أبرز أنواع الهجمات السيبرانية حتى عام 2021الهجمات السيبرانية أبرز أنواع الهجمات السيبرانية حتى عام 2021 مجموعة ريناد المجد لتقنية المعلومات RMGتعتبر الهجمات السيبرانية مصدر القلق الأول لدى كل المنظمات والأفراد حول العالم في ظل العصر الرقمي الذي نعيشه اليوم، فمع زيادة التقدم والتطور بالتقنية والنمو المستمر لحجم التعاملات ونقل البيانات الحساسة التي تتم عبر الشبكات، وكذلك التخزين على الأجهزة المتصلة بالشبكة،إذاً ما هو الهجوم السيبراني؟الهجوم السيبراني هو عمل متعمد يقوم به مجرم إلكتروني أو أكثر لسرقة البيانات أو تلفيق المعلومات أو تعطيل الأنظمة الرقمية لأفراد او منظمات بأكلمها. من خلال هجمات الأمن السيبراني ، يحصل مجرمو الإنترنت على وصول غير قانوني وغير مصرح به إلى واحد أو أكثر من أجهزة الكمبيوتر ليتم استخدامها فيما بعد وفقاً لأهدافهم الإجرامية.للتعامل مع الأنواع المختلفة من الهجمات السيبرانية،ما هي أنواع الهجمات السيبرانية؟أظهرت دراسات مختلفة تنوع الهجمات الإلكترونية في الأمن السيبراني، وكذلك وجود محاولات مستمرة من المجرمين الاكترونيين لتطوير أساليب الهجمات السيبرانية لتتوافق مع أي تحديثات أمنية يقوم بها خبراء الأمن السيبراني.وفي هذا المقال سنذكر 20 من أبرز أنواع الهجمات الإلكترونية شيوعاً والمكتشفة حتى عام 2021 وهي كالآتي:الهجمات السيبرانية أبرز أنواع الهجمات السيبرانية حتى عام 2021 مجموعة ريناد المجد لتقنية المعلومات RMG1. هجمات التصيد الاحتيالي (PHISHING ATTACKS) بما في ذلك بيانات اعتماد تسجيل الدخول وأرقام بطاقات الائتمان.كيف يحدث هذا النوع من الهجمات السيبرانية؟يبدأ هذا الهجوم عندما يتمكن المجرم الإلكتروني من خداع ضحية ما بعد تنكره على شكل كيان موثوق به، حيث يصل للضحية بريد إلكتروني أو رسالة نصية تحفزه على النقر فوق ارتباط ضار، وحالما يستجيب المستلم وينقر على الرابط يتم تثبيت برامج ضارة على جهازه أو تجميد النظام كجزء من هجوم برامج الفدية أو الكشف عن معلومات حساسة خاصة بالمستلم.يمكن أن يكون لهذا النوع من الهجمات السيبرانية نتائج مدمرة بالنسبة للأفراد، أما بالنسبة للمنظمات فغالباً ما يتم استخدام التصيد الاحتيالي للحصول على موطئ قدم في شبكات المنظمة أو الشبكات الحكومية كجزء من هجوم أكبر، مثل حدث التهديد المستمر المتقدم (APT)، في هذه الحالة يتم اختراق الموظفين من أجل تجاوز الحدود الأمنية الخاصة بالمنظمة، أو توزيع البرامج الضارة داخل بيئة مغلقة، أو الحصول على تصريح للوصول إلى بيانات المنظمة الحساسة المحمية. واعتماداً على نطاق هذا الهجوم من المحتمل أن تتصاعد محاولة التصيد الاحتيالي إلى حادث أمني للمنظمة يجعلها بموقف صعب قد لا تجد قدرة على التعافي منه.2. هجمات التصيد الاحتيالي بالرمح (SPEAR PHISHING)التصيد بالرمح هو عملية احتيال تتم أيضاً عبر البريد الإلكتروني أو الاتصالات الإلكترونية، وتستهدف فرداً أو منظمة أو شركة معينة. على الرغم من أن مجرمي الإنترنت يسعون غالباً إلى سرقة البيانات لأغراض ضارة،كيف يحدث هذا النوع من الهجمات السيبرانية؟تصل رسالة بريد إلكتروني للضحية وتبدو بأنها من مصدر موثوق، ولكنها بدلاً من ذلك تقود المستلم إلى موقع ويب مزيف مليء بالبرامج الضارة،على سبيل المثال، حذر مكتب التحقيقات الفيدرالي (FBI ) من عمليات التصيد بالرمح حيث كان يصل للضحايا رسائل بريد إلكتروني تبدو بأنها واردة من المركز الوطني للأطفال المفقودين والمستغلين لتبدو أنها كيان موثوق،3. هجمات تصيد الحيتان (WHALE PHISHING)تصيد الحيتان هو مصطلح يستخدم لوصف هجوم التصيد الذي يستهدف بشكل خاص الوصول إلى معلومات حساسة وسرية لشخصيات قوية من الأفراد الأثرياء أو الأقوياء أو البارزين (على سبيل المثال، إذا أصبح فرد ما ضحية لهجوم تصيد احتيالي من هذا النوع، فيمكن اعتباره "تصيداً كبيراً" أو ما يسمى،ما علاقة هذا الهجوم بهجمات التصيد الاحتيالي؟يعد صيد الحيتان في الأمن السيبراني مجموعة فرعية من هجمات التصيد الاحتيالي التي تستخدم طريقة استهداف محددة، تم إنشاؤها بواسطة مجرمي الإنترنت لانتحال شخصية عضو معين في شركة أو مؤسسة. حيث يستهدف المهاجمون الشركات المعنية لسرقة معلومات سرية أو إقناع الضحية بإرسال أموال أو بطاقات هدايا إلى المنتحل. دون إذن صريح منه. وغالباً ما تحدث هذه الهجمات عندما ينتقل المستخدم إلى صفحة ويب تم اختراقها ويتصفحها.تم تصميم هجمات Drive-by لإصابة الأجهزة أو سرقة المعلومات أو التسبب في تلف البيانات، والذي يستخدم غالباً مجموعات الاستغلال (Exploit kits) لبدء التنزيل التلقائي.ما هي Exploit kits؟ ثم يتم استخدام نقاط الضعف هذه لبدء عملية التنزيل التلقائي وتنفيذ الهجوم.5. برامج الفدية(RANSOMWARE) والذي تمكن من جعل المعلومات الحساسة للأفراد والمنظمات على المحك.في هذا النوع من الهجمات، يضطر الضحية إلى حذف جميع المعلومات الضرورية من نظامه إذا فشل في دفع فدية ضمن الجدول الزمني الذي قدمه مجرمو الإنترنت،للمزيد اقرأ، فيروس الفدية: المهاجم الأخطر للمؤسسات في العصر الرقميفي هذا النوع من الهجمات السيبرانية، إلا أن العديد من المنظمات لا تطبق الضمانات وأساليب الحماية بشكل صحيح.7. هجمات التنصت EAVESDROPPINGهجوم التنصت، هو سرقة المعلومات حيث يتم نقلها

عبر شبكة عن طريق جهاز كمبيوتر أو هاتف ذكي أو جهاز آخر متصل.كيف يمكن منع هذا النوع من الهجمات السيبرانية؟يمكن منع هجمات التنصت بعدة طرق أبرزها:استخدام جدار حماية شخصيالحفاظ على تحديث برامج مكافحة الفيروساتواستخدام شبكة افتراضية خاصة (VPN)تجنب شبكات wi-fi العامةاعتماد كلمات مرور قويةهجمات البرامج الضارة هي أي نوع من البرامج الضارة المصممة لإحداث ضرر أو تلف لجهاز كمبيوتر أو خادم أو عميل أو شبكة دون معرفة المستخدم النهائي.ينشئ المهاجمون عبر الإنترنت البرامج الضارة ويستخدمونها ويبيعونها لأسباب عديدة مختلفة، ولكن غالباً ما يتم استخدامها لسرقة المعلومات الشخصية أو المالية أو التجارية. على الرغم من اختلاف دوافعهم، يركز المهاجمون الالكترونيون دائماً تكتيكاتهم وتقنياتهم وإجراءاتهم (TTP) على الوصول إلى بيانات الاعتماد والحسابات المميزة لتنفيذ مهمتهم.9. حصان طروادة (TROJAN HORSES)وهو نوع من البرامج الضارة يتم إخفاؤه عادةً كمرفق في رسالة بريد إلكتروني أو ملف مجاني للتنزيل ، بمجرد التنزيل، سينفذ الكود الضار المهمة التي صممها المهاجم من أجلها، مثل الوصول إلى الباب الخلفي لأنظمة الشركة، أو سرقة البيانات الحساسة.تتضمن مؤشرات نشاط حصان طروادة على الجهاز نشاطاً غير عادي مثل تغيير إعدادات الكمبيوتر بشكل غير متوقع.10.هجوم man-in-the-middle هو نوع من هجمات التنصت،كيف يحدث ذلك؟!بعد تمكن المهاجمون من الدخول إلى "منتصف" النقل، يتظاهر المهاجمون بأنهم مشاركين شرعيين.يوجد العديد من الاختصارات الشائعة لهجوم man-in-the-middle منها: MITM وMitM وMiM.11.هجمات رفض الخدمة (DOS: DENIAL-OF-SERVICE) وهجمات رفض الخدمة الموزعة (DDOS: DISTRIBUTED DENIAL-OF-SERVICE)يؤدي هجوم رفض الخدمة (DoS) إلى إغراق الخادم بحركة المرور، أما هجوم رفض الخدمة الموزع (DDoS) هو هجوم DoS يستخدم أجهزة كمبيوتر أو أجهزة متعددة لإغراق مورد مستهدف.كلا النوعين من الهجمات يغمران الخادم أو تطبيق الويب بهدف مقاطعة الخدمات، فقد يتعطل، وقد تتلف البيانات، وقد يتم توجيه الموارد بشكل خاطئ أو حتى استنفادها لدرجة شل النظام.لا تعد عناوين URL مجرد عناوين للمتصفحات والخوادم لاستخدامها أثناء انتقال المستخدمين من صفحة إلى أخرى باستخدام الروابط، عندما يطلب المتصفح X من الخادم، يستجيب الخادم بـY .من الجدير بالذكر أنه لا يوجد ما يمنع المستخدمين من إدخال "أوامر" أخرى في شريط المتصفح لمعرفة ما سيعيده الخادم لهم.يمكن للمتسلل من خلال التلاعب بأجزاء معينة من عنوان URL التحول لصفحات الويب التي لا يُفترض أن يكون لديه إمكانية الوصول إليها. يعد التلاعب في عنوان URL أحد أسهل الهجمات التي يتم إجراؤها، والذي يمكن أن يتم تنفيذها بواسطة مستخدمين فضوليين ببراءة أو متسللين يبحثون عن نقاط الضعف.13. DNS TUNNELINGهو هجوم يصعب اكتشافه يقوم بتوجيه طلبات DNS إلى خادم المهاجم، يعمل نفق DNS على ترميز رسائل الأوامر والتحكم (C&C) أو كميات صغيرة من البيانات إلى استجابات واستعلامات DNS غير واضحة. نظراً لأن رسائل DNS لا يمكن أن تحتوي إلا على كمية صغيرة من البيانات، يجب أن تكون أي أوامر صغيرة ويتم استخراج البيانات ببطء. يصعب اكتشاف هذه التقنية لأن DNS بروتوكول صاخب، مما يجعل من الصعب التمييز بين استعلام مضيف عادي وحركة مرور DNS العادية عن النشاط الضار.14.اختطاف الجلسة SESSION HIJACKINGيعمل هجوم Session Hijacking على استغلال آلية التحكم في جلسة الويب،بمجرد الوصول إلى معرف جلسة المستخدم، يمكن للمهاجم أن يتنكر مثل هذا المستخدم ويفعل أي شيء مخول للمستخدم القيام به على الشبكة.15.القوة الغاشمة (BRUTE FORCE)يعل المهاجمون في هذا النوع من الهجمات السيبرانية على تجربة مجموعات مختلفة من أسماء المستخدمين وكلمات المرور حتى يعثروا على واحدة تعمل، سيكون القبض عليهم أكثر صعوبة.16.هجمات البرمجة النصية عبر المواقع (CROSS-SITE SCRIPTING)هجمات البرمجة النصية عبر المواقع (XSS) هي نوع من الحقن،تحدث هجمات XSS عندما يستخدم المهاجم تطبيق ويب لإرسال تعليمات برمجية ضارة، بشكل عام في شكل نص برمجي من جانب المستعرض، إلى مستخدم نهائي مختلف. لا بد من العمل بشكل دائم على اكتشاف العيوب التي قد تسمح لهذه الهجمات بالنجاح، حيث أنه من الممكن أن تحدث في أي مكان يستخدم فيه تطبيق الويب مدخلات من المستخدم ويعمل على معالجتها وتوليد المخرجات بشكل مباشر لها دون التحقق من صحتها أو تشفيرها.17.حقن SQL (SQL INJECTION)يتكون هجوم حقن SQL من إدخال أو "حقن" استعلام SQL عبر حقول الإدخال من العميل إلى التطبيق من أجل التأثير على تنفيذ أوامر SQL المحددة مسبقاً. وتعديل بيانات قاعدة البيانات من (إدراج / تحديث / حذف)، وتنفيذ عمليات الإدارة على قاعدة البيانات (مثل إيقاف تشغيل (DBMS ، واستعادة محتوى ملف معين موجود في DBMS وفي بعض الحالات إصدار أوامر لنظام التشغيل.18.التهديدات من الداخلتحدث العديد من أنواع الهجمات السيبرانية يومياً، ويتم ذلك من خلال تزويد أولئك المجرمين

بكل المعلومات الضرورية للولوج، مما يؤدي إلى عواقب كارثية على المنظمة.تعتبر التهديدات من الداخل أحد التهديدات الشائعة للهجمات السيبرانية على البنوك والمؤسسات المالية.19.هجمات الذكاء الاصطناعيركز التعلم الآلي على تعليم الكمبيوتر لأداء عدة مهام بمفرده بدلاً من الاعتماد على البشر في إجرائها يدوياً. لاختراق الأنظمة الرقمية للحصول على معلومات غير مصرح بها،هجمات عيد الميلاد (BIRTHDAY ATTACKS)هجمات عيد الميلاد هي من أنواع القوة الغاشمة من الهجمات السيبرانية التي تهدف إلى تشويه الاتصال بين العملاء ومختلف الأفراد في الشركة بدءاً من المدير التنفيذي وانتهاءً بموظفيها.تعتمد الطريقة على نظرية عيد الميلاد التي من خلالها تكون فرصة مشاركة شخصين في عيد ميلاد واحد أعلى بكثير مما تبدو عليه. وبنفس الطريقة، فإن فرصة اكتشاف التعارضات أعلى أيضاً ضمن وظيفة التجزئة المستهدفة، وبالتالي تمكن المهاجم من العثور على أجزاء مماثلة من خلال استخدام عدد قليل من التكرارات.