صور الاستخدام غير المشروع للفضاء الإلكتروني

الباحث/ خالد محمود محمد مهران

تحت إشراف

أ.د. عصام محمد أحمد زناتي

أستاذ القانون الدولي العام- ونائب رئيس جامعة أسيوط سابقا

أ.د. ناصر محمد عثمان

أستاذ القانون الدولي الخاص- كلية الحقوق بجامعة أسيوط

(ISSN: 2537 - 0758)

صور الاستخدام غير المشروع للفضاء الإلكتروني

الباحث/ خالد محمود محمد مهران

ملخص البحث

إن التطور التكنولوجي في عالمنا الحديث بات هو الأهم على جميع الأصعدة السياسية والاقتصادية والاجتماعية والثقافية والفنية والعسكرية والتجارية والبيئية وخلافه وأصبح الإعتماد عليه بصفة رئيسية في إدارة جميع تلك المنظومات .

فأصبحت قوة الدول تقاس بتقدمها التكنولوجى وبناء عليه تقدمها في جميع المجالات وباتت المنافسة في هذا المجال من الشراسة حتى ظهرت بما يسمى الهجمات الإلكترونية، ويتطور مشهد التهديد الإلكتروني بشكل ملحوظ مع مرور السنوات. ويتفق الخبراء والمسؤولون على حدوث تغير في سرعة الهجمات وتطورها بشكل جذري.

ويوجد اختلاف حيوي آخر في تنوع تلك الهجمات حيث تهدد المخاطر الإلكترونية المزايا الاقتصادية أو السياسية أو الاجتماعية التي يمكن أن تقدمها الاختراعات البشرية في مجال الفضاء الإلكتروني.

وقد استنتجنا من البحث أنه : يتضح أن جانب كبير من الصراعات بين الدول بات ينتقل شيئا فشيئا إلى ميدان الفضاء الإلكتروني، وذلك باعتباره ساحة بديلة عن المواجهة العسكرية التقليدية، بالنظر لكون هذا الفضاء أقل كلفة، ويحرر الدولة المهاجمة من التبعات، ويضعف احتمالية توجيه الإدانة اليقينية لها بشكل مباشر.

وكذلك من توصيات البحث أنه : يجب أن تكون مهمة تأمين نظمنا المعلوماتية لا بد أن تتم من داخلنا بدون الاستعانة بأي جهة خارجية، لأننا بذلك سنسلمها كل مفاتيحنا بأنفسنا.

Abstract

The technological development in our modern world has become the most important at all political, economic, social, cultural, artistic, military, commercial, environmental and other levels, and the dependence on it has become mainly in the management of all those systems. The power of countries has become measured by their technological progress and accordingly their progress in all fields and competition in this area has become fierce until the emergence of so-called cyberattacks, and the scene of the cyber threat has evolved significantly with the passage of

years. Experts and officials agree that there has been a radical change in the speed and evolution of attacks.

Another vital difference exists in the diversity of these attacks as cyber risks threaten the economic, political or social benefits that human inventions can offer in cyberspace. We have concluded from the research that: it is clear that a large part of the conflicts between states are gradually moving to the field of cyberspace, as an alternative arena to conventional military confrontation, given that this space is less expensive, frees the attacking state from the consequences, and weakens the likelihood of a definite condemnation of.

المقدمة:

لم تعد المجالات الأربعة التي عرفت في المواجهة المسلحة التقليدية بين الدول (البر والبحر والجو والفضاء) وحدها على الساحة الدولية بل دخل مجال خامس لهذه المواجهة وهو (الفضاء الإلكترونى)، حيث من المتوقع أن تكون الهجمات الالكترونية (Cyber attack) والحرب الإلكترونية (Cyber War) السمة الغالبة إن لم تكن الرئيسية للحروب المستقبلية في القرن الواحد والعشرين، وتكمن خطورة هجمات وحروب الإنترنت والشبكات في كون العالم أصبح يعتمد أكثر فأكثر على الفضاء الإلكترونى (Cyberspace) لا سيما في البنى التحتية المعلوماتية العسكرية والمصرفية والحكومية إضافة إلى المؤسسات والشركات العامة والخاصة، ولا شك أن إزدياد الهجمات الإلكترونية يرتبط أيضا بإزدياد هذا الإعتماد على شبكاتّ الكمبيوتر والإنترنت في البنية التحتية الوطنية الأساسية، وهو ما يعني إمكانية تطور الهجمات الإلكترونية اليوم لتصبح سلاحا حاسما في النزاعات بين الدول في المستقبل وكذلك وسيلة فعالة لزعزعة الإستقرار داخل الدول والحصول على المعلومات والسيطرة على الإقتصاد او احداث شلل لمرافق الدول حيث ان غالبية الدول توجهت الى التحول الرقمي(١).

ومع دخول عصر حروب الفضاء الإلكتروني، فإن العقيدة العسكرية تغيرت عن الذي كان سائدا في الحروب التقليدية، وتحولت إلى عقيدة جديدة مفادها أن الفضاء الإلكترونى أصبح يمثل ساحة المعركة الجديدة وميدانها، وأن من يسيطر على هذا الفضاء يسيطر على سير المعارك على الأرض وفي الجو، ويستطيع حسم المعركة لصالحه ومن ثم الإنتصار في الحرب؛ فحروب الفضاء الإلكتروني تكون عبر الدخول في الشبكات الإلكترونية والسيطرة عليها أو تدميرها، ما يعني شل قدرات الدولة ونشاطها

(ISSN: 2537 - 0758)

وتعطيل عمل مؤسساتها. إن هجمات الفضاء الإلكتروني غيرت بالفعل طبيعة الحرب ذاتها، وأخرجتها من النمط التقليدي إلى نمط آخر جديد؛ وذلك نتيجة لاختلاف ميدان المعركة والأدوات المستخدمة، والأهداف المراد تحقيقها والنتائج المترتبة عليها، بالمقارنة مع الحروب التقليدية؛ إذ لا تستهدف الحروب الإلكترونية في غاياتها تدمير الآلات والمعدات العسكرية والبشرية للعدو، ولا يدخل في أجندتها الإستيلاء على أرض العدو وإحتلالها، وإنما يكون مسرحها هو الفضاء الشبكي، والأهداف فيها تكون برامجية[٢].

وبذلك فهي قد أسهمت هذه المتغيرات في عقيدة الدول وأصبح فرض على الدول البحث عن إستراتيجيات مواجهة الهجمات الإلكترونية ، من قبيل تطوير وسائل تقنية دفاعية، مثل تطوير أنظمة إنذار مبكر ضد الهجمات، وتطوير برامج الحماية والتصدي. وكان في مقدمة الإجراءات أيضا قيام عدد من الدول بتأسيس جيوش ووحدات عسكرية سيبرانية خاصة بهدف تعزيز قدراتها الدفاعية في الفضاء السيبرانى ، وتزويدها بالكوادر المدربة، وتدعيم قدراتها بأحدث تقنيات المواجهة في الفضاء السيبراني، وفي سبيل ذلك عمدت إلى تجنيد محترفي القرصنة والبرمجة في وحدات قتالية خاصة ضمن صفوف القوات المسلحة.

أهمية البحث :

لم تعد الحروب بين الدول مقتصرة على إستخدام القوة العسكرية في الهجوم المباشر على المواقع المادية لتدمير الحصون و الجيوش المعادية، فمثلما تطورت الوسائل العسكرية من السيوف و الدروع إلى الطائرات و الصواريخ نتيجة لتغير الزمن و التقدم التكنولوجي.

حدث نفس التطور مؤخرا ولكن على مستوى آخر؛ نتيجة لظهور شبكة الإنترنت، و تحول نظم الإدارة الصناعة والمعلومات في معظم دول العالم من النظام الورقي المكتبي الأرشيفي إلى الأنظمة المعلوماتية على شبكات الكمبيوتر، فظهر مفهوم الهجمات الإلكترونية .. ثم الحروب الإلكترونية إلى الوجود.

إن الهجمات الإلكترونية ربما يقوم بها أفراد كمجموعات الهاكرز و ربما تقوم بها دول حيث تسمى بالحرب الإلكترونية.

منهج الدراسة :

سوف يتبع الباحث المنهج الوصفي من خلال وصف وتوضيح الفكرة الخاصة بموضوع البحث .

خطة البحث :

تتكون خطة البحث من مبحثين كالتالي:

المبحث الأول : الهجمات الإلكترونية غير المشروعة
المبحث الثاني : فيروسات الكمبيوتر وأنواع الهجمات السيبرانية

المبحث الأول
الهجمات الإلكترونية غير المشروعة

تمهيد وتقسيم :

إن التطور التكنولوجى في عالمنا الحديث بات هو الأهم على جميع الأصعدة السياسية والإقتصادية والإجتماعية والثقافية والفنية والعسكرية والتجارية والبيئية وخلافه وأصبح الاعتماد عليه بصفة رئيسية في إدارة جميع تلك المنظومات، فأصبحت قوة الدول تقاس بتقدمها التكنولوجى وبناء عليه تقدمها في جميع المجالات .

وباتت المنافسة في هذا المجال من الشراسة حتى ظهرت بما يسمى الهجمات الإلكترونية، ويتطور مشهد التهديد الإلكتروني بشكل ملحوظ مع مرور السنوات. ويتفق الخبراء والمسؤولون على حدوث تغير في سرعة الهجمات وتطورها بشكل جذري.

ويوجد اختلاف حيوي آخر في تنوع تلك الهجمات حيث تهدد المخاطر الإلكترونية المزايا الاقتصادية أو السياسية أو الاجتماعية التي يمكن أن تقدمها الاختراعات البشرية في مجال الفضاء الإلكتروني .

وسوف نتناول هذا المبحث من خلال المطلبين الآتيين :

المطلب الأول : الهجمات الإلكترونية على المسرح العالمي
المطلب الثاني : مفهوم الهجمات الالكترونية

المطلب الأول
الهجمات الإلكترونية على المسرح العالمي

تنظر العديد من الدول حاليًا إلى القدرات الإلكترونية بوصفها جزءًا مشروعًا وضروريًا من أدواتها الاستراتيجية بالإضافة إلى البراعة الدبلوماسية والمكانة الاقتصادية والقدرة العسكرية، وهذا يثير المخاوف حول ما إذا كنا قد نشهد في المستقبل القريب حربًا كاملة يدور رحاها في الفضاء الإلكتروني بين الدول. بالإضافة إلى ذلك، نلحظ وجود اهتمام في بعض الأحيان بالاستعانة بالقدرات الإلكترونية لجهات فاعلة غير حكومية – في الوقت الحالي دون أدلة تذكر على استخدامها الفعلي.

حقائق هامة حول الهجمات الإلكترونية :

- تشير التقديرات إلى أن القطاعات التجارية تتكبد ما يزيد عن 400 مليار دولار أمريكي سنويا كخسائر مادية نتيجة الهجمات الإلكترونية.

(ISSN: 2537 - 0758)

- يتراوح عدد الحوادث المتعلقة بالأمن الإلكتروني ما بين 90 – 80 مليون حادثة سنويا.
- ٢٠% من الشركات الصغيرة والمتوسطة تعرضت لجرائم إلكترونية مختلفة.
- ترصد شركة مايكروسوفت يوميا أكثر من 10 مليون محاولة لمهاجمة خدماتها المختلفة .
- عام ٢٠١٦، كان قطاع الرعاية الصحية هو الأكثر تعرضا لهجمات القراصنة.
- ٤٠% من ضحايا الجرائم الإلكترونية تعرضوا لعمليات احتيال مرتبطة ببطاقات الائتمان بأنواعها المختلفة(٣).
- كمعدل فإن مجرمي الإنترنت لديهم حوالي 200 يوم قبل أن يتم اكتشاف هجماتهم
- ٧٠% من الهجمات الإلكترونية لا يتم اكتشافها ويبقى فاعلوها مجهولين.
- الشبكات الاجتماعية المختلفة تعتبر الهدف المفضل بالنسبة للقراصنة لمهاجمة الضحايا.

وتعتمد بعض محاولات التصيّد الإلكتروني الموجّهة على إنشاء عنوان بريد إلكتروني لموظف وهمي في المؤسسة واستخدامه لطلب معلومات عن الشركة من موظفين آخرين في المؤسسة، وعندها لن يتردد الموظفون في إرسال هذه المعلومات ظن أحد منهم بأن مصدر الرسالة هو زميل لهم في المؤسسة.

وهناك نوع سائد من الهجمات الإلكترونية تعرف ب (watering hole)، ويقوم المخترقون في هذه الحالة بوضع برمجية خبيثة ضمن الكود البرمجي المستخدم في أحد مواقع الإنترنت المنتشرة على نطاق واسع، وفي حال قام أحد الموظفين بفتح هذا الموقع من كمبيوتر الشركة فستكون شبكة الشركة بأكملها عرضة للخطر الذي تحمله البرمجية الخبيثة.

والهجمات الإلكترونية على الشركات الصغيرة والمتوسطة تعود إلى 3 عوامل رئيسية، أولها افتقار الشركات الصغيرة والمتوسطة إلى الحماية، إذ لا تطبق معظم هذه الشركات معايير مناسبة للحماية من الهجمات الإلكترونية، ثم إن غالبية هذه الشركات لا تنوي زيادة استثماراتها في حلول الحماية الأمنية رغم ازدياد الهجمات الإلكترونية التي تستهدفها.

رصدت شركة ديل خلال عام 2014 حوالي 37 مليون برمجية خبيثة، وهي تقريبا ضعف كمية البرمجيات الخبيثة التي تم الكشف عنها في عام 2013 ، وإذا ما وصلت هذه البرمجيات إلى أحد مواقع الإنترنت فبإمكانها إلحاق الأذى بكافة الشركات، سواء

كانت كبيرة أو متوسطة أو صغيرة. وإذا أخذ بعين الاعتبار ضعف مستويات الحماية المتوفرة في الشركات الصغيرة والمتوسطة فإنها ستكون الأكثر تأثرا بتلك الهجمات.

ومن العوامل الرئيسية للهجمات الإلكترونية هو أن الشركات الصغيرة والمتوسطة هي بوابة عبور لشركات أكبر، وقد حصلت في السابق هجمات كبيرة على مؤسسات كبيرة انطلاقا من الشركات الصغيرة والمتوسطة التي تم اختراقها، ومن أبرزها الهجمة الشهيرة التي حصلت في الولايات المتحدة على منافذبيع شركة Target والتي تم من خلالها شن هجوم أوسع على مزوّد الخدمة لهذه الشركة وتسريب بيانات بطاقات الاعتماد لأكثر من 40 مليون عميل.

وبهذه المناسبة، قال مارك مورلاند، المدير الإقليمي لشركة SecureWorks (التابعة لشركة ديل) لمنطقة الشرق الأوسط" :تسبب الاختراقات الأمنية للمؤسسات الصغيرة والمتوسطة خسائر بالغة.

وفي ظل عدم وجود نسخة احتياطية عن البيانات فستكون لهذه الهجمات عواقب وخيمة على سمعة الشركة وسير العمليات فيها، أضف إلى ذلك الأضرار المرتبطة بإمكانية ضياع أو فقدان أحد الأجهزة التي يستخدمها موظفو هذه الشركات."[٤]

والمهاجم هو شخص أو عملية تحاول الوصول إلى البيانات أو الوظائف أو المناطق المحظورة الأخرى في النظام دون الحصول على إذن، ويحتمل أن يكون ذلك بقصد ضار[٥].

ويمكن أن تكون الهجمات الإلكترونية جزءًا من الحرب الإلكترونية أو الإرهاب الإلكتروني.

يمكن استخدام الهجوم الإلكتروني من قِبل دول ذات سيادة أو أفراد أو مجموعات أو مجتمع أو منظمات أو حتى عصابات، وقد تنشأ هذه الهجمات الإلكترونية (لسيبرانية) من مصدر مجهول. وقد يسرق الهجوم الإلكتروني هدفًا محددًا أو يغيره أو يدمره عن طريق اختراق نظام حساس .[٦]

ويمكن أن تتراوح الهجمات الإلكترونية بين تثبيت برامج التجسس على جهاز كمبيوتر شخصي ومحاولة تدمير البنية التحتية لدول بأكملها. ويسعى الخبراء القانونيون إلى قصر استخدام المصطلح على الحوادث التي تسبب أضرارًا جسدية، وتمييزه عن خروقات واختراقات البيانات الروتينية، وأنشطة القرصنة الأوسع نطاقًا.[٧]

أصبحت الهجمات الإلكترونية معقدة وخطيرة على نحو متزايد[٨]، منذ أواخر الثمانينيات من القرن الماضي، تطورت الهجمات الإلكترونية عدة مرات لاستخدام الابتكارات في تكنولوجيا المعلومات كمتجهات لارتكاب جرائم الانترنت.

(ISSN: 2537 - 0758)

وفي السنوات الأخيرة، ازداد حجم وقوة الهجمات السيبرانية بشكل سريع، كما لاحظ المنتدى الاقتصادي العالمي في تقريره لعام ٢٠١٨" :القدرات السيبرانية الهجومية تتطور بسرعة أكبر من قدرتنا على التعامل مع الحوادث العدائية"[٩].

ويوجد بعض الإجراءات التي يمكن اتباعها لتعزيز حماية الشركات الصغيرة والمتوسطة وكذا الشبكات من محاولات الاختراق ومن الأضرار الناجمة عن ضياع أو فقدان أحد الأجهزة التي يستخدمها موظفو هذه الشركات. او تعطل او حجب الخدمة او الإختراق بالنسبة للشبكات.

ومن أبرز هذه الإجراءات تشفير البيانات، فقد بات من الممكن اليوم استخدام هذه الطريقة لحماية البيانات بغض النظر عن مكان وجودها، سواء كانت على الكمبيوتر المكتبي أو الجوال أو وسائط التخزين المحمولة أو في السحاب، ودون أن يشعر المستخدم بوجود إجراءات أمنية مزعجة تعرقل سير العمل. ومن الإجراءات أيضا تقنيات المصادقة أو التعرّف المتقدمة والتي تجمع عدّة نماذج للتعرّف على المستخدمين والمصادقة على صلاحياتهم معا، وذلك للتأكد من هوية المستخدمين الذين يحاولون الوصول إلى تلك البيانات.

كما ينبغي احتواء الهجمات، ووقف البرمجيات الخبيثة التي تصيب أنظمة الشركات والشبكات والبنية التحتية ومنعها من الانتشار. وتقوم برامج الاحتواء بتوجيه المستخدمين لتشغيل التطبيقات المستهدفة في بيئات افتراضية لضمان حمايتها، ففي هذه الحالة إذا زار المستخدم إحدى الصفحات التي تحتوي على برمجية خبيثة فإن هذه البرمجية لن تتمكن من العمل وإلحاق الأذى بجهاز المستخدم[١٠].

المطلب الثاني

مفهوم الهجمات الالكترونية

ما المقصود بالهجمات الإلكترونية (الهجمات السيبرانية):

خلال السنوات الماضية واجه امن الحاسوب صعوبات شديدة بداية من سرقة البنوك ووصولا الى الهجمات شبه المفتوحة (Semi–Open Attacks).

هناك العديد من التعريفات وردت فى شأن الهجمات الإلكترونية نسردها فيما يلى :

<u>تعريف الهجمات الالكترونية (الهجمات السيبرانية) :</u>

بعبارات بسيطة الهجمات الالكترونية عبارة عن هجوم يتم شنه من أحد أجهزة الكمبيوتر او مجموعة من الأجهزة على جهاز كمبيوتر اخر او عدة أجهزة كمبيوتر او شبكات.

ويمكن تقسيم الهجمات الالكترونية الى نوعين رئيسيين: هجمات يكمن الهدف من ورائها الى تعطيل جهاز الكمبيوتر المستهدف. هجمات يكون الغرض منها الوصول الى بيانات جهاز الكمبيوتر المستهدف وربما الحصول على امتيازات المسئول عنه.

ويرى اتجاه آخر أن الهجوم الإلكتروني (سايبر اتاك) أو الهجمات السيبرانية : عبارة عن اختراق عالمي لأنظمة الكمبيوتر، والشبكات، والشركات التي تعتمد على التكنولوجيا. تستخدم تلك الهجمات تعليمات برمجية ضارة لتعديل شفرة أجهزة الكمبيوتر أو البيانات او الأرقام. ويُفضي ذلك إلى نتائج مُدمِّرة يمكن أن تتسبب في الإضرار بالبيانات الخاصة بك وانتشار جرائم الفضاء الإلكتروني مثل سرقة المعلومات والهوية كما يُعرف الهجوم الإلكتروني أو السيبراني بالهجوم باستخدام شبكة الكمبيوتر (CNA).

وهناك اتجاه يرى أن الهجوم السيبراني: هو هجوم إلكتروني بواسطة أجهزة الكمبيوتر عبر شبكات الانترنت والاتصالات الرقمية بهدف تغيير أو تعطيل برامج أو تدمير معطيات أو سرقة معلومات أو اختراق انظمة التحكم والاوامر بهدف احداث اضرار في انظمة وبرامج واجهزة الطرف الاخر وتعطيلها عن العمل. وعموما الهجوم السيبراني أو "الهجوم الإلكتروني" هو أي نوع من الهجوم الاليكتروني الذي تستهدف أنظمة معلومات الكمبيوتر أو البنية التحتية أو شبكات الكمبيوتر أو الأجهزة الالكترونية الرقمية للطرف الآخر بنية الإضرار به(١١).

ويرى اتجاه آخر أن الهجوم السيبراني: أي هجوم هو يعتبر محاولة لفضح أو تغيير أو تعطيل أو تدمير أو سرقة أو الحصول على وصول غير مصرح به أو استخدام غير مصرح به للأصول (١٢).أو هو أي نوع من المناورة الهجومية التي تستهدف أنظمة معلومات الكمبيوتر أو البنية التحتية أو شبكات الكمبيوتر أو أجهزة الكمبيوتر الشخصية.

وفي شهر مايو من عام ٢٠٠٠، عرّفت فرقة هندسة الإنترنت للهجوم في RFC 2828: على إنه الإعتداء على أمن النظام ينبع من تهديد ذكي، وعليه فإن أي فعل ذكي يمثل محاولة متعمدة (خاصة بمعنى الأسلوب أو الممارسة) للتهرب من خدمات الأمن وانتهاك سياسة الأمان الخاصة بالنظام.

تعريف CNSS رقم 4009 بتاريخ يوم ٢٦ بشهر أبريل في عام ٢٠١٠ من قبل لجنة أنظمة الأمن القومي بالولايات المتحدة الأمريكية [١] يُعرّف الهجوم بأنه: أي نوع من النشاط الضار الذي يحاول جمع أو تعطيل أو رفض أو تدهور أو تدمير موارد نظام المعلومات أو المعلومات نفسها:

(ISSN: 2537 - 0758)

الهجوم السيبراني، يعبر الفضاء الإلكتروني، ويستهدف استخدام مؤسسة ما للفضاء الإلكتروني بغرض تعطيل بيئة/ بنية تحتية حاسوبية أو تعطيلها أو تدميرها أو التحكم فيها بشكل ضار؛ أو تدمير سلامة البيانات أو سرقة المعلومات التي تمت السيطرة عليها.

أدى الاعتماد المتزايد للمجتمع الحديث على شبكات المعلومات والحواسيب، سواء في القطاعين العام والخاص، بما في ذلك الجيش[١٣] [١٤][١٥] إلى مصطلحات جديدة مثل الهجوم السيبراني والحرب الإلكترونية.

معنى كلمة ومصطلح سيبراني:

كلمة السيبراني جاءت من الكلمة الانجليزية Cyber الذي يعني شبكات الانترنت وشبكات الاتصال والمعلومات وأنظمة التحكّم الرقمية، ومنها جاء مصطلح الهجوم السيبراني Cyber Attack الذي يعني الهجوم الالكتروني عبر شبكات الانترنت وغيرها من شبكات الاتصال باستخدام الحواسب والاجهزة الرقمية.

من أين تأتي التهديدات السيبرانية ":

يكون المهاجم في الغالب شخص أو مجموعة أشخاص أو منظمة ، ويمكن أن تكون الهجمات السيبرانية جزءًا من الحرب الإلكترونية بين الدول أو الإرهاب الإلكتروني. واليوم يتم استخدام الهجوم الإلكتروني من قِبل دول ذات سيادة أو أفراد أو مجموعات أو مجتمع أو منظمات أو حتى عصابات، وقد تنشأ هذه الهجمات الإلكترونية (السيبرانية) من مصدر مجهول. قد يسرق الهجوم السيبراني هدفًا محددًا أو يغيره أو يدمره عن طريق اختراق نظام حساس.

يمكن أن تتراوح الهجمات الإلكترونية بين تثبيت برامج التجسس على جهاز كمبيوتر شخصي ومحاولة تدمير البنية التحتية لدول بأكملها، يسعى الخبراء القانونيون إلى قصر استخدام المصطلح على الحوادث التي تسبب أضرارًا جسدية و بنيوية وتجهيزية، وتمييزه عن خروقات واختراقات البيانات الروتينية وأنشطة القرصنة الأوسع نطاقًا.

يمكن للمتطفلين المحترفين، سواء كانوا يعملو بمفردهم أو يعملون لدى الوكالات الحكومية أو الجيش العثور على أنظمة كمبيوتر بها نقاط ضعف تفتقر إلى برنامج الأمان المناسب.

بالتعرف على هذه الثغرات الأمنية، يمكنها أن تصيب الأنظمة برمز خبيث ثم تتحكم عن بعد في النظام أو الكمبيوترعن طريق إرسال أوامر لعرض المحتوى أو لتعطيل أجهزة الكمبيوتر الأخرى .يجب أن يكون هناك خلل في النظام موجود مسبقًا داخل الكمبيوتر لكي تكون الهجمة الإلكترونية قد تمت بالنجاح، مثل عدم وجود حماية ضد

الفيروسات أو تكوين نظام معيب لكي يعمل الرمز الفيروسي. سيقوم العديد من المتسللين المحترفين بترويج أنفسهم للإرهابيين عبر الإنترنت، حيث تحكم مجموعة جديدة من القواعد تصرفاتهم .الإرهابيون الإلكترونيون لديهم خطط متعمدة ولا تولد هجماتهم من الغضب.

ولكن أيضاً يحتاجون مثل هؤلاء إلى تطوير خططهم خطوة بخطوة والحصول على البرنامج المناسب لتنفيذ هجومهم الإلكتروني السيبراني. عادة ما يكون لديهم جداول أعمال سياسية، وتستهدف الهياكل السياسية. الإرهابيون الإلكترونيون هم قراصنة لديهم دوافع سياسية، ويمكن أن تؤثر هجماتهم على الهيكل السياسي من خلال هذا الفساد والدمار، كما أنها تستهدف المدنيين والمصالح والمنشآت المدنية كما ذكر سابقًا يهاجم الإرهابيون الإلكترونيون الأشخاص أو الممتلكات ويتسببون في أضرار كافية لتوليد الخوف وزعزعة أمن بعض الكيانات هناك عدد من التقنيات لاستخدامها في الهجمات الإلكترونية ومجموعة متنوعة من الطرق لإدارتها للأفراد أو المؤسسات على نطاق أوسع .يتم تقسيم الهجمات إلى فئتين : الهجمات النحوية والهجمات الدلالية .الهجمات النحوية واضحة .يعتبر برنامجًا ضارًا يتضمن الفيروسات والديدان وأحصنة طروادة.

أولا : الهجمات النحوية:

الفيروسات:

الفيروس هو برنامج متماثل ذاتيًا يمكنه ربط نفسه ببرنامج أو ملف آخر من أجل التكاثر، يمكن للفيروس أن يختبئ في أماكن غير محتملة في ذاكرة نظام الكمبيوتر ويربط نفسه بأي ملف يراه مناسبًا لتنفيذ التعليمات البرمجية الخاصة به و يمكنه أيضًا تغيير بصمته الرقمية في كل مرة يتكرر فيها مما يجعل من الصعب تعقبه في جهاز الكمبيوتر.

الديدان:

الدودة لا تحتاج إلى ملف أو برنامج آخر لنسخ نفسها ؛ إنه برنامج تشغيل قائم بذاته .يعمل النسخ المتماثل للديدان عبر شبكة باستخدام البروتوكولات، يستخدم التجسد الأخير للديدان نقاط الضعف المعروفة في الأنظمة لاختراق شفرة الشفرة وتنفيذها وتكرارها في التي أصابت Code Red II الأنظمة الأخرى مثل دودة أكثر من 259000 نظام في أقل من 14 ساعة20 . على نطاق أوسع بكثير، يمكن تصميم الديدان للتجسس الصناعي لمراقبة وتجميع أنشطة الخادم وحركة المرور ثم إعادة إرسالها إلى منشئها.

(ISSN: 2537 - 0758)

أحصنة طروادة:

تم تصميم حصان طروادة لأداء مهام مشروعة ولكن يؤدي أيضًا نشاطًا غير معروف وغير مرغوب فيه أنشطة ضارة .(يمكن أن يكون حصان طروادة هو أساس العديد من الفيروسات والديدان التي يتم تثبيتها على جهاز الكمبيوتر مثل أجهزة تسجيل لوحة المفاتيح والبرامج الخلفية .بالمعنى التجاري)، ويمكن دمج أحصنة طروادة في الإصدارات التجريبية من البرامج ويمكنها جمع معلومات إضافية حول الهدف دون أن يعرف الشخص حدوث ذلك. من المحتمل أن يهاجم هؤلاء الثلاثة فردًا وتأسيسًا من خلال رسائل البريد الإلكتروني ومتصفحات الويب وعملاء الدردشة والبرامج عن بُعد والتحديثات.

الهجمات الدلالية:

الهجوم الدلالي هو تعديل ونشر المعلومات الصحيحة وغير الصحيحة. المعلومات المعدلة كان يمكن القيام بها دون استخدام أجهزة الكمبيوتر على الرغم من أنه يمكن العثور على فرص جديدة باستخدامها ولتعيين شخص ما في الاتجاه الخاطئ أو لتغطية مساراتك، يمكن استخدام نشر المعلومات غير الصحيحة(١٦).

المبحث الثاني
فيروسات الكمبيوتر وأنواع الهجمات السيبرانية

تمهيد وتقسيم :

بحسب جريدة القبس الالكترونية فيروسات الكومبيوتر هي برامج تتم كتابتها بطريقة معينة بغرض إلحاق الضرر بكمبيوتر آخر، أو السيطرة عليه،سُمّيت بالفيروسات، لأنها تشبه تلك الكائنات المتطفلة في صفتين **رئيسيتين:**

أولا : تحتاج دائما الى عائل تعيش متسترة فيه :-

فالفيروسات، دائم ا تتستر خلف ملف آخر، ولكنها تأخذ زمام السيطرة على البرنامج المصاب .بحيث أنه حين يتم تشغيل البرنامج المصاب،فإنه يتم تشغيل الفيروس أولا.

ثانيا : تستطيع ان تنسخ نفسها:

تتم كتابة هذه البرامج المؤذية بحيث تقوم بنسخ نفسها فور ا بمجرد تشغيل البرنامج المصاب .وهي تنسخ نفسها للأقراص المدمجة (CD's) الأخرى، فإذا كان الكومبيوتر مصاباً ووضعت فيه أسطوانة (CD) يتم نسخ الفيروس أوتوماتيكيا للاسطوانة، ونظر ا لهذه الخاصية في الفيروسات، تجد أن ال CD المصاب يعطيك علامة أنه ممتلئ تماما برغم عدم تخزين غير ملفات ذات حجم صغير.

وسنتناول هذا المبحث من خلال المطلبين الآتيين :
المطلب الأول: كيفية عمل الفيروسات وأنواعها
المطلب الثاني : أنواع الهجمات السيبرانية

المطلب الأول
كيفية عمل الفيروسات وانواعها

يقوم الفيروس في حالة إصابة الملف بإضافة نفسه في بداية أو نهاية الملف المصاب، دون أن يقوم فعليا بأي تغيير في مكوّنات الملف الأصلية. وعند استدعاء البرنامج فإنه يعمل بشكل طبيعي بينما يقوم الفيروس بلصق نفسه في البرنامج دون أن يغير في محتويات الملف شيء.

وطريقة اللصق تكون، إما أنه يقوم بلصق نفسه في بداية البرنامج، بحيث يتم تشغيله هو قبل البرنامج نفسه وقد تكون طريقة التحاق الفيروس بالملف بأن يضع نفسه في نهاية البرنامج المصاب ويضع علامة في بدايته، فيختبئ في نهاية الملف المصاب، ويضع في مقدّمة البرنامج مؤشّر ا بحيث أنه عندما يتم استدعاء البرنامج وتشغيله، يحوّل السيطرة للفيروس بدلا من تشغيل البرنامج ويسبب أضرار جسيمة للجهاز.

أنواع الفيروسات: هناك الآلاف من الفيروسات المنتشرة عبر الانترنت ، لكن أغلبها ما يقع تحت هذه النقاط الستة:

(١) فيروسات بدء التشغيل BOOT SECTOR VIRUS

تعتبر من أقدم الفيروسات المعروفة لدى المستخدمين حيث تستطيع ان تصيب القرص الصلب (Hard Disk) والأقراص المدمجة (CD's) وتنتشر عن طريقها من مستخدم الى اَخر وتكمن خطورة هذا النوع من الفيروسات في قدرتها على اصابة جزء أساسي من أي قرص صلب أو مدمج وهو الجزء المخصص لتوجيه الجهاز في كيفية تحميل برنامج نظام التشغيل ويقوم هذا الفيروس بتحميل نفسه للذاكرة في كل مرة يتم فيها تشغيل الجهاز[١٧] . وهذا النوع من الفيروسات يصيب قطاع الإقلاع (The boot sector) في الجهاز، وهو المكان المخصص الذي يتجه إليه الكمبيوتر في بداية تشغيل الجهاز وهذا النوع من الفيروسات قد يمنع المستخدم من الوصول إلى النظام ويمنعه من تشغيل الجهاز.

(٢) فيروس الملفات FILE VIRUS:

هذا النوع من الفيروسات يلحق نفسه كملف في أي برنامج تنفيذي و يتميز هذا النوع من الفيروسات بقدرته على الإنتشار بعدة طرق و بسرعة كبيرة منها وسائط التخزين

(ISSN: 2537 - 0758)

المختلفة Storage media والأقراص المدمجة (CD's) ورسائل البريد الإلكتروني Email messagesكملف ملحق كما يمكنه الإنتقال من البرامج المجانية و المتوفرة في الإنترنت و تكمن خطورته في قدرته على الانتشار السريع واصابة بقية الملفات الموجودة في البرامج التنفيذية الأخرى ويصيب البرامج عادة ، وينتشر بين الملفات الأخرى و البرامج الأخرى عند تشغيله.

(٣) فيروس المايكرو MIKRO VIRUS

هذا النوع أيضا سريع الانتشار بين المستخدمين خاصة أنه قادر على الانتشار بكل الطرق كوسائط التخزين المختلفة (Storage media) والأقراص المدمجة (CD's) ورسائل البريد الإلكتروني (Email messages) والبرامج المجانية وكذلك أثناء تحميل أو تنزيل البرامج من الأجهزة الخادمة(Servers) ومن الجدير بالذكر أن هذا النوع لا يصيب الا البرنامج التطبيقي التي صمم ليصيبه أساسا فمثلا لو كان هناك فيروس مصمم ليصيب برنامج تحرير الكلمات والنصوص فإنه لا يستطيع الحاق الأذى ببرنامج آخر مثل برنامج قواعد المعلومات و هكذا و لكن يستطيع أن يصيب أي ملف تم انشاؤه بواسطة البرنامج المستهدف(١٨).

وهذه الفيروسات عادة تصيب برامج الميكروسوفت أوفيس(Microsoft Office مثل الوورد Word)و الإكسل Excel و تعتبر ذات انتشار واسع جدا تقدر ب 75 %من الفيروسات الموجودة. يقوم هذا النوع من الفيروسات بتغيير بعض المستندات الموجودة في القرص الصلب و خصوصا الوورد،قد تجد بعض التصرفات الغير منطقية في بعض الأحيان مثل طلب باسوورد (Password) لفتح ملف تعرف انك لم تضع عليه باسوورد ، و أيضا تجد بعض الكلمات قد تغير مكانها و أضيفت كلمات جديدة لا علاقة لها بالموضوع . هي أساسا ليست ضارة، لكنها مزعجة نوعا ما وقد تكون مدمرة أحيانا.

(٤) فيروس متعدد الاجزاء MULTIPARTITE VIRUS

وهو الذي يقوم بإصابة الملفات مع قطاع الإقلاع (boot sector) في نفس الوقت ويكون مدمر في كثير من الأحيان إذا لم تتم الوقاية منه.

(٥) الفيروس المتطور POLYMORPHIC VIRUS

هي فيروسات متطورة نوعا ما حيث أنها تغير الشفرة كلما انتقلت من جهاز إلى آخر. نظريا يصعب على مضادات الفيروسات (Antivirals) التخلص منها لكن عمليا و مع تطور المضادات فالخطر أصبح غير مخيف.

(٦) الفيروس المختفى

تخفي نفسها بان تجعل الملف المصاب سليما و تخدع مضادات الفيروسات بان الملف سليم ليس مصاب بفيروس، مع تطور مضادات الفيروسات أصبح من السهل كشف هذا النوع [١٩].

المطلب الثاني
أنواع الهجمات السيبرانية

توجد عدة أنواع و طرق للهجوم السيبراني ، وهذه القائمة تحددها من الأقل ضررًا إلى الأكثر خطورة.

الاختراق: يستخدم هذا الهجوم لتغيير معطيات أو محو معلومات، أو هجمات الحرمان من الخدمة ... هذا النوع عموما سهل التنفيد وعادة لا يسبب الا القليل من الضرر.

التجسس: يتم هذا الهجوم باستخدام أحصنة طروادة و برامج التجسس بهدف سرقة المعلومات السرية التي لم يتم تأمينها بشكل صحيح يمكن أن يتم اعتراضها ايضا وقرصنتها.

وقف المعدات أو تخريبه: يستهدف هذا النوع من الهجوم الأنشطة العسكرية التي تستخدم أجهزة الكمبيوتر والأقمار الصناعية لتنسيق وسائل الدفاع. يمكن اعتراض الأوامر والاتصالات أو تغييرها، مما يعرض القوات للخطر.

الهجمات السيبرانية على البنى التحتية الحساسة: تهدف هذه الهجمات السيبرانية لتعطيل محطات الطاقة وتوزيع المياه وأنابيب النفط والاتصالات ووسائل النقل والمستشفيات وغيرها من البنى التحتية الحساسة للدول.

وسوف نقوم بشرح هذه الانواع بشئ من التفصيل :

هجوم التَصيُّد Drive-by : يُعتبر هجوم التصيد Drive-by طريقةً شائعةً لنشر البرامج الضارة. يبحث المهاجم الإلكتروني عن موقع ويب غير مؤمن ويقوم بزرع برنامج نصي ضار في PHP أو HTTP بإحدى الصفحات. يقوم هذا البرنامج النصي بتثبيت برنامج ضار في جهاز الكمبيوتر الذي يزور موقع الويب هذا أو يصبح IFRAME ويقوم بإعادة توجيه مستعرض الضحية إلى أحد المواقع التي يتحكم بها المهاجم. في معظم الحالات، يتم تظليل هذه البرامج النصية، ويُصعِّب ذلك من عملية تحليل الكود او الرمز التي يقوم بها الباحثون الأمنيون. تُعرف هذه الهجمات باسم Drive-by لأنها لا تتطلب أي إجراء من الضحية سوى زيارة موقع الويب المخترق، وحين يزور الضحية الموقع المخترق يهاجمه الفيروس تلقائيًا وبشكل غير ملحوظ .

(ISSN: 2537 - 0758)

ويندرج تحت مسمى هجمات التصيد ما يلي:

(أ) هجمات التَصيُّد الإلكتروني:

التَصيُّد الإلكتروني أحد أنواع الهندسة الاجتماعية المُستخدمة عادةً لسرقة بيانات مثل أرقام البطاقة الائتمانية وبيانات اعتماد تسجيل الدخول. ويحدث حين يقوم المهاجم، المنتحل صفة الشخص محل الثقة، بخداع الضحية لفتح إحدى الرسائل النصية أو البريد الإلكتروني أو الرسائل الفورية. ويتم خداع الضحية بعد ذلك لفتح رابط ضار يمكن أن يتسبب في إيقاف النظام كجزء من هجمة برنامج فدية ضار، يؤدي بدوره إلى الكشف عن معلومات حساسة، أو تثبيت برنامج ضار.

يمكن أن يترتب على هذا الاختراق نتائج كارثية، على صعيد الأفراد، يتضمن ذلك سرقة الهوية أو سرقة الأموال أو عمليات الشراء غير المُصرَّح بها. كثيرًا ما يُستخدم التَصيُّد للحصول على موطئ قدم في الشبكات الحكومية أو شبكات الشركات كجزء من خطة خداع كبيرة مثل التهديدات المستمرة المتطورة (APT). وفي مثل هذه الحالة، يتم مساومة الموظفين من اجل الحصول على إمكانية التوصل الى البيانات الهامة واختراقها ومن ثم استغلالها للحصول على المال، وكذلك نشر البرامج الضارة بإحدى البيئات المغلقة، والالتفاف حول معايير الأمان[٢٠].

(ب) هجمات التَصيُّد الاحتيالي :

التصيُّد الاحتيالي المُوجَّه عبارة عن رسالة بريد إلكتروني تستهدف أحد الأشخاص أو المؤسسات، بغرض الوصول غير المُصرَّح به إلى معلومات هامة. لا يتم تنفيذ تلك الهجمات من قبل مهاجمين عشوائيين بل على الأرجح من خلال أفراد ظهروا لأجل الحصول على أسرار تجارية أو الحصول على مكاسب مالية أو استخبارات عسكرية.

ويبدو أن مصدر رسائل البريد الإلكتروني الخاصة بالتصيُّد الاحتيالي المُوجَّه، أحد الأفراد بداخل مؤسسة مملوكة للمرسل اليه أو أحد الأشخاص الذي يعرفه الشخص المستهدف شخصيًا. في الكثير من الأحيان، يقوم نشطاء القرصنة الحاسوبية والمخترقون الممولون من جهات حكومية، بتنفيذ تلك الأنشطة، كما أن مجرمو الفضاء الإلكتروني يُنفذون تلك الهجمات بهدف إعادة بيع البيانات السرية إلى الشركات الخاصة والحكومات، يستخدم هؤلاء المهاجمون الهندسة الاجتماعية وأساليب فردية لتخصيص مواقع الويب والرسائل بطريقةٍ فَعَّالة.

(ج) هجمات تَصيُّد الحيتان :

هجوم تَصيُّد الحيتان هوأحد أنواع الهجمات السيبرانية التي تركز على موظفين بارزين مثل المسؤول المالي أو المسؤول التنفيذي الأول. ويَهدُف إلى سرقة معلومات

هامة لأن هؤلاء الذين يشغلون مناصب رفيعة بإحدى الشركات لديهم كم غير محدود من المعلومات الهامة، في معظم حالات تَصيُّد الحيتان يتم خداع الضحية لإرسال حوالات مصرفية ضخمة إلى المهاجم.

يُشير مصطلح تَصيُّد الحيتان إلى حجم الهجوم، ويتم استهداف الضحايا على أساس منصبهم الوظيفي داخل المؤسسة. توجد صعوبة كبيرة في هجمات تَصيُّد الحيتان بالمقارنة مع هجمات التَصيُّد العادية، وذلك نظرًا لأهمية استهدافهم.

في مجال الشركات، يمكن أن يقلل مسؤولو أمن الأنظمة من تأثير هذا الاختراق وذلك من خلال تشجيع موظفي الإدارة بالشركات على حضور جلسات التدريب في مجال التوعية الأمنية.

هجمات البرامج الضارة(Malware Attacks)

البرنامج الضار(Malware Attacks) عبارة عن رمزيتم إدخاله على جهاز الشخص المستهدف للتأثير بصورة سرية على نظام الكمبيوتر الخاص به دون الحصول على موافقة المستخدم، ويشمل هذا التعريف الشامل عدة أنواع محددة من البرامج الخبيثة (البرامج الضارة) مثل برامج التجسس، وبرامج الفدية الضارة، والأمر ، والتحكم.

تورطت العديد من المؤسسات التجارية المعروفة، والمدن، والعناصر الإجرامية في نشر البرامج الضارة وتم الكشف عنها أثناء قيامها بذلك.

تختلف البرامج الضارة (Malware Attacks) عن البرامج الأخرى من حيث قدرتها على الانتشار في جميع أنحاء الشبكة، والتسبب في حدوث تغييرات وأضرار ، والتخفي دون الكشف عنها، والاستمرار في النظام المخترق. ويمكن لهذه البرامج أن تدمر الشبكات وتُعطِّل تشغيل الماكينات داخل اي مؤسسة.

هجمات عن طريق برامج فيرس الفدية:-

تقوم برامج الفدية الضارة بحظر الوصول إلى بيانات الضحايا، وعادةً ما تُهدد بحذفها إذا لم يتم سداد قيمة الفدية، ولا يوجد ضمان بأن دفع قيمة الفدية سيمكن الضحايا من استعادة الوصول إلى البيانات، وغالبًا ما يتم نشر برامج الفدية الضارة من خلال فيروس حصان طروادة الذي يقوم بإرسال بيانات أساسية متخفيًا في صيغة ملف صالح. عندما يشن القراصنة هجو ما باستخدام فيروس" الفدية "الخبيث، يُرسلون إلى ضحاياهم بريد ا إلكترونيا يحتوي على رابط يبدو للوهلة الأول عنوان ويب غير ضار أو ملف مُرفق عبر البريد .غير أنه في حقيقة الأمر يحتوي الرابط على ملفات مضغوطة مُشفّرة، تُصعّب من اكتشاف أهدافهم الشائنة. ما إن يضغط الضحية على الملف

(ISSN: 2537 - 0758)

المُرفق، حتى يُصاب حاسوبه بالفيروس الخبيث. وحينها يتم تشفير الملفات والمجلدات ومحركات الأقراص على جهازه، والأخطر من هذا هو" عدم اكتشاف المُستخدمين تعرّض أجهزتهم للاختراق، وأنه لم يعد بإمكانهم الوصول إلى بياناتهم، سوى بعد إرسال القراصنة رسالة تُعلِمهم بأمر الهجوم وتُطالبهم بدفع فِدية مقابل فكّ التشفير"، بحسب مكتب التحقيقات الفيدرالي تنطوي الرسائل التي يتلقّاها الضحايا على إرشادات لطريقة دفع الفدية .وعادة ما يطلب الهاكرز الدفع باستخدام عملة" بيتكوين "الافتراضية.

وكانت شركة مايكروسوفت اكتشفت ثغرة مُحتملة في خوادمها، مكّن فيروس" الفدية " وفيروسات خبيثة أخرى من التوغّل بداخل شبكاتها. في فبراير 2017 ، تعرّضت مستشفى في لوس أنجلوس لهجوم مماثل، اضطرت على إثره دفع 17 ألف دولار بعُملة بيتكوين.

برامج حصان طروادة:

طروادة هو برنامج ضار يتخفى ويظهر في صورة برنامج مفيد. ينتشر عن طريق التمويه ومشابهته للبرامج العادية وإقناع الضحية بتثبيته. تُعتبر برامج حصان طروادة أحد أخطر أنواع البرامج الضارة، لأنها مُصممة في الكثير من الأحيان لسرقة المعلومات المالية.

١ – هجمات الويب (هجمات شبكة الانترنت)

حقن هجوم SQL (Structured Query Language):

حقن هجوم SQL، والمعروفة كذلك باسم SQL، أحد أنواع الهجمات السيبرانية التي تقوم بنشر كود ضار لاختراق قواعد البيانات الخلفية بغرض الوصول إلى المعلومات التي من المقصود اخفاءها ، وقد يشمل ذلك عدة عناصر بما في ذلك تفاصيل العملاء الخاصة، أو قوائم المستخدمين، أوالبيانات الهامة الخاصة بإحدى الشركات، يمكن أن يكون لهجوم SQLI تأثيرات مُدمِّرة على إحدى المؤسسات التجارية، ويمكن أن يتسبب الهجوم الناجح لـ SQLI في حذف جداول كاملة، وعرض غير مُصرَّح به لقوائم المستخدمين، وفي بعض الحالات، يمكن أن يحصل المهاجم على حق وصول إداري إلى إحدى قواعد البيانات. وقد تلحق هذه الأشياء ضررًا جسيمًا بإحدى المؤسسات التجارية. عند احتساب التكلفة المحتملة لهجوم SQLI، يتعين عليك أن تفكر في فقدان ثقة العميل في حالة سرقة المعلومات الشخصية الخاصة به مثل العناوين، وتفاصيل البطاقة الائتمانية، وأرقام الهواتف ،ورغم أنه من الممكن استخدام SQLI للهجوم على أي قاعدة بيانات SQL، فكثيرًا ما يستهدف الجناة مواقع الويب[٢١].

٢- البرمجة النصية للمواقع المشتركة:-

البرمجة النصية للمواقع المشتركة هي نوع من الهجمات السيبرانية حيث يقوم المهاجم بإرسال برامج نصية ضارة إلى المحتوى من إحدى مواقع الويب الأخرى الموثوق بها. ويحدث ذلك عند السماح لأحد المصادر المشكوك فيها بإرفاق الكود او الرمز الخاص بها في تطبيقات الويب، ومن ثم يتم دمج ذلك الكود مع المحتوى الديناميكي الذي يتم إرساله بعد ذلك إلى مستعرض الضحية، وعادةً ما يتم إرسال الكود في شكل أجزاء من التعليمات البرمجية Javascript التي يتم تنفيذها بواسطة مستعرض الشخص المُستهدَف، يمكن أن تشمل عمليات الاختراق برامج نصية ضارة قابلة للتنفيذ بعدة لغات ويشمل ذلك Flash، وHTML، وJava، وAjax، يمكن أن يكون لتلك الهجمات تأثيرات مدمرة، ومع ذلك، فإن التقليل من نقاط الضعف التي تُمكِّن تلك الهجمات من الحدوث يُعتبر أمرًا سهلاً نسبيًا.

الأنواع الأخرى من الهجمات السيبرانية

١- هجوم حجب الخدمات المُوزعة (DDoS) :-

يَهدُف هجوم حجب الخدمات المُوزعة (DDoS) إلى إيقاف تشغيل إحدى الشبكات أو الخدمات، وهو ما يجعلها غير قابلة للوصول إلى مستخدميها. وتُحقق الهجمات أهداف هذه المهمة من خلال تزويد الضحية المستهدفة بحركة بيانات كبيرة أو إرسال سيل من المعلومات التي تتسبب في حدوث عطل. في الحالتين، يتسبب هجوم DDoS في منع المستخدمين ذوي الأهلية مثل الموظفين، وأصحاب الحسابات، وأفراد المصدر، من تلقي الخدمات التي كانوا ينتظرون الحصول عليها.

كثيرًا تستهدف هجمات DDoS خوادم الويب الخاصة بالمؤسسات المعروفة مثل المؤسسات التجارية والحكومات، وشركات الإعلام، والتجارة والبنوك(٢٢)

ورغم أن هذه الهجمات لا تُفضي إلى فقدان أو سرقة المعلومات الهامة أو الأصول الأخرى، إلا انه يمكنها أن تُكلِّف الضحية الكثير من المال والوقت لتقليل الخطر.

٢ -هجوم كلمة المرور:

هجوم كلمة المرور يعني ببساطة محاولة فك تشفير كلمة مرور أحد المستخدمين أو الحصول عليها بنوايا إجرامية.

يمكن أن يستخدم المخترقون تطبيقات مراقبة كلمة المرور، وهجمات بتخمين كلمات القاموس، وبرامج الاختراق أثناء تنفيذ هجمات كلمة المرور. يوجد عدد قليل من آليات الحماية من هجمات كلمة المرور، لكن عادةً، يكون الحل في تطبيق أحد نُهج كلمة

(ISSN: 2537 - 0758)

المرور المتعارف عليها والتي تشمل حد أدنى للطول، وتغييرها بشكل متكرر، وكلمات مرور لا يمكن التعرف عليها.

كثيرًا ما يتم تنفيذ هجمات كلمة المرور عن طريق استرداد كلمات المرور المُخزَّنة بإحدى أنظمة الكمبيوتر أو تصدير كلمات المرور من خلالها، وعادةً ما تُنفذ عملية استرداد كلمة المرور عن طريق التخمين المتواصل لكلمة المرور من خلال خوارزمية أجهزة الكمبيوتر. يحاول جهاز الكمبيوتر تجربة عدة أرقام حتى ينجح في اكتشاف كلمة المرور.

٣- هجوم التنصت:

تبدأ هجمات التنصت باعتراض حركة بيانات الشبكة. اختراق التنصت، والمعروف أيضًا بالتطفل أو التتبع، عبارة عن هجوم على أمان الشبكة حيث يسعى أحد الأشخاص إلى سرقة المعلومات التي ترسلها أو تستقبلها الهواتف الذكية وأجهزة الكمبيوتر والأجهزة الرقمية الأخرى. يستغل هذا المخترق عمليات الإرسال عبر الشبكات غير المؤمنة للوصول إلى البيانات التي يتم إرسالها، يَصعُب اكتشاف هجوم التنصت نظرًا لأنه لا يتسبب في حدوث أي أعطال غير عادية بعمليات إرسال البيانات.

تستهدف تلك الهجمات عمليات الإرسال الضعيفة بين العميل والسيرفر والتي تُمكِّن المهاجم من الحصول على عمليات إرسال الشبكات، ويمكن أن يقوم المهاجم بتثبيت برامج عرض مثل تطبيقات المراقبة على السيرفر أو الكمبيوتر لتنفيذ هجوم التنصت واعتراض البيانات أثناء إرسالها.

أي جهاز بداخل شبكة الإرسال والاستقبال مُعرَّض للاختراق، بما في ذلك الأجهزة الطرفية وأجهزة بدء التشغيل نفسها، تتمثل إحدى الوسائل في الحماية من تلك الهجمات في معرفة الأجهزة المتصلة بإحدى الشبكات والبرامج التي يتم تشغيلها على تلك الأجهزة.

٤ - 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

٥- هجمات القوة العمياء وشبكة القاموس:

هجمات القاموس والقوة العمياء هي هجمات على الشبكات حيث يسعى المهاجم إلى تسجيل الدخول إلى حساب أحد المستخدمين من خلال التحقق بصورة نظامية ومحاولة إدخال جميع كلمات المرور المُحتملة حتى يصل إلى كلمة المرور الصحيحة.

أسهل طريقة للهجوم هي من خلال الباب الأمامي لأنك لا بد أن يكون لديك طريقة لتسجيل الدخول، إذا كانت بحوزتك بيانات الاعتماد، فمن الممكن أن يتم السماح بدخولك كمستخدم عادي دون القيام بعمليات تسجيل دخول مشكوك في صحتها، وهو ما يتطلب إدخال غير مُصحح، أو تعثر توقيعات IDS. إذا كانت لديك بيانات الاعتماد الخاصة بأحد الأنظمة، فحياتك في أمان لأن هؤلاء المهاجمون ليست لديهم هذه الرفاهيات.

يعني مصطلح القوة العمياء القدرة على السيطرة على النظام من خلال التكرار. عند اختراق كلمات المرور، تتطلب القوة العمياء برنامج قاموس يتضمن هذا البرنامج كلمات القاموس بآلاف من الخيارات المختلفة ، وهي عملية أبطأ وأقل بريقًا.

تبدأ تلك الهجمات بخطابات بسيطة مثل "أ" وبعد ذلك تنتقل إلى كلمات كاملة. يمكن أن تُنفذ هجمات القوة العمياء القائمة على برنامج قاموس، محاولات يتراوح عددها بين ١٠٠ إلى ١٠٠٠ في الدقيقة. بعد عدة ساعات أو أيام، يمكن ان تنجح هجمات القوة العمياء في اختراق أي كلمة مرور.

هجمات القوة العمياء تكرر تأكيد أهمية استخدام أفضل الممارسات لكلمة المرور، وتحديدًا في تواجد المصادر الهامة مثل أجهزة تبديل الشبكات، وأجهزة التوجيه وأجهزة السيرفر.

٦- التهديدات الداخلية:-

ليس كل هجوم على الشبكة يُنفذه شخص من خارج المؤسسة ، الهجمات الداخلية هجمات ضارة يتم تنفيذها على أحد أنظمة الكمبيوتر أو الشبكات من خلال أحد الأشخاص المُصرَّح لهم بالوصول إلى النظام، إن المنفذين لتلك الهجمات بالداخل لديهم أفضلية عن المهاجمين الخارجيين حيث أن لديهم حق وصول معتمد إلى النظام، كما أنهم قد يفهمون نُهج النظام وتصميمات الشبكات اكثر من غيرهم، وفضلاً عن ذلك، تتوفر وسائل حماية قليلة ضد الهجمات الداخلية لأن معظم المؤسسات تركز على ردع الهجمات الخارجية فالتهديدات الداخلية من الممكن أن تؤثر على جميع عناصر أمان الكمبيوتر وتتراوح بين فيروسات حصان طروادة وسرقة البيانات الهامة من إحدى

(ISSN: 2537 - 0758)

الشبكات أو الأنظمة. كما أن المهاجمون ممكن أن يؤثروا في توفر النظام من خلال التحميل الزائد لسعة معالجة الكمبيوتر أو السعة التخزينية للكمبيوتر وهوما يؤدي بدوره إلى حدوث أعطال بالنظام.

٧ – **هجمات الرجل في المنتصف (MITM):**

هجمات الرجل في المنتصف هي نوع من الهجمات الأمنية عبر الإنترنت يسمح للمهاجم باعتراض الاتصالات بين جهتين. يحدث هذا الهجوم بين اثنين من الأطراف يتواصلان مع بعضهم بصورة قانونية، ويُمكِن المهاجم من اعتراض اتصالات كان من المفترض الا يتمكن من الوصول اليها. ولذلك يُسمى "الرجل في المنتصف." "يستمع" المهاجم إلى المحادثة من خلال اعتراض عملية إرسال الرسائل التي تحمل مفتاحًا عامًا وإعادة إرسال الرسائل أثناء استبدال المفتاح المطلوب بالمفتاح الخاص به. يتواصل الطرفان على النحو المعتاد، ولا يعرفان أن مرسل الرسالة مُخترِق غير معروف يحاول تعديل الرسائل والوصول إليها قبل إرسالها إلى المستلم. ولذلك، يتحكم المخترق في الاتصالات بأكملها[٢٣].

٨ – **هجمات الذكاء الاصطناعي:**

إن مفهوم تعلم الكمبيوتر برامجه بنفسه، وبناء المعارف، وزيادة التطور، ربما يكون أمرًا مخيفًا.

ويمكن بسهولة تعريف الذكاء الاصطناعي على أنه مصطلح تكنولوجي جديد. لكنه يتم استخدامه بالفعل في جميع التطبيقات اليومية من خلال خوارزميات يُشار إليها بالتعلم الآلي. يهدُف برنامج التعلم الآلي إلى تدريب جهاز الكمبيوتر على تنفيذ مهام محددة من تلقاء نفسه. تتعلم أجهزة الكمبيوتر إنجاز المهام من خلال تكرار القيام بها وفي الوقت ذاته تعلم بعض العقبات التي قد تعرقل تقدمها.

ويمكن استخدام الذكاء الاصطناعي لاختراق عدة أنظمة بما في ذلك المركبات الذاتية والطائرات بلا طيار، وتحويلها إلى أسلحة كامنة.

وفي يناير ٢٠٢٠، حذر مكتب التحقيقات الفيدرالي من أن تقنية التزييف العميق قد وصلت بالفعل إلى النقطة التي يمكن فيها إنشاء شخصيات اصطناعية يمكنها اجتياز اختبارات القياسات الحيوية. قال مسؤول في مكتب التحقيقات الفيدرالي في ذلك الوقت، إنه بالمعدل الذي تتطور فيه الشبكات العصبية للذكاء الاصطناعي، يمكن تقويض الأمن القومي من خلال مقاطع الفيديو المزيفة عالية الدقة التي تم إنشاؤها لتقليد

الشخصيات العامة بحيث يبدو أنهم يقولون أيا كانت الكلمات التي يضعها منشئو الفيديو في صورهم. أفواه تم التلاعب بها[٢٤].

إن الذكاء الاصطناعي يساعد على أن تكون الهجمات الإلكترونية مثل سرقة الهوية، واختراق كلمة المرور، وهجمات رفض الخدمات، آليةً وأكثر قوةً وكفاءةً. كذلك يمكن استخدامها في قتل الأشخاص أو إصابتهم أو سرقة الأموال، أو إلحاق الضرر المعنوي. يمكن أيضًا تنفيذ هجمات كبيرة للتأثير على الأمن القومي، وإغلاق المستشفيات، وفصل مصادر الطاقة عن مناطق بأكملها.

الخاتمة

أولا- النتائج :

١- لا يزال من غير الواضح من هو المسؤول الحقيقي عن الهجمات كما أنه لم يتبيّن على وجه الدقة "من هم قراصنة وسطاء الظل بالرغم من أن قراصنة "وسطاء الظل "أفصحوا عن إحدى الأدوات المستخدمة في الهجوم.

٢- الهجمات التي تقوم بها الدول و المعبر عنها بالحرب الإلكترونية فإنها تكون بين دولتين، أحدهما معتدية على الأخرى، أو أنهما يتبادلان الإعتداء .

٣- تعد الحرب الإلكترونية الدائرة بين الصين و أمريكا واحدة من أكبر و أطول الحروب الإلكترونية القائمة بالعالم .

٤- مؤخرا تم الهجوم إلكترونيا على بعض المنشئات النفطية العربية، مثل شركة راس غاز في قطر عن طريق فيروس شيمون، وتوجهه أصابع الاتهام نحو إيران .

٥- العالم في خطرفي ظل الأزمة المستمرة بين روسيا وأوكرانيا حول شبه جزيرة القرم والمناطق الشرقية والجنوبية الشرقية من البلاد، بدأت سلسلة من الهجمات الروسية الإلكترونية على مواقع المنظمات والمؤسسات الأوكرانية، بما في ذلك البنوك والوزارات والصحف وشركات الكهرباء، وإستخدم المهاجمون الروس فيها برمجيات خبيثة من نوع" بيتا" وأنتهت بالحرب الروسية الأكرانية التى تحدث الآن.

٦- إحتمالية تعرض البنية التحتية المالية لضربات شديدة من الهجمات الإلكترونية لأن النظام المالي مرتبط بأنظمة الكمبيوتر وهي في الأصل عبارة عن أموال ثابتة يتم تبادلها في هذه المؤسسات.

٧- الصراع بين الدول بات ينتقل شيئا فشيئا إلى ميدان الفضاء الإلكتروني، وذلك باعتباره ساحة بديلة عن المواجهة العسكرية التقليدية، بالنظر لكون هذا الفضاء أقل كلفة، ويحرر الدولة المهاجمة من التبعات، ويضعف احتمالية توجيه الإدانة اليقينية لها بشكل مباشر.

(ISSN: 2537 - 0758)

ثانيا – التوصيات :

١- عدم الاستعانة بأي جهة خارجية للقيام بمهمة تأمين نظمنا المعلوماتية لا بد أن تتم من داخلنا ، لأننا بذلك سنسلمها كل مفاتيحنا بأنفسنا.

٢- إصدار تشريع دولي يكافح الحرب الالكترونية ، وأن ينص هذ القانون على كافة الجرائم والهجمات الالكترونية الممنهجة التي ظهرت في العصر الحديث تحت مظلة الأمم المتحدة .

٣- الانضمام الى الاتفاقيات والمعاهدات العربية والدولية التي تتعلق بمكافحة الجرائم الالكترونية بكافة أشكالها ، والتي منها ما يندرج في إطار شن الحروب النفسية، ومنها ما يمكن اعتبارها بمثابة حرب أفكار وشائعات تهدف لتأليب الرأي العام وبث الفتن وتشجيع الاضطرابات الداخلية أو تغيير مجرى العمليات الانتخابية في الدول المستهدفة.

مراجع وهوامش البحث:

(١) علي حسين باكير، المجال الخامس، الحروب الإلكترونية في القرن الـ ٢١ ، مركز الجزيرة للدراسات، ١٢ يناير، ٢٠١١ .

(٢) المجال الخامس ـ الفضاء الإلكتروني : سياسات التطوير والهيمنة العدد الخامس عشر يوليو ٢٠١٩ / دراسات مجلة المعهد المصري د. عمر حامد شكر ص ٧٩.

صلاح حيدر حروب، الفضاء الالكترونى دراسة فى مفهومها وخصائصها وسبل مواجهتها ص ٨ و٩، (دراسة خليفة ايهاب ٢٠١٨ عن الحرب الشيبانية : مراجعة العقيدة العسكرية استعدادا للمعركة القادمة).

(٣) مجلة الدراسات الدورية العدد التاسع باسم الهجمات السيبرانية الصادرة الدعم الفني للاستثمار بقطاع الاستثمار والموارد ببنك الاستثمار القومي، ص١٨.

(٤) مجلة الدراسات الدورية العدد التاسع باسم الهجمات السيبرانية الصادرة الدعم الفنى للاستثمار بقطاع الاستثمار والموارد ببنك الاستثمار القومى ص١٨ و١٩

(5) ISTQB Standard glossary of terms used in Software Testing .
مؤرشف من الأصل في ٥ نوفمبر ٢٠١٨.

(6) W., Lin, Tom C. (14 April 2016). "Financial Weapons of War ."
مؤرشف من الأصل في ٨ فبراير ٢٠٢٠.

(7) SATTER, RAPHAEL (28 March 2017). "What makes a cyberattack? Experts lobby to restrict the term
مؤرشف من الأصل في ٢٧ يوليو ٢٠١٨. اطلع عليه بتاريخ ٠٧ يوليو ٢٠١٧. المصدر : *هجوم سيبراني – ويكيبيديا*

https://ar.wikipedia.org

(8) S. Karnouskos: Stuxnet Worm Impact on Industrial Cyber-Physical System Security. In:37th Annual Conference of

the IEEE Industrial Electronics Society (IECON 2011), Melbourne, Australia, 7-10 Nov 2011. Stuxnet worm impact on industrial cyber-physical system security.

(9) World Economic Forum (2018). "The Global Risks Report 2018 13th Edition". World Economic Forum

(١٠) مجلة الدراسات الدورية العدد التاسع باسم الهجمات السيبرانية الصادرة الدعم الفنى للاستثمار بقطاع الاستثمار والموارد ببنك الاستثمار القومى ص١٨، ١٩

http://kenanaonline.com/users/tamer2011-com

http://alqabas.com/160012

https://al-ain.com/article/nhs-ransomware-cyber-attack

http://www.bbc.com/arabic/science-and-tech-39907190

http://www.elbalad.news/2760492

(11) *https://www.tathwir.com/2020/12/Cyber-Attack.html*

(12) cite_note-CNSSI4009/ #هجوم سيبراني https://ar.wikipedia.org/wiki

(13) Cortada, James W ٢٠٠٣ (ديسمبر)، The Digital Hand: How Computers Changed the Work of American Manufacturing, Transportation, and Retail Industries ،USA: Oxford University Press،٥١٢ . ص ، ISBN 978-0-19-516588-
https://openlibrary.org/books/OL7390694M/The_Digital_Hand

(14) Cortada, James W. ٢٠٠٥ (نوفمبر)، The Digital Hand: Volume II: How Computers Changed the Work of American Financial, Telecommunications, Media, and Entertainment Industries ،USA: Oxford University Press، ISBN 978-0-19-516587-6.

(15) Cortada, James W. ٢٠٠٧ (نوفمبر)، The Digital Hand, Vol 3: How Computers Changed the Work of American Public Sector Industries ،USA: Oxford University Press،٤٩٦ . ص ، ISBN 978-0-19-516586-9

(16) Janczewski, Lech, and Andrew Colarik. Cyber Warfare and Cyber Terrorism Hershey, New York: Information Science Reference, 2008. Web المصدر:
https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.670.9033&rep=rep1&type=pdf.

(١٧) مجلة الدراسات الدورية العدد التاسع باسم الهجمات السيبرانية الصادرة الدعم الفنى للاستثمار بقطاع الاستثمار والموارد ببنك الاستثمار القومى ص٤.

(١٨) مجلة الدراسات الدورية العدد التاسع باسم الهجمات السيبرانية الصادرة الدعم الفنى للاستثمار بقطاع الاستثمار والموارد ببنك الاستثمار القومى ص٥

(١٩) مجلة الدراسات الدورية العدد التاسع باسم الهجمات السيبرانية الصادرة الدعم الفنى للاستثمار بقطاع الاستثمار والموارد ببنك الاستثمار القومى ص٦

http://alqabas.com/160012

https://al-ain.com/article/nhs-ransomware-cyber-attack

http://www.bbc.com/arabic/science-and-tech-39907190

http://www.elbalad.news/2760492

(20)*https://www.tathwir.com/2020/12/Cyber-Attack.html*

(ISSN: 2537 - 0758)

(٢١) SQL هي اختصارٌ للعبارة Structured Query Language أي لغة الاستعلام البنوية، وهي اللغة المستخدمة لإجراء عمليات على قواعد البيانات، بما في ذلك إضافة أو تحديث أو حذف البيانات من قاعدة البيانات، أو لتعديل بينة قاعدة البيانات نفسها.(https://wiki.hsoub.com/SQL)

(٢٢) (1) DDOS وهي اختصار ل "Distributed Denial-of-Service Attack"، وتعني أن مجموعة من أجهزة الكمبيوتر تقوم بمهاجمة سيرفر واحد (خادم واحد) بهدف حجب الخدمة عليه.
الكثير من المواقع تحجب عن العمل بسبب هذه الهجمة " Distributed Denial-of-Service Attack"، هذه الهجمة هي من نوع "DoS attack" و تأتي من أكثر من حاسوب او مصدر في نفس الوقت. لكن ما معنى "DoS attack" ؟
هي نوع من الهجمات التي تحاول ان تجعل موارد السيرفر او الخادم غير متاحة للمستخدم. هذا يعني أنه عندما يحصل "DoS attack" يتم استهلاك "Traffic" الموقع مما يؤدي الى انقطاع الموقع عن العمل والظهور للزوار (/https://almajd.ps/news7062)

(٢٣) هجوم الرجل في المنتصف MAN IN THE MIDDLE ATTACK (MITM)
يعرف أيضاً باسم هجوم الوسيط أو هجوم رجل في الوسط؛ وهو مصطلح يصف الحالة التي يعترض فيها المخترق الاتصالَ بين طرفين؛ إما للتنصت بشكل سري على البيانات المتبادلة أو تعديلها. يستخدم المخترقون هذا النوع من الهجمات عادةً لسرقة بيانات تسجيل الدخول أو المعلومات الشخصية والتجسس على الضحية أو تخريب البيانات أو تخريب الاتصال ككل. ويستهدف بشكل أساسي مستخدمي التطبيقات المالية والخدمات السحابية ورواد مواقع التجارة الإلكترونية.
https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm

(24)https://e.paaet.edu.kw/institutes/AR/HigherInstituteOfCommunicationsAndNavigation/TechnicalSections/ComputerSection/SectionArticles/Pag