البرامج الخبيثة

التعريف

البرامج الخبيثة (Malicious Software) أو ما تختصر أيضا ب Malware تعرف بأنها برامج عادية مثل البرامج التي نستخدمها بشكل دوري، و لكن لها طابع خبيث مختلف عن البرامج العادية وتقوم بوظائف غير مرغوب بها، وتتراوح الوظائف التي تقوم بها هذه البرمجية ما بين نشر اعلانات مزعجة أو خلل كبير في النظام يودي الي تدميره البيانات بشكل كلي. كما تقوم هذه البرمجيات بعمليات سرقة لبيانات الحاسوب من كلمات مرور وملفات حساسة وإرسالها إلى جهات خارجية إضافة إلى إصابة أجهزة الشبكة الداخلية

أنواع البرامج الخبيثة و آلية عملها

1. **البرامج الخبيثة المعدية**

- **الفيروسات** (viruses) هي عبارة عن برامج لها قابلية نسخ نفسها و الانتشار إلى أجهزة الحاسوب الأخرى من خلال دمج نفسها مع ملفات و بيانات موجودة بالفعل بما يسبب تلفاً للبيانات و خلل في عمل البرامج المختلفة أي أنها تحتاج الى وسيط يساعدها على الانتشار خلال الشبكة. و بعض الفيروسات قد تستهلك ذاكرة الحاسوب بشكل كامل أو تصدر رسائل مزعجة للمستخدم وغيرها.
- **الديدان** (worms) هي عبارة عن برامج يقوم بنشر نفسه على الشبكة لتصيب الحواسب الأخرى دون الحاجة لوسيط لعملية الانتشار مستعينا بالثغرات الأمنية الموجودة في البرامج أو الأنظمة. و هي أكثر خطورة من الفيروسات لسرعة انتشارها.

2. **البرامج الخبيثة الصامتة**

- **أحصنة طروادة** – (Trojan horses) :حصان طروادة هو أي برنامج يدعو المستخدم لتشغيله لكنه يخفي في الحقيقة أذىً أو نتائج سيئة. فهذه النتائج قد تكون أي شيء: قد تقوم بالعمل مباشرةً كأن يتم حذف جميع ملفات المستخدم، أو من الممكن (وذلك منتشر أكثر) أن تقوم بدورها بتنصيب برنامج مؤذي في نظام المستخدم لتخدم أهداف منشئ الحصان على المدى البعيد. فمثلاً بعض برامج المحادثة الفورية التي تقوم بتثبيت برامج تجسس مثل برنامج WildTangent ، بالإضافة إلى برامج المشاركة P2P مثل Kazaa و eMule 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 وغيرها.

- **الثغرات الخلفية** – (backdoor): وهي من أحد واهم الطرق التي تستخدم لتجاوز نظم المصادقة الطبيعية، وتحدث عندما يتم اختراق نظام معين فيقوم المخترق بفتح ثغرات خلفية (backdoor) لتسهل عليه عملية الدخول في المستقبل.

- **الجذور الخفية** – (Rootkit) وهي تقنية تقوم علي إخفاء البرمجية الخبيثة بعد تنصيبها على النظام. وهذه التقنية التي تعرف باسم RootKits تؤمن هذا الإخفاء وذلك عن طريق تعديل ملفات النظام المضيف بحيث يكون البرنامج الخبيث مخفياً عن المستخدم. علاوةً على ذلك قد تقوم الـ RootKit بمنع الإجرائية process الخاصة بالبرمجية الخبيثة من الظهور في قائمة البرامج التي تعمل، أو منع ملفاتها من القراءة.

3. البرامج الخبيثة لأغراض ربحية

- **برامج التجسس** – (Spyware) هي برمجيات تقوم خلسةً بجمع المعلومات عن المستخدمين و إرسالها 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 الجهاز (IP) الخاص به.

- **برنامج تسجيل نقرات لوحة المفاتيح** – (key logger) هو برمجية خبيثة تقوم بنسخ ضربات المستخدم على لوحة مفاتيح الحاسب عند إدخاله كلمة سر أو رقم بطاقة ائتمانية أو أية معلومة مفيدة أخرى. و من ثم يتم إرسالها إلى منشئ البرنامج تلقائياً مما يمكنه من سرقة البطاقة الائتمانية وأي شكل آخر من السرقة. و بالطريقة نفسها يمكن للبرمجية نسخ مفتاح القرص الليزر أو كلمة سر للعبة على الإنترنت فتسمح له بسرقة حسابات أو أمور أخرى افتراضية.

طرق الانتشار

1. **و سائط التخزين:** تنقل البرامج الخبيثة من حاسوب مصاب لآخر سليم من خلال وسائط التخزين التي تنقل الملفات والبرامج ومن أمثلة وسائط التخزين (Flash)
2. **مُدمجة مع برمجيات أخرى**
3. **استغلال الثغرات الأمنية** في أنظمة التشغيل أو البرامج كمتصفح الانترنت وغيرها وذلك من خلال تصفح مواقع مشبوهة التي تقوم باستغلال هذه الثغرات وغالبا ما تكون المواقع المشبوهة هي التي توفر البرامج المجانية أو مفاتيح البرامج المجانية.
4. **المراسلات من خلال المتحدث الفوري (Instant Messenger)** وهي برامج للتخاطب المباشر و نقل الملفات بشكل مباشر بين الاصدقاء.
5. **عبر البريد الالكتروني :** و هي طريقة شائعة لنشر البرمجيات الخبيثة بأنواعها، فقد يتم ارسال هذه البرامج من خلال مرفقات يتم ارسالها مع البريد الالكتروني

طرق الوقاية

1. لا تفتح أي ملف مرفق مع رسالة من شخص معروف إلا إذا كنت تتوقع ذلك الملف، وإذا كنت شاكل في سلامة الملف يمكنك التحقق من صديقك بأي طريقة اتصال.
2. لا تقم بفتح و قراءة أي رسالة من أشخاص مجهولين تحمل عنوانا غريبا مثل: (I love you, Your money, You win) لأن بعض برامج تصفح البريد الالكتروني.
3. من الأفضل عدم استعراض الرسائل المعدة بواسطة لغة HTML.
4. قم بتحميل البرامج من مواقعها الرسمية ولا تحمل أي ملف من غريب، سواء عن طريق البريد الإلكتروني، أو المراسل الآني، أو مواقع مشبوهة أو غيرها من الطرق.
5. أفحص أي ملف تريد تحميلة لجهازك بواسطة برنامج مكافح الفيروسات للتحقق من برامج خبيثة.
6. قم بأخذ نسخة احتياطية لملفاتك بشكل دوري، ولتكن خارج جهازك قد تستفيد منها في حال تمكن أحد الفيروسات من جهازك وحذف بعض الملفات.
7. قم بتحديث جميع برامجك لتفادي الثغرات الأمنية.