

المحاضرة السابعة عشر

برامج التجسس - طرق مكافحة برامج التجسس

برامج التجسس وطرق مكافحتها

مقدمة : خلال السنوات القليلة الماضية ظهرت فئة جديدة من البرامج الماكرة هي برامج التجسس، وبرنامج التجسس ليس بفيروس ولكن فعله أقوى وأخطر من الفيروسات والديدان وأحصنة طروادة، فبالرغم من عدم تسببه في تلف البيانات، إلا أنه يعمل عمله من وراء الكواليس بكل هدوء ودون علم المستخدم، ويقوم بنقل المعلومات لمالكه، وبرنامج التجسس هو عبارة عن خدعة ماكرة مثله في ذلك مثل الفيروس ولكن بصورة عامة أقل شهرة.

تعريف برنامج التجسس

يعتبر تعريف ويبوديا لبرنامج التجسس أفضل التعاريف الموجودة حيث عرّفه بأنه " أي برنامج يقوم سراً بالحصول على معلومات عن المستخدم عن طريق الربط بالإنترنت وخاصة بدعاوى دعائية وإعلانية". عادةً يتم تضمين برامج التجسس في شكل مكونات مجانية خفية أو برامج مشاركة يمكن تنزيلها من شبكة الإنترنت.

يمكن تصنيف برامج التجسس إلى نوعين رئيسيين: برامج رصد وتسجيل، وبرامج تتبع.

١. برامج الرصد والتسجيل

- النوع المعروف من برامج الرصد والتسجيل هو مسجل أو راصد المفاتيح (من لوحة المفاتيح) وحركات الفأرة وهي أكثر الأنواع شيوعاً وإزعاجاً في عملية سرقة كلمات السر وأرقام بطاقات الائتمان.
- يعمل في صمت في الخلف ويقوم بتسجيل ضغوطات المفاتيح وحركات الفأرة لكي يعيد ترتيب وتكوين ما يقوم بفعله المستخدم.
- هناك أيضاً راصدات ومسجلات للبريد الإلكتروني والردشة.

٢. برامج التتبع (المتتبعات)

تقوم بمراقبة عادات الاستخدام وأنماطه وتخزينها كبيانات إحصائية بهدف عمل التقارير بناءً عليها

طريقة عمل برنامج التجسس

تقوم الفيروسات بإتلاف البيانات على جهاز الحاسب الآلي ونسخ نفسها ذاتياً، في حين تعمل برامج التجسس خلسة ولا تتلف البيانات بل تتجسس عليها. يمكن لبرامج التجسس أن تقوم بنسخ نفسها على الجهاز وتعمل كمهمة خلفية، وتنقل المعلومات السرية الخاصة بالمستخدم لمالكها دون علم المستخدم. يمكن لبرنامج التجسس البقاء في أي صورة أو شكل من أشكال البرامج القابلة للتنفيذ بما في ذلك التطبيقات مثل (ActiveX, Plug-in) أو أكواد (Applets).

لدى برنامج التجسس مكونات أساسيان:

١. جزء في الواجهة الأمامية وهو برنامج عادي يعمل في العلن ويوفر وظائف مفيدة،
٢. جزء في الخلف وهو برنامج تجسس يراقب وينقل المعلومات.

- عادة لا تقوم برامج التجسس بجمع المعلومات الشخصية فقط، ولكن بالإضافة إلى ذلك تجمع المعلومات الديموغرافية وعادات التصفح.
- المعلومات المتحصل عليها من المحتمل أن يتم بيعها وإضافتها لقواعد البيانات الأخرى لبناء سجلات عن المستخدم وعادات استخدامه.
- يقوم البرنامج (الذي في جهاز الضحية) في كل مرة بنسخ المعلومات من جهاز الضحية بغرض تحديث سجل الضحية لدى مالك برنامج التجسس.

أعراض وجود برامج التجسس وطرق انتقالها :

- نشاط أعلى من الحد المعتاد.
- القيام بطلب الاتصال بالإنترنت تلقائياً .
- ظهور أشرطة أدوات غير مألوفة تتم إضافتها لمتصفح الإنترنت.
- اختيار صفحة بداية لمتصفح الإنترنت خلاف الصفحة التي تم ضبط المتصفح عليها من قبل المستخدم.
- أعراض وجود برامج التجسس وطرق انتقالها

ومن أشهر الطرق التي تنتقل بها برامج التجسس طريقتين هما :

١. تظهر وكأنها برامج نافعة أو عادية حتى يتم تثبيتها على الحاسب الآلي من قبل المستخدم وبعلمه.
٢. الاختفاء في برامج أخرى بحيث يتم تثبيتها مع تثبيت هذه البرامج دون علم المستخدم.

مكافحة برامج التجسس

- من أخطر ما تقوم به برامج التجسس هي أنها تقوم بإزالة برامج مكافحة التجسس. ويمكن القول بأنه ليس هناك برنامج يقوم بالحماية من برامج التجسس بدرجة كاملة

ولكن يمكن أخذ بعض التدابير الوقائية ومنها :

١. فلانتر خصائص استرجاع البيانات.
٢. حاجبات الإعلانات والنوافذ المنبثقة.
٣. استخدام مضادات برامج التجسس.
٤. استخدام جدار النار الشخصي وبرامج كشف التطفل.
٥. تأمين متصفح الإنترنت.
٦. تأمين إدخال كلمات المرور.

١. فلاتر خصائص استرجاع البيانات

يمكن إعداد (تفعيل/تعطيل) وسائل استرجاع البيانات أو ما يسمى بملفات الكوكي (Cookie Screeners) الخاصة بالمواقع التي تتم زيارتها وذلك من خلال المتصفح.

العديد من المستخدمين يقومون بتعطيل كافة وسائل استرجاع البيانات إلا أن هذا الإجراء قد لا ينصح به لأن الكثير من المواقع تتطلب تفعيل هذه الخدمة بالكامل.

البديل الآخر هو استخدام خاصية "التحذير قبل القبول" لكي يتم تنقيح المسترجعات يدوياً ولكن هذا من شأنه أن يؤدي لامتلاء الجهاز بأوامر حث تشغيل ملفات الكوكي (Cookie) عند القيام بتصفح الإنترنت.

في متصفحات الإنترنت الحديثة يمكن للمستخدمين نقل إعدادات الخصوصية للمواقع التي تتم زيارتها، وسيقوم المتصفح برفض الاسترجاع تلقائياً بالنسبة للمواقع التي ليس بها سياسة خصوصية

٢. حاجبات الإعلانات والنوافذ المنبثقة

حاجبات الإعلان والنوافذ المنبثقة (Pop-UP Blockers) هي عبارة عن برامج تقوم على إجهاض تنزيل وعرض صور الإعلانات الدعائية والإغراق الإعلاني، وكذلك منع النوافذ المنبثقة من الظهور التلقائي.

يمكن لحاجبات الإعلان أن تحسن من أداء المتصفح. ويمكن للمستخدمين أن يحافظوا على خلو الأقراص الصلبة الخاصة بهم من أي ملفات غير ضرورية باستخدام حاجبات الإعلانات.

يمكن لبعض حاجبات الإعلانات أن تحسن من عملية الخصوصية عن طريق تحديد المعلومات التي يتم إعطاؤها .

لدى مانعات الإعلان بعض الأثر السلبي الخفيف حيث إنها تعمل على حجب بعض الإعلانات المفيدة من خلال بعض المواقع غير الموقع الأصلي للإعلان.

ينصح بشدة بعدم السماح للنوافذ المنبثقة التي تظهر تلقائياً عند زيارة بعض المواقع وعدم استخدامها إلا بعد التأكد من مرجعيتها وصحة العنوان الذي تحمله.

٣. استخدام مضادات برامج التجسس

من أفضل وسيلة للدفاع ضد برامج التجسس وإزالتها في حال وجودها هي استخدام برامج مكافحة التجسس (Antispyware Scanners) وهي برامج شبيهة ببرامج مضادات الفيروسات من حيث طريقة تركيبها وتشغيلها وتحديثها.

يعمل برنامج مكافحة برامج التجسس بنفس طريقة برنامج مكافحة الفيروسات، كما يقوم برنامج مكافحة التجسس بحذف ملفات الكوكي الغير آمنة.

٤. استخدام جدار النار الشخصي وبرامج كشف التطفل

برامج التجسس يمكن أن تثبت نفسها أثناء تصفح الإنترنت، لذا فإن تثبيت برنامج الجدار الناري (Personal Firewall) قد يوفر بعض الحماية. وهذه الجدران النارية تقوم بحجب برامج التجسس إن وجدت ومنعها من الاتصال بالإنترنت دون إذن المستخدم.

يمكن للجدران النارية تنبيه المستخدمين حول أي محاولات للدخول لجهاز الحاسب أثناء تصفح الإنترنت، وكذلك إعلام المستخدمين إن كان هناك أي برنامج يحاول إرسال بيانات دون تفويض بذلك.

تستخدم أنظمة كشف التطفل (Intrusion Detection Systems (IDS)) لرصد محاولات الدخول الغير المصرح به، وكذلك مراقبة حركة الشبكة أو حالة النظام.

يعتمد نظام (IDS) على الخطة الموضوعية له. فهو يتطلب قاعدة بيانات تحدد ما هي السلوكيات السيئة أو غير المقبولة. عن طريق قاعدة البيانات يتعرف نظام كشف التطفل على ماهية الأنشطة العادية، ومن ثم يمكنه مراقبة التغييرات التي جرت والتي تدل على عملية التطفل أو النشاط المشكوك فيه.

٥. تأمين متصفح الإنترنت

من الإجراءات المضادة لبرامج التجسس هي ضبط إعدادات أمان متصفح الإنترنت لدرجة مقبولة من الأمان. يجب وضع الأمان في المستوى المتوسط أو العالي، مع الخيارات التالية لكل من (ActiveX) و (Plug-ins) في أنظمة تشغيل ويندوز :

١. ابطال كود (ActiveX) الغير مؤثر عليها بأنها آمنة.

٢. تنشيط التحكم بكل من (ActiveX) و (Plug-ins)

٣. تنشيط التحكم بتنزيل (ActiveX) وذلك من خلال السماح للمعروفة منها بأنها آمنة (Signed) ومنع غير

الآمنة (Unsigned)

تأمين إدخال كلمات المرور

من أحد طرق مكافحة برامج التجسس هي استخدام لوحة مفاتيح افتراضية مرسومة على الشاشة عوضا عن لوحة المفاتيح العادية عند إدخال كلمات المرور والأرقام السرية.

- يمكن من خلال هذا الإجراء منع برامج الرصد والتسجيل من التقاط الأزرار التي يتم الضغط عليها من قبل المستخدم وقد تم استخدام هذه الطريقة من قبل العديد من مواقع البنوك التجارية.