أجهزة الجامعة التي كانت تعمل بمعالج تبلغ سرعته 1.77 ميغاهيرتز للوصول إلى جهاز «آربانيت» ARPANet التي ما هي سوى الإنترنت في أولى أشكالها، والتي كانت محجوزة للجيش والشركات الضخمة والجامعات. وتجدر الإشارة إلى أن تحقيقات وزارة الدفاع الأميركية لم تظهر أي أعمال تخريبية أو سرقات، بل كانت مجرد فضول وفحوص لقدراته التقنية. وعثر مراقب النظام على كيفين، وألقي القبض عليه فورا في حرم الجامعة، وحكم عليه بالسجن لـ6 أشهر بتهمة الدخول غير القانوني إلى شبكة كومبيوتر.

- ولعل حلم جميع الـ«هاكرز» بعد الدخول إلى شبكات الجيش والبنتاغون، هو الدخول إلى أجهزة وكالة الفضاء الأميركية «ناسا» المعروفة باستخدام تقنيات أمن متطورة. واستطاع جوناثان جيمس عمل ذلك في عام 1999 عندما كان عمره 16 عاما فقط، حيث استطاع كسر كلمة السر لجهاز خادم تابع للوكالة، ومن ثم التجول بحرية في الشبكة وسرقة العديد من الملفات، من ضمنها النص البرمجي لبرنامج محطة الفضاء الدولية، التي يقدر ثمنه بحوالي 1.7 مليون دولار أميركي. وأصيبت «ناسا» بالذعر، واضطرت إلى إيقاف أجهزتها عن العمل وإعادة تشغيلها، الأمر الذي كلفها حوالي 41 ألف دولار أميركي. وألقي القبض على جوناثان بسرعة، إلا أن عمره الصغير شفع له في المحكمة.

# انواع الهكرز

- *ومن أنواع الـ«هاكرز» الأخرى مجموعة لا تريد الدخول إلى الشبكات الإلكترونية، بل دراسة كيفية عمل الكومبيوترات والأجهزة الإلكترونية والبرامج من الداخل، وكسر نظم الحماية التي تضعها الشركات، وذلك للسماح للجميع بالاستمتاع بالبرامج والأجهزة من دون قيود. ومن مشاهير هذا العالم جون جوهانسن الذي استطاع معرفة كيفية تجاوز نظم الحماية الموجودة على أقراص «سي دي» و«دي في دي» الليزرية، وملفات الموسيقى الرقمية المحمية التي يمكن الاستماع إليها لعدد محدد من المرات أو على مشغلات موسيقى معينة، مثل ملفات الموسيقى التي تشترى من متجر «آي تونز» iTunes الخاص بشركة «آبل». وأطلق جون على برنامجه الذي يستخلص الموسيقى من دون الحماية اسم «كيو تي فير يوس» QTFairUse. واستطاع جون أيضا تجاوز نظم الحماية الموجودة في هاتف «آي فون»، وهو أول فرد استطاع استخدام الهاتف من دون الاشتراك مع شركات الاتصالات المتعاقدة مع شركة «آبل».

عمل الطالبه:الريم ظافر الاحبابي.

الصف:التاسع.

الماده:حاسوب.

الموضوع:مشروع-الحماية الالكترونية-