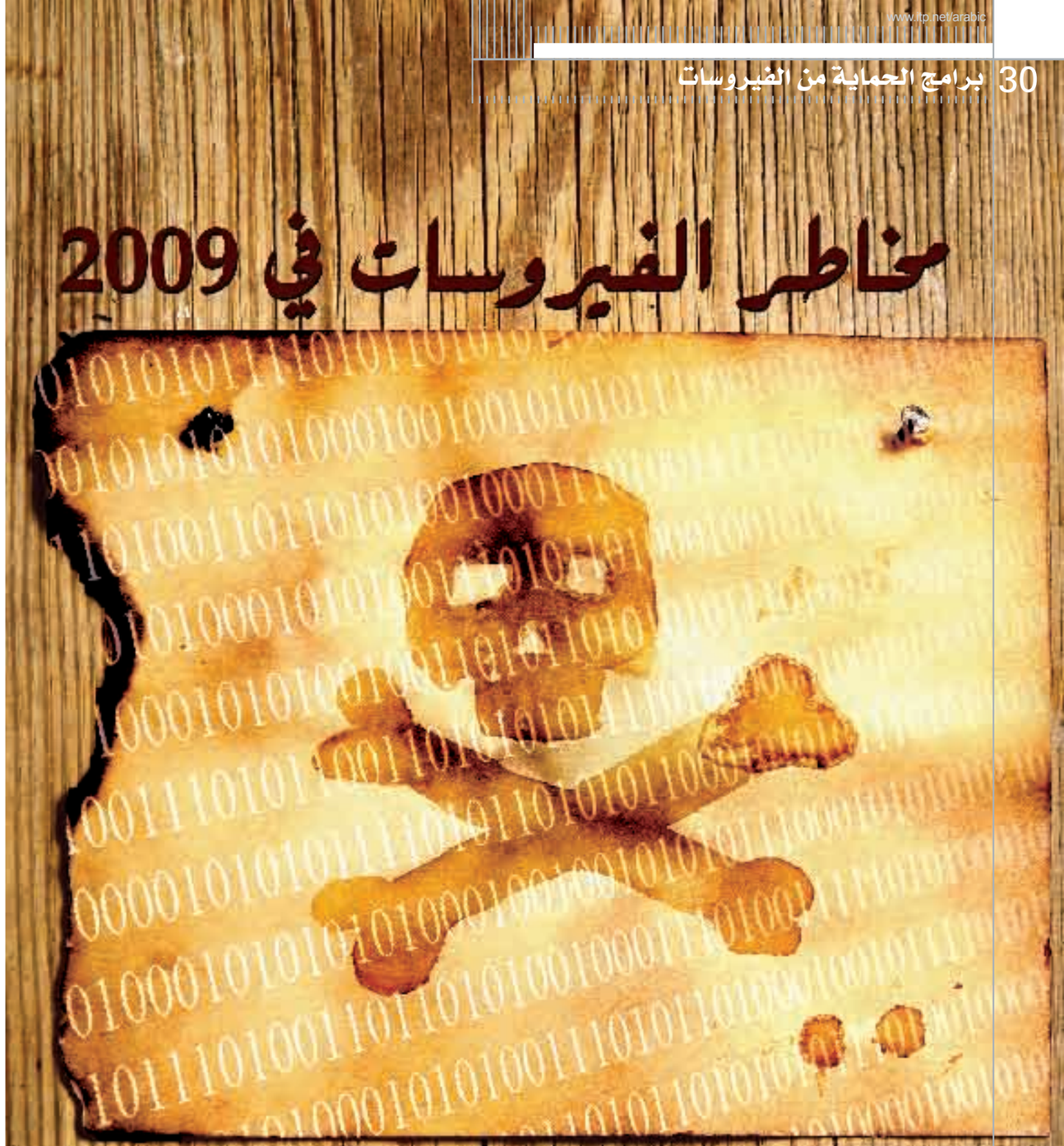
مخاطر الفيروسات في 2009



أصبحت الفيروسات الجديدة أكثر ذكاء وخطرا، وذلك لاستغلالها عدة قدرات تجمع بين أنواع الفيروسات التقليدية، حيث يجمع فيروس الكمبيوتر الجديد ما بين خطر التجسس على ملفاتك الشخصية واستنساخ ذاته، فضلا عن التخفي عن برامج الحماية اعتمادا على تقنيات مختلفة.

تختلف برامج الحماية من الفيروسات عن التطبيقات الأخرى بأنها تتعامل مع معطيات متغيرة، ووفقا لبعض الدراسات فإن كل ثانية نمر بها تشهد ولادة فيروسات جديدة وانتشارها عبر الإنترنت.
ورغم التركيز في كثير من الأحيان على ذكر الفيروسات، فهناك برامج خبيثة عدة يمكن أن تتسبب بأضرار للكمبيوتر أو البيانات المخزنة عليه، فهل لديك المعلومات الكافية عن هذه الأنواع؟

1 الفيروسات Viruses:

هي الشكل الأكثر شيوعا من البرامج الخبيثة، وتنتقل هذه الفيروسات إلى الكمبيوتر نتيجة خطأ من قبل المستخدم، مثل استقبال بريد إلكتروني ملوث بالفيروسات من طرف مجهول، أو زيارة بعض مواقع الإنترنت التي قد يؤدي النقر على أحد الأوامر فيها إلى انتقال الفيروس إلى الكمبيوتر.

إذا، فالفيروسات لا تنتقل تلقائيا إلى الكمبيوتر، وإنما بفعل المستخدم، وإن كان ذلك يتم بصورة غير مباشرة، إذ يمكن مثلا أن ينتقل الفيروس إلى الكمبيوتر بمجرد نسخ ملف عادي من قرص مضغوط CD إلى الكمبيوتر دون علم المستخدم.

وتنقسم الفيروسات إلى عدة أصناف، أبرزها:

- فيروسات الإقلاع Boot Viruses: تعمل هذه الفيروسات تلقائيا عند بدء تشغيل الكمبيوتر، وتكون عادة ملتصقة بما يسمى سجل الإقلاع الرئيسي MBR. إذ أنها تمسح المحتويات الأصلية للسجل لتضيف مكانها محتويات جديدة.
- فيروسات البرامج Program Viruses: تؤثر هذه الفيروسات على الملفات التنفيذية ذات الامتداد exe أو com أو ملفات النظام ذات الامتداد bin أو sys، وذلك بالالتصاق بها، وبالتالي تعمل هذه الفيروسات بمجرد تشغيل تلك الملفات ليتم تحمي الفيروس إلى الذاكرة.
- الفيروسات الخفية Stealth Viruses: تعتمد هذه الفيروسات على تقنيات عدة لتجنب اكتشافها من قبل برامج الحماية من الفيروسات، مثل توجيه رؤوس القراءة في القرص الصلب إلى منطقة أخرى لقراءتها بدلا من قراءة القطاع الذي يحتوي على الفيروس من القرص الصلب، مما يمنع برامج الحماية من التعرف عليها بسهولة.

2 الديدان Worms:

تختلف الديدان عن الفيروسات بأنها ليست بحاجة إلى تدخل من المستخدم لانتشارها، أي أنها تنتقل تلقائيا إلى الكمبيوتر بمجرد اتصاله بالإنترنت أو الشبكة المحلية التي تحتوي على الدودة، أو عند وضع القرص المدمج DVD الذي يحتوي على الدودة في السواقة الخاصة به.

يعتبر التعرف على الديدان أمرا أكثر صعوبة من التعرف على الفيروسات بالنسبة لبرامج الحماية، وذلك لأنها تعمل ذاتيا دون تشغيل برامج أخرى.

3 ملفات تروجان Trojan:

تعود تسمية هذه الملفات إلى الحادثة الشهيرة لاقتحام القلعة في جزيرة طروادة المحاصرة، وفيها تسلل الجنود إلى القلعة مختبئين ضمن تمثال كبير على هيئة حصان.

ومثلا قد تقوم بتحميل إحدى الملفات من الإنترنت على أنه لعبة كمبيوتر، لتفاجأ بعد تشغيل اللعبة المفترضة بأنها برنامج خبيث من نوع تروجان هدفه حذف أو تعديل بعض البيانات الموجودة على كمبيوترك.

إذا فالمستخدم يقوم بتحميل ملف تروجان إلى الكمبيوتر وتشغيله عمدا، لكن دون معرفة محتواه الحقيقي.

4 ملفات وبرامج التجسس Spyware:

تصل هذه البرامج إلى كمبيوتر المستخدم دون علمه، لتتنصت على استخداماته للكمبيوتر، إذ تقوم مثلا بمراقبة كلمات المرور التي يكتبها في حسابات البريد الإلكتروني، أو تلك الخاصة بالحسابات والمعاملات البنكية التي تتم عبر الإنترنت.

لا تعمل برامج التجسس بصورة مستقلة، بل تكون بمثابة برنامج الزبون Client الذي يتصل بالبرنامج الأساسي Server الموجود لدى مطوري برنامج التجسس، وذلك لتسريب بيانات المستخدم إليه.

آلية اختيار برامج الحماية:

يتقاطع في قرار اختيار برنامج الحماية المناسب محوران، الأول هو المزايا التقنية والتي يمكن مقارنتها بين برامج الحماية من خلال الاطلاع على التفاصيل الكاملة لبرنامج الحماية والاتصال بالشركة المطورة للحصول على مزيد من التفاصيل، وقد اضطلعنا بهذه المهمة لنعرض نتائجها للمستخدمين.
أما المحور الثاني فهو الاختبارات العملية التي تتم من خلال نسخ بعض الفيروسات عمدا إلى الكمبيوتر، والتحقق من قدرة برامج الحماية على اكتشاف هذه الفيروسات وإزالتها.
ونظرا لصعوبة تنفيذ هذه المهمة فقد أثرنا الإشارة إلى اثنين من المواقع المتخصصة في إجراء هذا النوع من الاختبارات، وعنوانهما www.av-test.org و www.vi-rusbtn.com، وفيهما تجد تقييم برامج الحماية من الفيروسات في اختبارات شتى، كالتصدي للفيروسات والتخلص من ملفات تروجان، ويشرف على هذين الموقعين مجموعة من الخبراء المحايدين.

المزايا التقنية في الاختيار:

فحص محتويات البريد الإلكتروني:

لا غنى عن ميزة فحص رسائل البريد الإلكتروني والملفات المرفقة معها، لاسيما إن كانت التعامل مع رسائل البريد الإلكتروني يتم بصورة متكررة كما هو الحال في المكاتب أو الشركات.
ولا تقتصر أهمية هذه الميزة في فحص الرسائل مجهولة المصدر، وإنما قد تصلك رسائل بريد إلكتروني غير سليمة من عناوين أصدقائك التي يمكن أن تتعرض للاختراق من قبل طرف آخر.
وجود هذه الميزة سيضمن سلامة رسائل البريد الإلكتروني التي تصلك أو التي ترسلها إلى أطراف أخرى، وسيكون بمقدورك آنذاك التعرف على الجهات التي قد تتعمد إرسال محتويات ضارة إليك بصورة متكررة وإضافتهم إلى القائمة الممنوعة من إرسال البريد إليك.

الجدار الناري:

قد يكون برنامج الجدار الناري Firewall جزءا من برنامج الحماية من الفيروسات أو من طقم الحماية الذي توفره الشركة، وبكل الأحوال، فلا بد أن يكون هذا الجدار مجهزا لمراقبة البيانات الواردة من الإنترنت إلى الكمبيوتر و الصادرة من الكمبيوتر إلى الإنترنت، وتحذيرك من البرامج أو الأدوات التي تحاول الاتصال بالإنترنت لإرسال أو استقبال البيانات دون علمك.
يفيد الجدار الناري بصورة أساسية عند وجود اتصال عالي السرعة بالإنترنت ومتوفر على مدار الساعة، فعندها قد لا ينتبه المستخدم إلى ضياع جزء من عرض حزمة الاتصال بالإنترنت نتيجة استخدامه خفية من قبل برامج وأدوات مختلفة.

معدل تحديث قاعدة البيانات:

تعتمد برامج الحماية من الفيروسات في عملها بشكل كبير على قاعدة البيانات التي تحتوي على تعريف الفيروسات، فكلما كانت هذه البيانات أكبر كلما كانت برامج الحماية أكثر فاعلية.
لا نستطيع بالتأكيد تحديد حجم البيانات التي يوردها كل برنامج للحماية، إلا أن ما يهمنا هو معدل تحديث قاعدة البيانات الخاصة ببرامج الحماية.
في برنامج BitDefender يتم تحديث قاعدة بيانات تعريف الفيروسات كل ساعة.
وفي برنامج ESET NOD 32 يتم تحديث قاعدة البيانات مرتين أو ثلاث مرات يوميا.
أما كاسبرسكي فتشير إلى أن تحديث قاعدة البيانات يتم بمعدل 50 مرة في اليوم.
بالنسبة لشركة تريند مايكرو فإنها تعتمد على مبدأ مختلف، وذلك من خلال الاحتفاظ بقاعدة البيانات التي تحتوي على تعريف الفيروسات على الإنترنت، وبالتالي تتم مقارنة الملفات المشبوهة مع هذه القاعدة التي يتم تجديدها بصورة متكررة، إلا أن ذلك يعني ورطة للمستخدمين الذين لا يتصلون بالإنترنت بصورة مستمرة.
أما سيمانتيك فيشير المتحدث باسمها إلى أن الشركة لا تطرح التحديثات الجديدة بعد التعرف على الفيروسات مباشرة، وذلك لأنها تقوم بتصميم التحديث المناسب للتعرف على الفيروسات الجديدة بعناية وفق المتحدث باسم الشركة.

التحديث التلقائي لقاعدة البيانات:

لا مشكلة في التحديث اليدوي لقاعدة بيانات برامج الحماية، لكن الانتشار السريع للفيروسات يجعل مسألة التحديث التلقائي لقاعدة البيانات أكثر فاعلية هذه الأيام، لأن المستخدم قد يغفل عن هذه المسألة، مما يجعل وجودها في برامج الحماية أمرا أساسيا.
يوفر برنامج BitDefender ميزة التحديث التلقائي لقاعدة البيانات، وكذلك الأمر بالنسبة لبرنامج NOD32 من ESET.
كذلك الأمر في برامج كاسبرسكي للحماية، وتشير الشركة إلى نقطة هامة هنا، فعند تحديث البرنامج تتم مقارنة قاعدة البيانات الموجودة على الكمبيوتر مع تلك الموجودة على خادم الشركة، وفي حال وجود ملفات جديدة على خادم الشركة يتم فقط نسخ الأجزاء الجديدة منها إلى الكمبيوتر وليس كامل هذه الملفات، وذلك للتقليل من عرض حزمة الاتصال بالإنترنت اللازمة لتحديث البرنامج.
أما ميزة التحديث التلقائي في برامج سيمانتيك، لاسيما نورتون أنتي فايروس 2009 فإنها تتعرف على الأجزاء الجديدة فقط في قاعدة بيانات تعريف الفيروسات لتضيفها إلى التعريفات الموجودة على الكمبيوتر الشخصي.

سرعة المسح وإقلاع الكمبيوتر:

تؤثر برامج الحماية من الفيروسات على أداء الكمبيوتر بصورة متفاوتة، فمنها ما يستهلك الكثير من موارده لدرجة تصعب معها التعامل مع بعض التطبيقات الأخرى، كما أن بعض البرامج التي تقوم بالمسح عند بدء تشغيل الكمبيوتر تطيل الفترة اللازمة لإقلاع الكمبيوتر بصورة غير مقبولة.

سهولة الاستخدام:

لا تتطلب معظم برامج الحماية بإصداراتها الحديثة الكثير من التعديلات على إعداداتها الافتراضية، وإنما يمكن غالبا البدء باستخدامها مباشرة مع المحافظة على الإعدادات الافتراضية لها.

ومع ذلك فقد تحتاج في بعض الأحيان، للوصول إلى بعض الإعدادات في البرنامج، وهنا سيكون من الأسهل التعامل مع برنامج ذو واجهة بسيطة تكون الأوامر فيها مرتبة بصورة منطقية، كما قد تكون البرامج التي تتمتع بواجهة استخدام عربية مثل كاسبرسكي أنتي فايروس Kaspersky Antivirus 2009 أكثر جاذبية للمستخدمين الذين لا يتقنون الإنكليزية بصورة كبيرة مما هو عليه الحال مع البرامج التي لا تدعم العربية.

مزايا إضافية:

تشير بعض شركات الحماية إلى عوامل أخرى تلعب دورا هاما في اختيار برنامج الحماية المناسب.

تشير شركة بت ديفندر BitDefender على سبيل المثال إلى مسألة بساطة الاستخدام المتمثلة في عدم إزعاج المستخدم بعرض الكثير من الرسائل والتنبيهات على الشاشة كل فترة وأخرى، والاكتفاء بسؤاله للأمور الأساسية، فتخيل مثلا أنك تشترك في لعبة ما عبر الإنترنت لتظهر رسائل تحذيرية كل فترة تشير إلى وجود تحديث جديد أو ما شابه ذلك!

تشير بت ديفندر أيضا إلى مسألة توافق برنامج الحماية من الفيروسات مع تطبيقات حماية مقدمة من شركات أخرى، إذ لا ينبغي أن يكون هناك تضارب بين برنامج الحماية من الفيروسات المقدمة من شركة X مع برنامج الجدار الناري المقدم من شركة Y.

وعموما ننصح باختيار تطبيقات الحماية من شركة واحدة تجنبا لهذا النوع من التضارب.

أخيرا تشير الشركة إلى مسألة إلغاء تثبيت برنامج الحماية، والتي لا بد أن تكون سهلة ومبسطة، لأن المستخدم هو صاحب القرار الوحيد في الإبقاء على أحد برامج الحماية أو استبداله في حال كان أداؤه ضعيفا.

ومن تجربتنا الطويلة مع برامج الحماية، فإن برامج سيمانتيك هي الأكثر استعصاء في الكمبيوتر والأصعب في الحذف، وقلما نجحنا بإزالة أحد برامج سيمانتيك من الكمبيوتر دون الحاجة إلى الاستعانة بأدوات مساعدة مثل أداة حذف برامج سيمانتيك Norton Removal Tool.

خضعت برامج الحماية من الفيروسات لاختبارات عملية، والجدول التالي يوضح نتائج هذه الاختبارات، إذ يشير التقييم في كل حقل إلى النسبة من عشرة لنجاح البرنامج في المهام التي تم اختباره فيها.

	BitDefender Antivirus 2009	Kaspersky Anti-Virus 2009	Norton AntiVirus 2009	McAfee VirusScan Plus 2009	Trend Micro AntiVirus plus AntiSpyware 2008
التعرف على الفيروسات	9	8	4	5	4
التعرف على الديدان	8	6	6	4	3
التعرف على ملفات تروجان	8	6	5	4	3
التعرف على ملفات التجسس	8	6	4	5	3
فحص محتويات البريد الإلكتروني	9	6	5	4	3
تحديث قاعدة البيانات	9	8	4	4	3
استهلاك موارد الكمبيوتر	9	7	3	2	4