1-Malware

هي اختصار لكلمة برنامج ضار ويمكن ان يشير البرنامج الضار الى اي نوع من البرامج ، بصرف النظر عن طريقة تكوينه او تشغيله، وهو “مصمم لإلحاق الضرر بجهاز الكمبيوتر او السيرفر او شبكة جهاز الكمبيوتر مثلما تعرفه Microsoft : إن الفيروسات المتنقلة والفيروسات وحصان طروادة تندرج كلها تحت البرامج الضارة، ولايميزها عن بعضها البعض سوى الوسائل التي يتم استخدامها لإنشائها ونشرها.

2- التصيد (Phishing) :

التصيد تقنية يستخدمها مجرمو الفضاء الإلكتروني في إرسال رسائل بريد إلكتروني لخداع المستهدف من أجل القيام ببعض الأعمال الضارة.ربما يتم خداع المستلم في تنزيل برنامج ضار متخفي في صيغة مستند هام، على سبيل المثال ، او مطالبته بالنقر فوق احد الروابط التي تقوم بتوجيهه الى موقع ويب زائف حيث يتم سؤاله عن معلومات حساسة مثل اسماء المستخدمين وكلمات المرور الخاصة بالبنك

3- حجب الخدمات (Denial Of Service)

هجوم حجب الخدمات هو اسلوب استخدام القوة الغاشمة لمحاولة إيقاف تشغيل بعض الخدمات عبر الإنترنت . على سبيل المثال، قد يقوم المهاجمون بإرسال الكثير من البيانات الى احد مواقع الويب او الكثير من الطلبات الى احدى قواعد البيانات والتي تتسبب في ملئ تلك الأنظمة وتعطيلها عن العمل ، وهو ماقد يجعلها غير متاحة لأي شخص. يستخدم هجوم حجب الخدمات الموزعة (DDoS) مجموعة من أجهزة الكمبيوتر ، وعادة ماتكون مخترقة عن طريق البرامج الضارة وتحت سيطرة مجرمي الفضاء الإلكتروني ، لإرسال البيانات الى المستهدفين

4- هجمات الرجل في المنتصف (Man In The Middle):

هجوم الرجل في المنتصف (MITM) طريقة ينجح بها المهاجمون في إقحام أنفسهم سرا بين المستخدم وخدمة الويب التي يحاولون الوصول اليها. على سبيل المثال،ربما يقوم المهاجم بإعداد شبكة Wi-Fi مزودة بشاشة تسجيل مصمة بشكل يحاكي احدى شبكات الفنادق ؛وبعد ان يقوم المستخدم بتسجيل الدخول ، يمكن ان يجمع المهاجم اي معلومات يرسلها المستخدم ، ويشمل ذلك كلمات المرور الخاصة بالبنك الذي يتعامل معه

5- التعدين الخبيث (CryptoJacking):

التعدين الخبيث عبارة عن هجوم مخصص وفيه يتم اختراق احد اجهزة الكمبيوتر الخاصة بأحد الاشخاص واستخدامها لتعدين العملات الرقمية المشفرة (إجراء يطلق عليه التعدين في قاموس مصطلحات عملات التشفير).

سيحاول المهاجمون إما تثبيت احد البرامج الضارة على جهاز الكمبيوتر الخاص بالضحية لتنفيذ العمليات الحسابية المطلوبة او احيانا تشغيل التعليمة البرمجية في JavaScript والتي يتم تنفيذها في المستعرض الخاص بالضحية .

6- حقن SQL:

حقن SQL عبارة عن وسيلة تُمكن المهاجم من استغلال الثغرات في السيطرة على قاعدة بيانات الضحية. توجد العديد من قواعد البيانات المُصممة لتنفيذ أي أوامر مكتوبة في لغة الاستعلامات المركبة (SQL)، وتقوم العديد من مواقع الويب التي تجمع المعلومات من المستخدمين، بإرسال هذه البيانات إلى قواعد بيانات SQL. أثناء الهجوم باستخدام حقن SQL، سيقوم المخترق، على سبيل المثال، بكتابة بعض أوامر SQL في أحد نماذج الويب التي تطلب معلومات الاسم والعنوان؛ وإذا لم يتم برمجة موقع الويب وقاعدة البيانات بشكلٍ صحيح، فربما تحاول قاعدة البيانات تنفيذ تلك الأوامر.

7- هجمات دون انتظار (Zero-Day) :

الهجمات دون انتظار هي عبارة عن ثغرات في البرامج لم يتم حلها الى الان وسميت كذلك لانه بمجرد إصدار حزمة ، يتناقص كل يوم عدد الأجهزة المفتوحة المعرضة للهجوم اثناء تسجيل المستخدم تحديثات الأمان .