من المحرر

لايوجد شيء دون مقابل!

● هناك قاعدة ذهبية عامة وليست في مجال الإنترنت فحسب تقول(لايوجد شيء دون مقابل)! وهذه العبارة أو الحكمة يمكن أن نوظفها اليكترونيا فهي ذات صلاحية واسعة في مجالنا نحن فالكرم الحاتمي بلغ أشده في شبكة الإنترنت.. لدرجة لم نعد نصدق أي البرامج الأكثر مصداقية هل هذا أم ذاك.. هل المعطى من هذه الشركة أم من تلك.. هل من هذا الموقع الذي يقوم بالترويج له أم من ذاك الموقع.. هل هذا البرنامج (الفري خالص) هو فعلا فري خالص مالص أم لا.. هل المنتج لهذا البرنامج هو بهذه الدرجة من الغباء أن (يستهبل) بالملكية الفكرية وحقوق الإنتاج فيوقفه لذوي الاحتياجات الخاصة بدون مقابل يذكر.. هل من الشبع والترف والتخمة أن وصل الحال بهؤلاء إلى وضع منتجاتهم من البرامج المختلفة في شكل منحة وهبة مجانية بدون مقابل يذكر.. ؟

هذه الأسئلة وغيرها لابد وان تخطر في بالنا في كل وقت وحين وبالتحديد عندما تقابلنا برامج ، في ذات الأهمية بمكان بالنسبة لنا معروضة للتملك مجانا بل لا يخلو مجموع ما يصلك من البريد الإليكتروني يوميا من البرامج والدعوات الساخنة من رسائل ، للتو حررت تبدي رغبتها لك واستعدادها ببرامج مجانية ذوات خاصية غير مسبوقة لك وحدك .. فقط مطلوب منك أن تمنحنا بعضا من الوقت الثمين لا تتعدى دقائق وربما لا يتوقف هذا الاتصال (الوثيق) في تلك المدة المحددة المرتبطة بوقت تنزيل البرنامج (العطية) لأن البعض قد يستمر معك (في السراء والضراء) حتى بعد ولو بعد أن شربت المقلب.

● قد يتساءل الكثير منا إذا كان والحال كذلك فما الحل؟

النصيحة بعد هذا كله هو أن تتعلم، وأن يكون لديك العلم بهذه الشقوق.. ثم بعد ذلك سوف تتعلم الكثير من خلال المران والممارسة وتجربة الخطأ والصواب... يكفي مثلا أن المستخدم اللبيب يتعلم الحذر ! ثم يتعلم لماذا يقرأ الاتفاقيات اللوائح التي تصبح وثيقة تفاهم بين المستخدم والمنتج.. يكفي أن تعلم أن المستخدم أيا كان في المشرق أو المغرب هو حقل تجارب لهذه المنتجات ثم بعد ذلك له الخيار في الاستمرار مع / أو المقاطعة.! يكفي أن تعلم عزيزي المستخدم أن معظم المعاهدات والاتفاقيات واللوائح والتعليمات نشرات المساعدة المدمجة مع أي برنامج فيها من التحذيرات ما يكفي من البيان بعدم المسئولية وعدم تحمل أي أضرار ناجمة أو ناتجة بشكل مباشر أو غير مباشر عن استخدامك هذه البرامج وبالتالي فكل مستخدم هو مسئول كليا عن أي حادث يتعرض له بسبب ذلك.

● إذا كنا نعلم أن برامج تنتجها شركات عملاقة مثل مايكروسوفت وغيرها تتخلى هي عن مسئوليتها في استخدامك لمنتجاتها فما بالك بعيوب برامج مجانية لمواقع شخصية غير معروف أصحابها، وبرامج لشركات غير مسجلة، وبرامج بدون هوية!! إذا ماهو العمل المطلوب من المستخدم أن يتخذه أسلوبا في التعامل مع الشبكة؟

● حب التجريب متاح لكن بحذر، معرفتك بالطريق والتمهيد لخط الرجعة مطلوب إذا وقعت في فخ وكنت ضحية هاكرز مثلا، لا تثق في كل الأشياء المعروضة ، وكل من هذه الأشياء ينبغي أن تضعها تحت مجهرك الشخصي، لا تثق دائما بالمواقع (إلا ماندر) التي تستسمحك بعمل فحص مجاني لجهازك، والبعض الآخر الذي ينبهك إلى وجود عيوب ومنافذ أمنية مفتوحة في جهازك ولذلك نحن (البعض) ننصحك بإجراء الكشف الطبي بأسرع وقت ممكن قبل فوات الأوان!

لاتصدق ذلك؟!

لاشك أننا في آخر المطاف ربما لن نصدق أحدا وسوف نشكك في كل شيء.. هذا غير صحيح.. والمعنى النقي الذي نهدف من ورائه هو أن تكون لدينا الفراسة الكافية والسلاح.. والحاذق من بيتهم لا يحتاج إلى تذكير، لكن حتى لا يأخذ البعض هذا الموضوع بمحمل أكثر من اللازم (حساسية زائدة) فيقاطع كل البضائع التي تعرضها الشبكة فلا يعقل مع هكذا أن نتصرف.. وحتى لاتكون لينا فتعصر ولا يابسا فتكسر فالحذر والحيطة والمرونة مطلوبة ، وسلطان العلم مطلوب في كل الأحوال.

● وأخيرا أعتقد انه من الظلم التشكيك في كل المواقع فبعضها على درجة كبيرة من المصداقية وشهرتها وسمعتها تحتم عليها أن تكون في مستوى المسئولية ، وقليل جدا من هذه المواقع محترمة ، وإنما هي تمنح مجانية برامجها بهدف التعريف بمنتجاتها ، ثم أيضا ترويجها وبيعها بشكل أكثر ضمانة وربحية للشركات والمؤسسات الكبيرة .. ومع ذلك علينا بقراءة الاتفاقية وسياسة حماية الخصوصية لذلك الموقع جيدا قبل الإقدام على تحميل البرامج.. وسلامتكم.!

عبدالرحمن الكبسي
alkepsi@althawra.gov.ye

أوفيس إكس بي Office Xp يوفر لك درجة عالية من الحماية والأمان

● يتضمن إصدار المطورين من أوفيس إكس بي مكونات جديدة مثل نقطة المشاركة Share point التي تعد الحل المثالي للحوسبة التعاونية المعتمدة على الويب، وهناك أيضا فرونت بيج FrontPage الذي سيتوفر أخيراً بدعم مميز للغة العربية وكذلك هو الحال مع ببلشر ١٠ الذي سيتضمن بدوره دعما جيدا للعربية وقد تم طرحه في نفس موعد طرح أوفيس إكس بي، كما يأتي أوفيس إكس بي مزوداً بمجموعة جديدة متميزة من الخيارات والأدوات الفريدة مثل العلامات الذكية، فضلاً عن إمكانات البحث العالية عن الملفات وخاصية استعادة العمل في حال حدوث خطأ أو انهيار في النظام والكثير من الميزات الأخرى الهامة، أما المزايا التي نتمنى أن تتوفر في المستقبل القريب للمستخدم العربي، فهي ميزة التعرف على الكلام والعمل بالأوامر الصوتية وميزة التعرف على خط اليد.

تعتبر العلامات الذكية smart tags واحدة من أهم مزايا أوفيس إكس بي الجديدة، وهي خلية مربع تظهر في الوثائق إذا قمت مثلا بالتمرير بمؤشر الماوس على اسم ما حيث تستحضر لك إذا أردت عنوان البريد الإلكتروني لشخص ما، وغير ذلك من المزايا التي تطلبها أنت وتقوم بتخصيص تلك العلامات الذكية لإدراجها لك دوما. ويمكنك مثلا أن تقوم بترتيب موعد على التقويم لديك مع نفس الشخص الذي ظهر اسمه في الوثيقة وغير ذلك من الإمكانيات الواسعة.كما تتيح هذه العلامات الذكية خيارات واسعة مثل ترقيم أسطر الوثيقة وتنسيقها بالطريقة التي تريدها كاعتماد قالب معين لشركتك وشعارها أو جلب قوالب من موقع مايكروسوفت.

● وتضم العلامات الذكية هذه مزايا اخرى مثل ارتباطها مع قاعدة البيانات ضمن الشبكة المحلية للشركة لتقديم المعلومات لمستخدم مستجد او تقديم مستجدات في المعلومات التي كانت موجودة قبل ذهابك في إجازة مثلا. وبالطبع تتوفر هذه العلامات الذكية في كل تطبيقات أوفيس إكس بي ويكون لها مهام متنوعة حسب كل تطبيق. توفر هذه الأداة مرونة في العمل إذ تعتمد على السياق وعلى المضمون لتؤمن وسيلة سهلة للوصول إلى المعلومات المطلوبة، وذلك عن طريق التنبيه إلى الإجراءات الهامة لخيارات إعداد المعلومات الملصقة وكيفية تصحيح اخطاء المعادلات وما إلى ذلك.

وهناك أيضاً واجهة المهام task bin التي تتيح خيارات مثل عرض محتويات الحافظة وتتسع لـ٢٥ من عمليات النسخ، وضمن خيار لصق يتاح لك حفظ تنسيق المادة الأصلية التي نسختها أو مسايرة تنسيق الوثيقة الحالية، فمثلا إذا قمت بالنسخ من وورد وأردت المحافظة على نفس تنسيق المادة كما كانت في وورد يمكنك لصقها كذلك ضمن وثيقة إكسل أو باور بوينت power point.

● يحمل أوتلوك في إوفيس إكس بي مزايا جديدة أهمها جمعه لبريدك من الإنترنت مثل حسابك مع هت ميل، وكانت هذه الميزة متوفرة فقط في أوتلوك إكسبرس فيما سبق، وذلك لتتبع مراسلاتك ضمن أوتلوك من كل حساباتك البريدية حيث يتم تنزيل كل الرسائل والرد عليها من نفس التطبيق. كما يمكنك البحث في كامل محتوى أوتلوك وحتى ضمن المرفقات، وهناك أيضاً إمكانية التكملة التلقائية لعناوين البريد الإلكتروني، فمثلا بمجرد طباعة ثلاثة حروف من عنوان شخص في حقل العناوين في أوتلوك يقوم البرنامج بعرض خيار العنوان لتكملته تلقائيا.

كما ويمكنك التعامل مع جميع رسائلك البريدية في مكان واحد حيث يتيح لك هذا البرنامج إرسال وتسلم رسائل البريد الإلكتروني من عدة حسابات بريدية مختلفة في الوقت ذاته بما في ذلك حسابات هوت ميل Hotmail فضلاً عن إمكانية إرسال وتسلم رسائل فورية عبر إم إس إن ميسينجر MSN Messenger وكل ذلك عبر نافذة واحدة. ومن جهة أخرى يضع أوتلوك حلاً لمشكلة التضارب في المواعيد إذ تستطيع بسهولة مراجعة جميع مواعيدك وتنسيقها عن طريق نافذة تذكير واحدة جامعة.

● لطالما طالب واستفسر المستخدمين حول أداة بحث تعمل بالبحث عن محتوى الوثائق ولا تقتصر على أسماء الملفات، ولنقل مثلا انك نسيت اسم ملف دونت فيه معلومات عن سعر سلعة ما، يكفي هنا أن تورد في حقل البحث عبارة من النص داخل الوثيقة ليقوم محرك البحث هذا باستحضار الوثيقة التي تبحث عنها. ويمكنك ايضا أن تضيق نطاق البحث ليضم التطبيقات التي يحتمل أن تكون فيها الوثيقة. ويتمكن من العثور على غايتك حتى لو كانت ضمن مرفقات رسالة بالبريد الإلكتروني.

وفي إكسل هناك مزايا جديدة مثل تحديث بيانات بعض الوثائق التي تضم أرقام مغيرة مثل الأسعار، فأسعار الأسهم تنال تعديلات ومزامنة حسب وضعها في السوق، وكل ذلك طبعا بعد اختيارك لهذه الميزة وطلبها. حيث تقوم بالتمرير على السعر في خلايا إكسل لتظهر العلامات الذكية ويأخذك لموقع الأسهم المعنية. كما يضم إكسل في أوفيس إكس بي أدوات سهلة لرسم الجداول بالقلم بصورة شبه يدوية وكذلك هو الحال بالنسبة لتلوين الوثيقة وجداولها.

● هذا ما تعد به مايكروسوفت في أوفيس إكس بي حيث يتاح لك استعادة الوثيقة التي كنت تعمل بها في حال انهار النظام ولم تقم قبلها بحفظ الوثيقة. وهي ميزة استعادة الوثائق التي تحفظ للمستخدم الوثائق والمستندات التي يعمل بها سواء اكانت نصاً أم جدولاً بشكل تلقائي في اللحظة التي يتوقف فيها احد برامج أوفيس إكس بي لأي سبب من الأسباب.

كما يتيح أوفيس إكس بي لمستخدميه إنجاز أمور كثيرة لم يعهدوها من قبل حيث بالإمكان وبنقرة ماوس واحدة الوصول إلى لوحات المهمات الجديدة كالبحث عن ملف معين أو إعداد المحتويات. كما ويسمح إوفيس إكس بي الوصول إلى المعلومات المطلوبة على الويب وتحليلها بسرعة وسهولة إضافة إلى إمكانية إضافة مؤشرات الأسهم وآخر الأخبار وأحوال الطقس إلى قواعد المعلومات والجداول وغير ذلك من الملفات الخاصة بالمستخدم ومن ثم يمكن ضبطها أيضاً ليتم تحديثها بشكل تلقائي عبر الإنترنت.

● ويأتي أوفيس إكس بي مزوداً بمجموعة متميزة من الخيارات الجديدة التي تزيد مستوى الاحتراف كوسائل التحرير المطورة وسبل العرض الجديدة وإمكانية دمج المكونات الشبكية ضمن الوثائق أضف على ذلك تقنية التعرف على الكلام التي يمكن من خلالها وعن طريق الإملاء الصوتي طباعة النصوص وتحريرها والتنقل بين القوائم وما إلى ذلك.

اما خدمات مايكروسوفت شير بوينت -Share Point المتعلقة بفرق العمل فهي تتيح وسيلة سهلة لمشاركة المعلومات والبيانات بين تطبيقات أوفيس إكس بي وموقع الشركة مثلاً على الإنترنت، إذ يستطيع أعضاء فريق العمل الواحد حمل وثائقهم على الموقع ومشاركتها في مناقشات موسعة واستبيانات متنوعة فضلاً عن إضافة مواد إلى الموقع كالإعلانات وأخبار الفعاليات المختلفة. ومن المزايا الجديدة ، وفي مجال الحوسبة التعاونية وعند قيامك بعمل مشترك في وثيقة ما يمكنك تتبع التعديلات وحفظها او استرداد الوثيقة الأصلية مع عرض التعديلات التي اجراها فريق العمل، و لكل واحد منهم على حدا.

● ويؤمن أوفيس إكس بي درجة عالية من الحماية والأمان فبإمكانك أثناء استخدام أحد برامج أوفيس إكس بي استرجاع وثائقك الضائعة في حالات الخطأ حيث يحتفظ أوفيس إكس بي بنسخة احتياطية من عملك ليتسنى لك استرجاعه وحفظه ثانية دون خسارة للبيانات أو إضاعة للوقت. كما يؤمن أوفيس إكس بي الحماية ضد الفيروسات إذ يضع بين أيدي خبراء تكنولوجيا المعلومات سلاحاً قوياً وفعالاً ضد الفيروسات يساعدهم على ضبط أنظمة حماية فرق العمل وبالتالي يقلل من الخسائر الناجمة عن تعطل العمل وفقدان البيانات.

إعداد/ نجود الزراجي

كيف تعمل الفيروسات

الخطوة الأولى في مكافحة فيروسات الكمبيوتر، هي فهم أنواعها وآليات عملها

● تتضمن معظم الكمبيوترات الشخصية المباعة حديثاً برامج لمكافحة الفيروسات، وهذه الحقيقة، أكثر من أي شيء آخر، تدلنا على مدى انتشار الفيروسات، ومدى قبول صناعة الكمبيوتر بها، كقدر لا مفر منه! لقد أصبحت الفيروسات أمراً واقعاً في عالم الكمبيوتر اليوم.

يوجد حالياً الآلاف من فيروسات الكمبيوتر، ويمكن تصنيفها إلى عدة فئات، لكنها جميعاً، على العموم، تخضع لتعريف مشترك بسيط: الفيروس هو برنامج كمبيوتر مصمم عمداً ليقترن ببرنامج آخر، بحيث يعمل الفيروس عندما يعمل ذلك البرنامج، ومن ثمّ يعيد إنتاج نفسه باقترانه ببرامج أخرى. ويقترن الفيروس بالبرنامج الأصلي بإلصاق نفسه به، أو باستبداله أحياناً، وقد يغير الفيروس نفسه عند إعادة الإنتاج، فيظهر كنسخة معدلة عن النسخة التي قبلها، كلما كرر العملية. ويمكن أن تتلوث برامج الماكرو بالفيروس، أو قطاع الإقلاع boot sector على القرص، وهو أول برنامج يتم تحميله من قرص يحمل ملفات إقلاع نظام التشغيل.

● لاحظ عبارة "مصمم عمداً" في التعريف، فالفيروسات لا تظهر صدفة، بل يكتبها مبرمجون ذوو مهارات عالية عادة، ثم يجدون طريقة لنشرها في أجهزة المستخدمين الغافلين عنها. وكلما اصبحت برامج مكافحة الفيروسات أقوى، زاد المبرمجون من جهودهم لتطوير فيروسات أذكى، للتحايل عليها. والهدف من تطوير الفيروسات، بالنسبة للكثير من مؤلفيها، ليس أكثر من تحد، والرغبة في إثبات تفوقهم، بينما هو للبعض الآخر التلذذ بإثارة حيرة الآخرين وشكوكهم في الكمبيوتر، أو إزعاجهم، وحتى إيذائهم! وهذا أمر سيئ جداً، إذ يمكنهم أن يجنوا أموالاً طائلة، إذا وجهوا مواهبهم لمساعدة الشركات على حل مشكلة العام ٢٠٠٠، بدلاً من هدرها في أعمال لا طائل منها، مثل تطوير الفيروسات.

اشتهرت فيروسات الكمبيوتر بقدرتها على الأذى وإحداث الأضرار، لكن في الحقيقة، فإن الكثير منها غير مؤذ. صحيح أن بعضها يحذف الملفات، أو يقوم بأعمال تخريبية أخرى، لكن معظمها يسبب إزعاجاً بسيطاً فقط، وبعضها لا يلحظه المستخدم العادي أبداً. ويكفي أن يتمكن البرنامج من إعادة إنتاج نفسه حتى يعتبر فيروساً، بغض النظر عن الأعمال التي ينفذها.

● لكن، في الحقيقة، حتى الفيروسات غير المؤذية، تسبب بعض الأذى! فهي تستهلك مساحات تخزين على القرص، وجزءاً من ذاكرة الكمبيوتر، وتشغل جزءاً من طاقة المعالج، وبالتالي فهي تؤثر على سرعة وكفاءة الجهاز. أضف إلى ذلك، أن برامج كشف الفيروسات وإزالتها، تستهلك أيضاً موارد الجهاز. ويرى الكثير من المستخدمين، أن برامج مكافحة الفيروسات تبطئ عمل الجهاز بشكل ملحوظ، وهي أكثر تطفلاً عليه من الفيروسات ذاتها! وبعبارة أخرى، تؤثر الفيروسات في عالم الكمبيوتر، حتى إذا لم تكن تفعل شيئاً.

الفيروسات وأشباه الفيروسات

إن الشرح المذكور في الفقرة السابقة عن الفيروس، أكثر تحديداً من الطريقة التي نستخدم فيها كلمة "فيروس" في الواقع. وتوجد أنواع أخرى من البرامج، ينطبق عليها تعريف الفيروس جزئياً. تشترك هذه الأنواع مع الفيروسات في أنها تعمل بدون علم المستخدم، وتقوم بأعمال ضمن الكمبيوتر، مصممة عمداً لتنفيذها. ومن هذه الأنواع: الديدان(worms)، وأحصنة طروادة(Trojan horses)، وبرامج الإنزال (droppers). وتعتبر كل هذه البرامج، بما فيها الفيروسات، جزءاً من فئة أكبر تدعى البرامج الماكرة (malware)، وهي مشتقة من عبارة malicious-logic software.

*والدودة برنامج يعيد إنتاج نفسه، لكنها لا تلوث برامج أخرى. تنسخ الدودة نفسها من وإلى الأقراص المرنة، أو عبر الشبكات، ويعتمد بعضها على الشبكة في إنجاز عملها. تستخدم إحدى أنواع الديدان -وهي الدودة المضيفة -(host worm) الشبكة لنسخ نفسها، فقط إلى أجهزة الكمبيوتر المتصلة بالشبكة. بينما توزع الدودة الشبكية ((network worm أجزاءها على عدة كمبيوترات، وتعتمد على الشبكة فيما بعد لتشغيل هذه الأجزاء. ويمكن أن تظهر الديدان على كمبيوترات منفصلة، فتنسخ نفسها إلى أماكن متعددة على القرص الصلب.

وسمي النوع الثاني من البرمجيات الماكرة "حصان طروادة"، نسبة للأسطورة الإغريقية الواردة في ملحمة الأوديسا لهوميروس، حيث ترك الجيش الإغريقي حصاناً خشبياً ضخماً، كهدية لسكان طروادة، وكان يختبئ ضمنه مجموعة من الجنود الأشداء، بعد أن تظاهروا بإنهاء الحصار الطويل، وعندما رحل الجيش وأدخل السكان الحصان إلى داخل أسوار المدينة، خرج الجند منه وانقضوا على الحامية، وسقطت المدينة في أيدي الإغريق. وتعتمد برامج أحصنة طروادة على المبدأ ذاته، فهي تختبئ ضمن برامج يبدو ظهرها بريئاً، وعندما يشغّل المستخدم واحداً من هذه البرامج، ينشط الجزء الماكر ويقوم بعمل معين مصمم له. وتختلف أحصنة طروادة عن الفيروسات العادية، في أنها لا تعيد إنتاج نفسها.

● وصممت برامج الإنزال (droppers) لمراوغة برامج مكافحة الفيروسات، وتعتمد على التشفير غالباً لمنع اكتشافها. ووظيفة هذه البرامج عادة، نقل وتركيب الفيروسات، فهي تنتظر لحظة حدوث أمر معين على الكمبيوتر، لكي تنطلق وتلوثه بالفيروس المحمول في طياتها.

وينتمي مفهوم قنبلة (bomb) الكمبيوتر إلى هذه الفئة، إذ تبنى القنابل ضمن البرمجيات الماكرة كواسطة لتنشيطها. وتبرمج القنابل لتنشط عند حدوث حدث معين. تنشط بعض القنابل في وقت محدد، اعتماداً على ساعة الكمبيوتر. فيمكن برمجة قنبلة مثلاً، لمسح كافة الملفات ذات الامتداد .DOC من قرصك الصلب، عشية رأس السنة الميلادية، أو لعرض رسالة على الشاشة، في اليوم المصادف لعيد ميلاد شخصية مشهورة. وتعمل بعض القنابل تحت شروط أو أحداث أخرى، فيمكن أن تنتظر القنبلة إلى أن يتم تشغيل برنامج معين، لعشرين مرة مثلاً، وعندها تمسح ملفات القوالب ((templates الخاصة بهذا البرنامج.

ومن وجهة النظر هذه، تعتبر القنابل مجرد برامج جدولة زمنية ماكرة.

● ويمكننا النظر إلى الفيروسات كحالات خاصة من البرمجيات الماكرة، إذ يمكن للفيروسات الانتشار بواسطة برامج الإنزال (ولا يشترط ذلك)، وهي تستخدم مفهوم برامج الديدان لإعادة إنتاج نفسها. ولا تعتبر الفيروسات مماثلة لأحصنة طروادة من الناحية التقنية، إلا أنها تشابهها في نقطتين: فهي تنفذ أعمالاً لا يريدها المستخدم، وتحول البرنامج الذي تلتصق به إلى حصان طروادة عملياً (تختبئ داخله، وتعمل عندما يعمل البرنامج، وتنفذ أعمالاً غير مرغوبة).

كيف يعمل الفيروس؟

تعمل الفيروسات بطرق مختلفة، وسنعرض فيما يلي للطريقة العامة التي تنتهجها كافة الفيروسات. في البداية يظهر الكمبيوتر على جهازك، ويكون قد دخل إليه مختبئاً في ملف برنامج ملوث (مثل ملفات COM أو EXE أو قطاع الإقلاع). وكانت الفيروسات في الماضي تنتشر بشكل أساسي عن طريق توزيع أقراص مرنة ملوثة. أما اليوم، فمعظمها يأتي مع البرامج المنقولة عبر الشبكات (ومن بينها إنترنت)، كجزء من برنامج تركيب نسخة تجريبية من تطبيق معين، أو ماكرو لأحد التطبيقات الشهيرة، أو كملف مرفق (attach(ment) برسالة بريد إلكتروني.

● ويجدر التنويه إلى أن رسالة البريد الإلكتروني نفسها لا يمكن أن تكون فيروساً، فالفيروس برنامج، ويجب تشغيله لكي يصبح نشطاً. إذاً الفيروس المرفق برسالة بريد إلكتروني، لا حول له ولا قوة، إلى أن تشغّله. ويتم تشغيل فيروسات المرفقات عادة، بالنقر عليها نقرة مزدوجة بالماوس. ويمكنك حماية جهازك من هذه الفيروسات، بالامتناع عن تشغيل أي ملف مرفق برسالة بريد إلكتروني، إذا كان امتداده COM أو EXE، أو إذا كان أحد ملفات بيانات التطبيقات التي تدعم الماكرو، مثل برامج أوفيس، إلى ما بعد فحصه والتأكد من خلوه من الفيروسات. أما ملفات الرسوميات والصوت، وأنواع ملفات البيانات الأخرى القادمة كمرفقات، فهي آمنة، ولا يمكن للفيروس أن ينشط من خلالها، ولذلك فهو لا يهاجمها.

إذاً يبدأ الفيروس دورة حياته على الجهاز بشكل مشابه لبرنامج حصان طروادة، فهو يختبئ في ثنايا برنامج أو ملف آخر، وينشط معه. في الملفات التنفيذية الملوثة، يكون الفيروس قد أضاف شيفرته إلى البرنامج الأصلي، وعدل تعليماته بحيث ينتقل التنفيذ إلى شيفرة الفيروس. وعند تشغيل الملف التنفيذي المصاب، يقفز البرنامج عادة إلى تعليمات الفيروس، فينفذها، ثم يعود ثانية لتنفيذ تعليمات البرنامج الأصلي. وعند هذه النقطة يكون الفيروس ناشطاً، وجهازك أصبح ملوثاً.

● وقد ينفذ الفيروس مهمته فور تنشيطه (ويطلق عليه فيروس العمل المباشر (direct-action)، أو يقبع منتظراً في الذاكرة، باستخدام وظيفة "الإنهاء والبقاء في الذاكرة" (terminate and stay resident, TSR)، التي تؤمنها نظم التشغيل عادة. وتنتمي غالبية الفيروسات لهذه الفئة، ويطلق عليها الفيروسات "المقيمة". ونظراً للإمكانيات الكبيرة المتاحة للبرامج المقيمة في الذاكرة، بدءاً من تشغيل التطبيقات والنسخ الاحتياطي للملفات إلى مراقبة ضغطات لوحة المفاتيح ونقرات الماوس (والكثير من الأعمال الأخرى)، فيمكن برمجة الفيروس المقيم، لتنفيذ أي عمل يمكن أن يقوم به نظام التشغيل. تقريباً. يمكن تشغيل الفيروس المقيم كقنبلة، فيبدأ مهمته على جهازك عند حدث معين. ومن الأمور التي تستطيع الفيروسات المقيمة عملها، مسح ((scan قرص الصلب وأقراص الشبكة بحثاً عن الملفات التنفيذية، ثم نسخ نفسها إلى هذه الملفات وتلويثها.

أنواع الفيروسات

يبحث مطورو الفيروسات، بشكل دائم، عن طرق جديدة لتلويث كمبيوترك، لكن أنواع الفيروسات معدودة عملياً، وتصنّف إلى: فيروسات قطاع الإقلاع (boot sector viruses)، وملوثات الملفات (file infectors)، وفيروسات الماكرو (macro viruses). وتوجد أسماء أخرى لهذه الفئات، وبعض الفئات المتفرعة عنها، لكن مفهومها يبقى واحداً.

● تقبع فيروسات قطاع الإقلاع في أماكن معينة على القرص الصلب ضمن جهازك، وهي الأماكن التي يقرأها الكمبيوتر وينفذ التعليمات المخزنة ضمنها، عند الإقلاع. تصيب فيروسات قطاع الإقلاع الحقيقية منطقة قطاع الإقلاع الخاصة بنظام دوس (DOS boot record)، بينما تصيب فيروسات الفئة الفرعية المسماة MBR viruses، قطاع الإقلاع الرئيسي للكمبيوتر (mas-ter boot record).

يقرأ الكمبيوتر كلا المنطقتين السابقتين من القرص الصلب عند الإقلاع، مما يؤدي إلى تحميل الفيروس في الذاكرة. يمكن للفيروسات أن تصيب قطاع الإقلاع على الأقراص المرنة، لكن الأقراص المرنة النظيفة، والمحمية من الكتابة، تبقى أكثر الطرق أمناً لإقلاع النظام، في حالات الطوارئ. والمشكلة التي يواجهها المستخدم بالطبع، هي كيفية التأكد من نظافة القرص المرن، أي خلوه من الفيروسات، قبل استخدامه في الإقلاع، وهذا ما تحاول أن تفعله برامج مكافحة الفيروسات.

● تلصق ملوثات الملفات (وتدعى أيضاً الفيروسات الطفيلية parasitic viruses) نفسها بالملفات التنفيذية، وهي أكثر أنواع الفيروسات شيوعاً. وعندما يعمل أحد البرامج الملوثة، فإن هذا الفيروس، عادة، ينتظر في الذاكرة إلى أن يشغّل المستخدم برنامجاً آخر، فيسرع عندها إلى تلويثه. وهكذا، يعيد هذا النوع من الفيروس إنتاج نفسه، ببساطة، من خلال استخدام الكمبيوتر بفعالية، أي بتشغيل البرامج! وتوجد أنواع مختلفة من ملوثات الملفات، لكن مبدأ عملها واحد.

تعتمد فيروسات الماكرو (macro viruses)، وهي من الأنواع الحديثة نسبياً، على حقيقة أن الكثير من التطبيقات تتضمن لغات برمجة مبيتة ضمنها. وقد صممت لغات البرمجة هذه لمساعدة المستخدم على أتمتة العمليات المتكررة التي يجريها ضمن التطبيق، من خلال السماح له بإنشاء برامج صغيرة تدعى برامج الماكرو. تتضمن برامج طاقم أوفيس، مثلاً، لغة برمجة مبيتة، بالإضافة إلى العديد من برامج الماكرو المبيتة أيضاً، والجاهزة للاستخدام المباشر. وفيروس الماكرو ببساطة، هو برنامج ماكرو مصمم للعمل مع تطبيق معين، أو عدة تطبيقات تشترك بلغة برمجة واحدة.

● أصبحت فيروسات الماكرو شهيرة بفضل الفيروس المصمم لبرنامج مايكروسوفت وورد. فعندما تفتح وثيقة أو قالباً ملوثين، ينشط الفيروس ويؤدي مهمته التخريبية. وقد برمج هذا الفيروس لينسخ نفسه إلى ملفات الوثائق الأخرى، مما يؤدي إلى ازدياد انتشاره مع استمرار استخدام البرنامج.

ويجمع نوع رابع يدعى الفيروس "متعدد الأجزاء" (multipartite) بين تلويث قطاع الإقلاع مع تلويث الملفات، في وقت واحد.. ستجد قائمة ضخمة بأسماء الفيروسات، مع شرح تفصيلي عن آثار كل منها، في قسم Virus Encyclopedia من موقع مختبر مكافحة الفيروسات، الخاص بشركة سيمانتك، على العنوان: http://www.symantec.com/avcenter/vinfodb.html

ذكاء الفيروسات في ازدياد

● نجح مبدأ فيروس الماكرو، لأن لغات البرمجة أمنت إمكانية الوصول إلى الذاكرة والاقتراض الصلبة. وهذا ما أمنته التقنيات الحديثة أيضاً، بما فيها عناصر تحكم ActiveX، وبرمجيات جافا (Java applets). صحيح أن هذه التقنيات صُممت مع ضمان حماية القرص الصلب من برامج الفيروسات (تعد جافا أفضل من ActiveX في هذا المجال)، لكن الحقيقة أن هذه البرامج تستطيع تركيب نفسها على جهازك بمجرد زيارتك لموقع ويب. ومن الواضح أن أجهزتنا ستكون أكثر عرضة لمخاطر الفيروسات والبرمجيات الماكرة الأخرى، مع ازدياد تشبيك الكمبيوترات ببعضها، وبشبكة إنترنت، خصوصاً مع المزايا التي تعدنا بها إنترنت لإجراء ترقية نظم التشغيل عبرها (يؤمن نظاما ويندوز٩٨ وويندوز٢٠٠٠ هذه الإمكانيات).

إن أقل ما يوصف به مطورو الفيروسات، هو مهارتهم وقدرتهم الفذة على الابتكار، فهم يخرجون إلينا دائماً بطرق جديدة لخداع برامج مكافحة الفيروسات. فمثلاً، تضلل الفيروسات المتسللة (stealth viruses) الجديدة، برامج مكافحة الفيروسات، بإيهامها أن الأمور تسير على ما يرام، ولا يوجد أي مؤشر على وجود فيروس. كيف؟

● يعتمد مبدأ عمل الفيروس المتسلل، على الاحتفاظ بمعلومات عن الملفات التي لوثها، ثم الانتظار في الذاكرة، ومقاطعة عمل برامج مكافحة الفيروسات خلال بحثها عن الملفات المعدلة، وإعطائها المعلومات القديمة التي يحتفظ بها عن هذه الملفات، بدلاً من السماح لها بالحصول على المعلومات الحقيقية من نظام التشغيل!

أما الفيروسات متغيرة الشكل -(polymorphic virus es)، فتعدل نفسها أثناء إعادة الإنتاج، مما يجعل من الصعب على برامج مكافحة الفيروسات التي تبحث عن نماذج معينة من مثل هذا الفيروس، اكتشاف كافة أشكاله الموجودة، وبالتالي تستطيع الفيروسات الناجية، الاستمرار وإعادة إنتاج أشكال جديدة.

● تظهر أنواع جديدة من الفيروسات إلى حيز الوجود بشكل دائم، مع استمرار لعبة القط والفار بين مطوري الفيروسات ومنتجي برامج مكافحتها. وأغلب الظن أن الفيروسات ظهرت لتبقى، إلى ما شاء الله.

دع الكمبيوتر يوقظك من النوم!

● بإمكانك الاعتماد على كمبيوترك الشخصي ليوقظك صباحاً، بالاتصال بأقرب هاتف إلى فراشك! لكن لماذا تفعل هذا بدلاً من استخدام الساعة المنبهة؟

وجدت أنه من السهل تجاهل أو إسكات معظم أصوات الساعات المنبهة، لكن سيكون من الصعب نفسياً، ترك الهاتف يرن لمدة طويلة!

● أنشأت لهذا الغرض ملف باتش باسم Wakeup. Bat، وأدخلت فيه الأوامر اللازمة، للاتصال برقم هاتف معين، وتركه يرن لمدة ٩٠ ثانية، وذلك بإرسال سلسلة حروف تمثل أمر مودم، إلى بوابة الاتصال التسلسلي. استخدمت الأمر T/ Choice في ملف الباتش كمؤقت للنجاة من الإخفاق، وضمان عودة حالة الهاتف إلى وضع الانتظار. بعد أن تنشئ ملف الباتش، انقر عليه بالزر الأيمن للماوس ضمن برنامج مستكشف ويندوز، ثم اختر "خصائص"، ثم لسان التبويب "برنامج"، وانقر مربع الاختيار "إغلاق عند الإنهاء".

تحتاج لتشغيل ملف Wakeup. Bat، إلى برنامج جدولة زمنية ((Scheduling مثل System Agent الذي يأتي مع ويندوز٩٥ بلس باك، أو أي برنامج مماثل. يمكنك إذا استخدمت برنامج System Agent، إضافة تشغيل ملف الباتش كمهمة جديدة، وتعيين الأوقات والأيام التي تريد تشغيله فيها خلال الأسبوع، وضبط تكرار تشغيله، على عدد المرات الذي تريده.

● تعين السلسلة الحرفية S7=90 للمودم طول المدة التي سيرن خلالها الهاتف قبل أن ينشئ الاتصال. وإذا أرسلت الأمر + FCLASS=1 للمودم، فسوف يرسل صوت جهاز الفاكس عند محاولته إنشاء الاتصال، لدى رفعك سماعة الهاتف، وبهذا تعلم أن المتصل مودم وليس شخصاً حقيقياً (رئيسك في العمل، مثلاً!).

استخدم هذه الطريقة ثلاث مرات أسبوعياً على الأقل، حيث يتولى تنفيذها برنامج System Agent، الذي يشغل ملف الباتش ضمن كمبيوتري الموجود في المكتب، ولعدة مرات، فلا أضيّع الاجتماعات المهمة، بعد جلسات البرمجة التي تبدأ من الغسق وتنتهي عند الفجر.

● أضفنا بعض الأوامر القليلة إلى ملف Wakeup. Bat، لنضمن أن حالة المودم السابقة لن تمنعه من طلب رقم الهاتف. يعمل الأمر MODE على تحضير المودم للاستخدام، حيث ضبطنا معدل سرعة ال