**البرمجيات الخبيثة Malware:**

**البرمجيات الخبيثة هو مصطلحٌ يُستخدم لوصف البرمجيات التي تخترق الشبكة أو الأنظمة دون علم ملّاكها من خلال ثغرةٍ أمنية، ويحدث تنشيطها عادةً من قِبل المستخدم عند النقر على رابط مشبوه، أو تنزيل مرفق بريد إلكتروني مجهول المصدر. ومن أمثلتها:**

**برمجيات التجسس Spyware: وهي برمجياتٌ تعمل على نقل المعلومات من الأجهزة المُصابة دون علم مالكيها بهدف التجسس.**

**برمجيات الفدية Ransomware : هي نوعٌ يُصمًّم بهدف ابتزاز المال، وذلك من خلال منع المستخدم من الوصول إلى الملفات أو نظام الحاسوب حتى تُدفع الفدية. ومع ذلك، لا يُعد دفعها ضماناً حتمياً لاسترداد الملفات أو النظام.**

**ومثالًا على ذلك هجوم برنامج الفدية "Wanna cry " الذي انطلق في شهر مايوعام 2017م، وأطاح بأكثر من 230 ألف جهاز، لا سيما المتعلقة منها بالقطاع الصحي، في 99 دولة حول العالم.**

**هجمات يوم الصفر Zero-Day Attack:**

**يُطلق هذا الاسم على الهجمات التي تستغل الثغرات الأمنية قبل اكتشافها من قِبل الجهة نفسها، وقبل أن تشرع في إصلاحها وإيجاد الحلول لها. ‍**

**الهجمات المستهدفة:**

**يتم فيه استخدام عدد من أساليب القرصنة لمهاجمة مستخدمٍ أو منظمةٍ محددةٍ مسبقاً.**

**حقن تعليمات الاستعلام "SQL":**

**يتضمن هذا النوع من الهجمات إدراج التعليمات البرمجية الخبيثة في خادم باستخدام حقن تعليمات الاستعلام الهيكلية (إس كيو إل)، وذلك يجبر الملقم على كشف المعلومات التي لا تُكشف غالباً. ويمكن للمهاجم تبنّي هذه الهجمة عبر إرسال شفرةٍ خبيثة إلى مربع بحث في أحد مواقع الويب الضعيفة.**

**الهندسة الاجتماعية Social Engineering:**

**وهو تهديدٌ يلجأ إلى استخدام أساليب مختلفةٍ للتأثير على الضحية ودفعه لكشف معلوماتٍ شخصية أو سرية حساسة دون أن يشعر، ومن ثم استخدامها بغرض الاحتيال.**

**التصيّد الاحتيالي Phishing:**

**يتضمن إرسال رسائل بريد إلكتروني احتيالية، تشبه رسائل المصادر الموثوقة. وتهدف إلى سرقة بيانات حساسة مثل أرقام بطاقات الائتمان، ومعلومات تسجيل الدخول. وهو من أكثر أنواع الهجمات السيبرانية شيوعاً.**

**هجوم الوسيط (Man-in-the-Middle):**

**نوعٌ من أنواع الهجمات التي تُعرف أيضاً باسم هجمات التنصت، ويحدث أن يعترض المهاجم خط التواصل بين طرفين بغرض التنصت، أو التلاعب بالمعلومات المتبادلة بينهما أو سرقتها.**

**حجب الخدمة DDos:**

**يستهدف هجوم حجب الخدمة الخدمات الإلكترونية أو الشبكة بهدف منع المستخدمين من الوصول إليها عبر إغراقها بطلبات وهمية تتسبب في عجز النظام عن تلبية الطلبات الحقيقية. ‍**