البرامج الخبيثة وأخطارها

ما المقصود بالبرامج الخبيثة؟

يُطلق مصطلح "البرامج الخبيثة"، (Malicious Software) أو اختصاراً بـ Malware، على أي برامج يتم تثبيتها على جهاز الحاسوب و تقوم بوظائف غير مرغوب فيها، و غالباً ما يكون مصدرها جهات ربحية إعلانية. تتراوح الوظائف التي تقوم بها البرامج الخبيثة ما بين نشر الإعلانات المزعجة إلى إحداث خلل حقيقي في عمل النظام و قد يؤدي بدوره إلى تدمير البيانات على جهاز الحاسوب. بالاضافة إلى عمليات سرقة كلمات المرور و إصابة الأجهزة الأخرى على نفس الشبكة. تقوم بعض البرامج الخبيثة أيضاً بمراقبة عادات التصفح للمستخدم و إرسال هذه البيانات إلى جهات خارجية بهدف الاستفادة لأغراض إعلانية.

أنواع البرامج الخبيثة وآلية عملها

فيما يلي بعض تصنيفات البرامج الخبيثة:

- **الفيروسات** (Viruses) – هي عبارة عن برامج لها قابلية نسخ نفسها و الانتشار إلى أجهزة الحاسوب الأخرى و قد تقوم بدمج نفسها مع ملفات و بيانات موجودة بالفعل بما يسبب تلفاً للبيانات و خلل في عمل البرامج المختلفة. و بعض الفيروسات قد تستهلك ذاكرة الحاسوب بشكل كامل.

- **برامج الإعلانات** (Adware) – هي برامج يتم دعمها مادياً من منتجها أو من جهات آخرى، و هذه البرامج تقوم بعرض إعلانات للمستخدم عند استخدامه للانترنت، و هي غالباً ما تقوم بمراقبة المحتوى الذي يتصفحه المستخدم ة بناءً عليها يتم عرض الإعلانات المختلفة.

- **برامج التجسس** (Spyware) – هي برمجيات تقوم خلسةً بجمع المعلومات عن المستخدمين و ارسالها إلى جهات خارجية مهتمة بجمع البيانات، و تتراوح المعلومات التي يتم جمعها ما بين قائمة المواقع التي يتصفحها المستخدم إلى معلومات متعلقة بعنوان المستخدم و نظام تشغليه و حتى بيانات بطاقات الائتمان و قوائم المحادثة و المراسلات و عناوين البريد

الالكتروني، و أيضاً قد تقوم بجمع معلومات عن نوع اتصال الانترنت لدى المستخدم و عنوان الآيبي الخاص به.

- **برامج التطفل على المتصفح** (Browser Hijacking) – و هي برامج إعلانية و لكن بدلاً من اظهار الاعلانات بصورة صريحة تقوم بتغيير الإعدادات في المتصفح كإضافة أشرطة ادوات إعلانية و تغيير محرك البحث الافتراضي و الصفحة الرئيسية و قد تقوم بانشاء اختصارات على سطح المكتب و قد تقوم أيضاً بتحويل الروابط أثناء التصفح إلى مواقع و عناوين أخرى.

طرق انتشار البرامج الخبيثة

- **مُدمجة مع برمجيات أخرى:** وتكون بصورة مخفية و يطلق عليها غالباً البرامج المخفية أو اصطلاحاً بأحصنة طروادة (Trojan Horses) – *و هي التسمية المتأثرة بالملحمة التاريخية التي تم تهريب الجنود فيها داخل حصان خشبي كبير*– فمثلاً يوجد بعض برامج المحادثة الفورية التي تقوم بتثبيت برامج تجسس مثل برنامج WildTangent، بالاضافة إلى برامج المشاركة P2P مثل Kazaa و eMule و LimeWire و غيرها من البرامج التي تكون مدموجة مع برامج ذات أنشطة دعائية أو إعلانية، و هناك أيضاً فئة من البرامج التي تدعي تسريع التصفح و تقوم لذلك بتغيير إعدادات المتصفح ليتم استخدام إعدادات تخدم جهات خارجية لأغراض ربحية دعائية.

- **استغلال الثغرات الأمنية في متصفح الانترنت:** بعض البرامج الخبيثة يتم تثبيتها على أجهزة المستخدمين عبر استغلال لبعض الثغرات الأمنية في متصفح الانترنت أو في بعض الاضافات التي يدعمها المتصفح، فمثلاً هناك تقنية ActiveX و التي تُستخدم في ربط التطبيقات المكتبية بالانترنت، هذه التقنية يتم استغلالها من بعض المواقع لتثبيت البرامج على الأجهزة و ذلك عبر ظهور رسالة استعلام و عند الضغط على Yes يتم تثبيت البرنامج، وقد يتم تثبيت البرنامج إذا كانت إعدادات الأمان أقل من الوضع الطبيعي، هذه البرمجيات التي يتم تثبيتها عبر ActiveX اصبحت قليلة جداً و قاربت على الانتهاء لأن المتصفحات الحديثة تقوم بحظر هذه العناصر إلا إذا تم السماح بها من المستخدم بشكل

صريح، و في المقابل فهناك نوع جديد من البرمجيات التي تقوم باستغلال تقنيات تفاعلية أخرى مثل الـFlash .

- **حاجة بعض المواقع لبرامج خاصة:** بعض مواقع الانترنت تطلب من المستخدم تثبيت برامج خاصة ليتمكن من تصفح محتوى الموقع، و عند الموافقة على تثبيت البرنامج يتم زرع برامج مخفية و أما الرفض فقد يؤدي إلى ظهور رسائل خطأ عديدة و التي غالباً ما تكون مزيفة. هناك بعض المواقع التي تقوم باستخدام شهادات الأمان HTTPS و تُعلم المستخدم بأن الموقع آمن بسبب استخدام شهادات الأمان و هذا يعتبر تفسير خاطئ لشهادات الأمان التي تنحصر مهمتها في أمرين، الأول هو اثبات ان الشركة التي تملك الموقع هي نفسها الشركة التي تم تسجيل الموقع باسمها و الثاني هو أن البيانات المدخلة يتم تشفيرها بحيث لا يتمكن أحد من قراءتها سوى المستخدم و السيرفر فقط. و في كلا الحالتين فإن شهادات الأمان لا تثبت حُسن نية صاحب الموقع الذي يملك السيرفر على الاطلاق.

- **عبر البريد الالكتروني:** و هي طريقة شائعة لنشر البرمجيات الخبيثة بأنواعها، فقد يتم ارسال هذه البرامج من خلال مرفقات يتم ارسالها مع البريد الالكتروني أو قد تكون من خلال ارسال رسائل مزيفة أو وهمية (Phishing or Spam) بحيث يتم وضع روابط لمواقع تحتوي على برمجيات خبيثة فيتم تثبيت هذه البرمجيات من هذه المواقع من خلال الطرق المذكورة أعلاه.

دائرة أمن المعلومات