الإسم :- جاستين ايهاب

الصف :- العاشر( ب )

المادة :- حاسوب

اليوم :- الثلاثاء

التاريخ :- 2023/3/28

**س:- عدد أهم أنواع الهجمات الإلكترونية(السيبرانية) مع توضيح بسيط لكل منها ؟**

**ج:- 7 انواع من الهجمات الالكترونية ( الهجمات السيبرانية)**

1. **البرامج الضارة (Malware)**
2. **التصيد (Phishing)**
3. **حجب الخدمات (Denial Of Service)**
4. **الرجل في المنتصف (Man in the middle)**
5. **التعدين الخبيث (Cryptojacking)**
6. **حقن هجوم SQL**
7. **هجمات دون انتظار (Zero-Day)**

**—--------------------------------------------------------------------------------------------------**

#### **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.**

**قد تتسبب هذه الهجمات في تعطيل جهاز الكمبيوتر او الشبكة ، او تمكن المهاجم من الوصول حتى يتمكن من التحكم في النظام عن بعد.**

#### **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.الكثي من رسائل البريد الإلكتروني المتصيدة تكون بدائية الى حد ما ويتم إرسالها الى الالاف من الضحايا المحتملين ، ولكن بعض رسائل البريد الإلكتروني يتم صياغتها وإرسالها بشكل خاص الى افراد مستهدفين ذوي قيمة لمحاولة الوصول على معلومات مفيدة منهم.**

#### **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 . كثيرا ما يتم شراء وبيع تقنيات استغلال الثغرات هذه على الانترنت المظلم (Dark Web) واحيانا يتم اكتشافها من خلال الوكالات الحكومية التي قد تستخدمها لأغراض الاختراق بدلا من إصدار معلومات عامة لأجل المنفعة المشتركة.**

**—------------------------------------------------------------------------------------------------------------------**

### **اشهر الهجمات السبرانية ( الهجمات الالكترونية )**

**الهجمات الالكترونية الأسوأ، والمثيرة للجدل، والشائكة إلى حد ما. ويرجع سبب إدراجنا لتلك الهجمات في قائمتنا إلى أنها نالت الحظ الأكبر من الاهتمام لأسباب عدة؛ حيث كانت منتشرة على نطاق واسع، ربما، أو لأنها كانت تمثل إشارات لاتجاهات كبيرة ومخيفة.**

**ودون أن نطيل عليكم، فيما يلي الهجمات الالكترونية ( الهجمات السيبرانية ) في التاريخ المعاصر:**

* **هجوم WannaCry**

[**هجوم**](https://www.it-pillars.com/ar/blog/xdata-and-sambacry/) **WannaCry هو هجوم باستخدام برامج الفدية الضارة وانتشر سريعًا في مايو 2017. ومثل كل برامج الفدية الضارة، استولى على أجهزة الكمبيوتر المخترقة وقام بتشفير المحتويات الموجودة على الأقراص الصلبة، وطلب بعد ذلك دفع فدية بعملة البيتكوين المُشفرة لفك تشفيرها. وتم تثبيت البرنامج الضار بشكل خاص في أجهزة الكمبيوتر بالمستشفيات التي تديرها هيئة الخدمات الصحية الوطنية البريطانية (NHS).**

**إلا أن هذا البرنامج الضار ليس شيئًا جديدًا. ما جعل هجوم WannaCry كبيرًا ومخيفًا، الوسائل التي استخدمها للنشر؛ فقد استغل إحدى الثغرات في Microsoft Windows واستخدم إحدى التعليمات البرمجية التي طورتها وكالة الأمن القومي الأمريكية وبشكل سري. يُطلق على أداة استغلال الثغرات هذه اسم *EternalBlue،* وقد تمت سرقتها واختراقها من إحدى المجموعات المخترقة التي تُطلق على نفسها اسم Shadow Brokers. وقامت شركة Microsoft بالفعل بتصحيح الثغرة قبلها بأسابيع قليلة، لكن لم يتم تحديث العديد من الأنظمة. كانت شركة Microsoft غاضبة لأن الحكومة الأمريكية قد طورت سلاحًا لاستغلال الثغرات بدلاً من مشاركة المعلومات بخصوص الفجوة مع مجتمع أمن المعلومات.**

* **NotPetya**

**كان هجوم Petya مجرد جزء من أجزاء البرامج الضارة عندما بدأ تداوله عبر البريد العشوائي المتصيد في 2016، وكان من بين اهم اسباب شهرته انه قام بتشفير سجل التشغيل الرئيسي في الأجهزة المخترقة ، وهو ماساعد على منع المستخدمين من الوصول الى الملفات الخاصة بهم بعد ذلك، وبشكل مفاجئ في يونيو 2017 ، بدأ انتشار نسخة اكثر خبثا من البرنامج الضار.كان مختلفا عن البرنامج الأصلي الذي تم تجاهله NotPetya;ظهر في الاساس عبر احد برامج المحاسبة الاوكرانية المخترقة ،وانتشر عبر أداة استغلال الثغرات EternalBlue ذاتها والتي استخدمها هجوم WannaCry. ويغلُب الظن أن NotPetya هو هجوم إلكتروني شنته روسيا ضد أوكرانيا، رغم أن روسيا قد أنكرت ذلك، وهو ما يفتح الباب أمام عصر محتمل من البلدان التي تستخدم البرامج الضارة كسلاح لها.**

* **Ethereum**

**قد لا يُمثل هذا النوع أهمية كبيرةً مثل بعض الأنواع الأخرى بالقائمة، لكن يستحق إلقاء نظرةً عليه هنا نظرًا للكم الهائل من مبالغ الأموال المتكبدة. Ether عملة مشفرة مثل عملة البيتكوين، وفي شهر يوليو تمت سرقة مبلغ قدره 7.4 ملايين دولارات أمريكية بعملة Ether وذلك في غضون بضع دقائق. وبعد ذلك، وبعد بضعة أسابيع فقط تمت سرقة 32 مليون دولارًا أمريكيًا. وقد أثارت الحادثة بكاملها الأسئلة بخصوص أمن العملات القائمة على تكنولوجيا البلوك تشين (blockchain).**

* **Equifax**

**إحدى وكالات التصنيف الائتماني الكبيرة أعلنت في يوليو 2017 أن مجرمون قد استغلوا ثغرةً بأحد مواقع الويب الأمريكية الخاصة بتقديم الطلبات للحصول على بعض الملفات،” وتمكنوا من الحصول على معلومات شخصية لحوالي 150 مليون شخصًا. وقد زادت النتائج المترتبة على ذلك من غضب الأشخاص، ولاسيما عندما كان موقع الويب Equifax الذي يرجع إليه الأشخاص للتحقق من حالة اختراق المعلومات، يبدو مصممًا بصورة رئيسية لبيع خدمات Equifax.**

**إيد سزوفير، الرئيس التنفيذي لشركة SenecaGlobal، أوضح أن اختراق Equifax كان سيئًا بصفة خاصة “لأن الموقع قد تم إخطاره بالحل وكان الحل يتطلب تنفيذه في أداة يُطلق عليها Apache Struts والتي كانوا يستخدمونها جيدًا قبل حتى حدوث الاختراق. ولكنهم فشلوا في القيام بذلك في الوقت المناسب. ومن أجل منع حدوث مثل تلك الاختراقات، يتطلب الأمر إجراء تغيير في الثقافة والمصادر؛ لم تكن هناك مشكلة تقنية، حيث كان الحل التقني معروفًا بالفعل. من المؤكد أن موقع Equifax كانت لديه المصادر، لكن لم تكن لديه الثقافة المناسبة للتأكد من تطبيق الإجراءات الصحيحة.”**

* **Yahoo**

**نال هذا الاختراق الكبير لنظام البريد الإلكتروني الخاص بشركة Yahoo اهتمامًا كبيرًا لأنه ورغم حدوثه منذ وقت طويل في عام 2013، لكن تداعياته، فيما يتعلق بعناوين البريد الإلكتروني الخاص بشركة Yahoo البالع عددها 3 مليار عنوان بريد إلكتروني والتي تم اختراقها، ظهرت فقط في أكتوبر 2017. وشملت المعلومات المسروقة كلمات المرور وعناوين البريد الإلكتروني المنسوخة، والمُشفرة باستخدام تقنيات غير محدثة، وسهلة الفك من حيث التشفير، وهو نوع من المعلومات يمكن أن يستخدمه المهاجمون لاختراق حسابات أخرى. وبالإضافة إلى الأضرار التي لحقت بأصحاب الحسابات، تسبب الاختراق في إعادة النظر في صفقة شراء Verizon لشركة Yahoo، حتى على الرغم أن الصفقة قد تمت بالفعل.**

**الشيء المخيف حقًا في هذا الاختراق أن ثقافة السرية التي ظلت طي الكتمان تعني أن هناك الكثير بالخارج. “لا يوجد أحد متحمس لمشاركة الاختراق، لأسباب واضحة تتعلق بالعلاقات العامة، “حسبما ورد على لسان ميتش ليبرمان، مدير الأبحاث فيG2 Crowd. “لكن تظهر الحقيقة في نهاية المطاف. ما الأشياء الأخرى التي لا نعرفها؟”**

* **GitHub**

**في 28 فبراير، 2018، تم اختراق الإصدار المتحكم في خدمة المضيف GitHub بهجوم حجب الخدمات، حيث تم إرسال بيانات بلغت 1.35 تيرابايت في الثانية إلى الموقع المشهور. ورغم أن GitHub قد تعرض فقط لعملية قطع اتصاله بالإنترنت بصورة متقطعة ورغم نجاحه في صد الهجوم كلياً بعد أقل من 20 دقيقةً، كانت الآثار الهائلة المترتبة على الاعتداء مثيرة للقلق؛ وتجاوز الهجوم الضخم على Dyn في أواخر 2016حيث بلغ الحد الأقصى للبيانات المرسلة 1.2 تيرابايت في الثانية.**

**وكانت المشكلة الأكبر تتمثل في البينة الأساسية التي ساعدت على الهجوم. كان هجوم Dyn ناجمًا عنMirai botnet، والذي تطلب وجود برنامج ضار لاختراق الآلاف من الأجهزة، لكن هجوم GitHub استغل أجهزة السيرفر التي تُشغل نظام التخزين المؤقت للذاكرة، والتي يمكنها إعادة مجموعات ضخمة للغاية من البيانات استجابةً للطلبات البسيطة.**

**تم تصميم Memcached لاستخدامه فقط مع أجهزة السيرفر المحمية التي تعمل على الشبكات الداخلية، وكوسيلة أمان بعض الشيء لمنع المهاجمين الضارين من تزييف عناوين IP وإرسال كميات كبيرة من البيانات إلى الضحايا الغافلين. ولسوء الحظ، تعتمد الآلاف من أجهزة السيرفر Memcached على الإنترنت المفتوح، وكانت هناك زيادة كبيرة في استخدامه أثناء هجمات DDoS. إن القول بأن أجهزة السيرفر “مخترقة” بالكاد يكون أمرًا معقولاً، لأنها سترسل الحزم بكل أريحية إلى أي مكان يتم مطالبتها به دون توجيه الأسئلة.**

**بعد أيام فقط على هجوم GitHub، تم شن هجوم آخر بواسطة DDoS القائم على Memecached، في أحد الشركات الأمريكية المُقدمة للخدمات ولم يتم ذكر اسمها وتم إرسال بيانات بلغت 1.7 تيرابايت في الثانية.**