**فيروسات الحاسب الآلي**

**أحمد محمد عبد الرؤوف المنيفي**

**وكيل نيابة جبلة / اليمن**

**ahmedalmoniefy@gmail.com**

**بسم الله الرحمن الرحيم**

**مقدمة**

مع ظهور تقنية الحاسوب وانتشار أجهزة الكمبيوتر الشخصية في انحاء العالم , اصبحت المؤسسات والشركات تعتمد على الحاسب الآلي في تسيير أعمالها المختلفة , وتطورت صناعة برامج كمبيوتر لتشمل أداء مختلف الاعمال التي تزاولها الشركات والمؤسسات مثل البرامج النمطية المتعلقة بالاعمال الادارية والمحاسبية , والبرامج التي تعد حسب الطلب وتختلف باختلاف مهام الشركات وانشطتها . واصبحت الشركات والمنظمات تنفق ملايين الدولارات في اعداد قواعد البيانات الخاصة بها أو في شراء البرامج التي تلزمها لادارة اعمالها ومزاولة انشطتها. وبالرغم من أن تقنية الحاسوب قد سهلت بشكل كبير اعمال الشركات والمنظمات إلا أنه في المقابل ظهرت مخاطر كبيرة تتعلق بهذه التقنية , وكان من أهم هذه المخاطر انتشار برامج الفيروسات التي تقوم باتلاف برامج وبيانات الحاسب الآلي , وقد أدت هذه البرامج الضارة الى حدوث خسائر بملايين الدولارات للشركات وللحكومات ,.

**يتضمن البحث :**

1-شرح تقنية فيروسات الحاسب الآلي من حيث تعريفها وآليات عملها وطرق انتشارها وأشهر الفيروسات التي انتشرت في شبكات الانترنت .

2-بيان دوافع المجرمين الذين يصنعون الفيروسات والاغراض التي يهدفون الى تحقيقها من وراء هذه الصناعة .

**خطة البحث :**

يتطرق هذا المقال إلى مشكلة فيروسات الحاسب الآلي وفقا للمباحث الآتية :

**المبحث الأول :** تقنية الاتلاف : فيروسات الحاسب الآلي .

* تعريف فيروسات الحاسب الآلي
* مكونات فيروسات الحاسب الآلي
* طرق انتشار فيروسات الحاسب الآلي
* أشهر فيروسات الحاسب الآلي
* دوافع صانعي الفيروسات

والحمد لله رب العالمين على منه وتوفيقه .

**فيروسات الحاسب الآلي**

* **تعريف فيروس الحاسب :**

فيروس الحاسب هو برنامج صغير ضار ينسخ نفسه ويتكاثر كالفيروس الحقيقي ، ويقوم باتلاف و تخريب البرامج والملفات في الحاسب أو يصيب نظام الحاسب بالضرر [[1]](#footnote-1) .

يستخدم فيروس الحاسب الالي العديد من التقنيات المعروفة لأداء مهامه التخريبية ، ومع ذلك فإن تقنية نسخ الفيروس نفسه ذاتيا هي المعيار الشائع الذي يميز الفيروس عن الانواع الاخرى من برامج الكمبيوتر [[2]](#footnote-2) .

أن فيروسات الكمبيوتر ليست مدمرة بطبيعتها ، والميزة أو الخاصية الأساسية لبرنامج الكمبيوتر التي تجعله يصنف كفيروس ليست قدرته على تدمير البيانات ، ولكن قدرته على التكاثر ونسخ نفسه ذاتيا ، وقدرته على السيطرة على الكمبيوتر وتوظيف موارده بشكل كامل لنسخ الفيروس . فعند تنفيذ نسخة من الفيروس ، تصنع النسخة المنفذة نسخة أو أكثر من نفسها ، وهذه النسخ عندما تنفذ تقوم هي الأخرى بانشاء نسخ اكثر وهكذا تستمر بانشاء نسخ من نفسها إلى مالا نهايه . ليست كل برامج الكمبيوتر الضاره والمدمرة فيروسات ، لأنها لا تعمل جميعها نسخ ذاتي لنفسها ، وانما يعتبر منها فيروس فقط من يملك القدرة على نسخ نفسه ذاتيا [[3]](#footnote-3).

* **مكونات الفيروس :**

 يتكون برنامج الفيروس بوجه عام من ثلاثة اجزاء رئيسية ؛ آلية للبحث , وآلية للإصابة , وآلية لالحاق الضرر ، فآلية البحث يقوم الفيروس من خلالها بتحديد البرامج والملفات التي ينسخ نفسه إليها ، أما آلية النسخ فمن خلالها يقوم الفيروس بنسخ نفسه إلى موقع محدد في البرنامج أو الملف , وقد تتضمن آليات البحث أو النسخ وظيفة أخرى هي إخفاء الفيروس بحيث يظل مختفيا ولا ينطلق لتنفيذ مهامه التخريبية إلا في وقت وتاريخ محدد [[4]](#footnote-4) ، والآلية الثالثة في الفيروس هي آلية الضرر التي تسمى البايلود payload.

 نتناول فيما يلي هذه الأجزاء من الفيروس :

**1-آلية النسخ الذاتي :**

آلية النسخ الذاتي هي اهم جزء في الفيروس ، بل هي جزء إلزامي في كل فيروس ، فإذا كان هذا الجزء غير موجود ،فان البرنامج لا يعتبر فيروس بحسب التعريف الرسمي له ,وإنما يدخل في أي نوع آخر من البرامج الضارة غير الفيروسات .

نقوم آلية النسخ بتحديد الأهداف أو البرامج التي يهدف الفيروس إلى إصابتها ،ثم نسخ الفيروس إلى هذه البرامج [[5]](#footnote-5).

عندما ينجح الفيروس في إصابة برنامج معين يقال عن هذا البرنامج أنه مصاب بالفيروس ، والبرنامج المصاب عند تشغيله يمكنه بدوره إصابة برنامج جديد ، وهكذا ، وهذا النسخ الذاتي الموجود في الفيروس هو كما رأينا المفتاح لتحديد خاصية الفيروس[[6]](#footnote-6) .

**2- آلية الضرر : the payload routine**

آلية الضرر ( البايلود payload ) ليس جزء إلزامي في الفيروس, وإنما هي مجرد إجراء ينفذ ما يريد كاتب الفيروس أن ينفذه من أضرار وتخريب على الحواسيب المصابة . وإجراءات الضرر التي يتضمنها الفيروس يمكن تقسيمها إلى مجموعتين ؛ خبيثة وغير خبيثة . الاجراءات الضارة الخبيثة مثل ؛ حذف الملفات ، محو أو تعديل البيانات ، تخريب البرامج , إنشاء أبواب خلفية في النظام ( back doors ) ، الكشف عن البيانات السرية ... إلخ .

الاجراءات الغير خبيثة مثل ؛ اللعب بالموسيقى ، عرض صور أو رسوم متحركه على الشاشة .... إلخ

اجراءات الضرر ( البايلود payload ) يمكنها في الواقع أن تعمل أي شيء تستطيع البرمجة عمله ، لكن لا يمكنها عادة الاضرار بالمكونات المادية لجهاز الكمبيوتر ، وقد كان هذا الأمر يعتبر من الحقائق المطلقة لفترة طويلة ، ومع ذلك فإن اجهزه الحاسب الجديدة تفتح إمكانيات الاضرار حتى بالمكونات المادية للجهاز [[7]](#footnote-7).

**3-علامة الفيروس :**

 إذا تم إصابة برنامج أو ملف معين بالفيروس , يترك الفيروس علامة في الجزء الاول من البرنامج أو الملف الذي يصيبه حتى لا يعود لإصابته من جديد ، ويعمل الفيروس على التحقق من وجود هذه العلامة في الملف أو البرنامج قبل أن يهاجمه ، فإذا وجدها فإنه يتركه ويبحث عن هدف آخر ، أما إذا لم يجد العلامة فإنه يصيب الملف أو البرنامج بالعدوى وينسخ نفسه إليه [[8]](#footnote-8) .

* **تغيير طريقة تنفيذ البرنامج :**

 وإذا تم إصابة برنامج أو ملف معين بالفيروس،فان الفيروس يغير من طريقة تنفيذ هذا البرنامج أو الملف وبحيث ينفذ الفيروس أولا عند كل عملية تشغيل للملف أو البرنامج المصاب ثم ينتقل التنفيذ بعد ذلك إلى البرنامج أو الملف المصاب ، وعندما ينفذ الفيروس فإنه يقوم بأداء المهام التخريبية والحاق الضرر ، كما يقوم بإعادة نسخ نفسه من جديد عدة نسخ وإصابة ملفات وبرامج أخرى وهكذا .

* **انواع الفيروسات :**

فيروسات الكمبيوتر يمكن أن تصنف إلى عدة أنواع مختلفة , النوع الأول الأكثر شيوعا هو الفيروس الذي يصيب أي ملف أو برنامج على جهاز الحاسب الآلي .

أما النوع الرئيسي الثاني فهي الفيروسات التي تصيب ملف أو برنامج معين , وكتابة هذا الفيروس مهمة صعبة تحتاج إلى معرفة تفصيلية بتركيب وبنية الملفات داخل الحاسب الآلي , والمساحات التي يمكن أن تتموضع فيها الفيروسات داخل البرنامج الهدف[[9]](#footnote-9) .

* **طرق انتشار الفيروسات[[10]](#footnote-10) :**

لن تستطيع الفيروسات إحداث الضرر بأجهزة الحواسيب إلا إذا كانت لديها طريقة للانتقال من كمبيوتر إلى آخر , وما لم تتوفر لها هذه الطريقة فإنها سوف تظل قابعة في جهاز الكمبيوتر الذي نشأت فيه . وهناك عدد من الطرق المعروفة التي تنتقل بواسطتها الفيروسات من حاسوب إلى آخر , من أهم هذه الطرق :

1. **الوسائط القابلة للإزالة :**

الوسائط القابلة للإزالة مثل الأقراص الضوئية والفلاشات هي واحدة من الطرق الرئيسية التي تتيح للفيروسات الإنتقال من حاسب إلى آخر , ومن شخص إلى آخر . وعادة ما كانت الملفات المصابة بالفيروس تنسخ أولا إلى وسيط قابل للإزالة , وعندما يقوم المستخدم الضحية بتشغيل ملف البرنامج في الوسيط أو على الجهاز فإنه ينشط وينفذ مهامه التخريبية وينتشر داخل الجهاز . وتستمر الدائرة عندما يقوم الضحية الجديدة بنسخ الملفات والبرامج المصابة بالفيروس وينقلها -بعلم أو بدون علم - إلى اشخاص آخرين وهكذا .

1. **خوادم الملفات :**

خادم الملفات هو حاسب الي قوي يتمتع بقدرات عالية من حيث المعالج والذاكرة ومساحة الاقراص الصلبة ، وتقوم المؤسسة او الشركة بوضع كل ما تريده من بيانات ومعلومات تهم الموظفين التابعين لها، او الزبائن والعملاء، داخل هذا الخادم , وتوضع فيه برمجيات تسهل وتنظم للمستفيدين، الوصول الى قواعد البيانات والمعلومات الموجودة فيه ، وعندما يرغب احد الموظفين التابعين للمنظمة في الحصول على بيانات او معلومات معينة ، فأنه يتصل عبر جهاز حاسوبه بقواعد البيانات في الخادم server، ويحصل على المعلومات المطلوبة منه .

ويمكن أن تكون خوادم أو ملقمات الملفات الخاصة بالشركات مأوى للفيروسات , حيث يمكن لأحد الأشخاص أن ينسخ الملف المصاب بالفيروس إلى موقع محدد على الخادم أو الملقم , وبحيث ينتقل الفيروس مع كل عملية نسخ تتم من قبل الموظفين والعملاء لهذا الملف المصاب , وبعض الفيروسات يتم إعدادها خصيصا لخادم الملفات , وتقوم هذه الفيروسات بالبحث عن خادم الملفات من أجل تثبيت نسخ من نفسها فيه .

1. **البريد الإلكتروني :**

ظهور البريد الالكتروني وارتفاع شعبيته وشيوع استخدامه بين الشركات والمؤسسات والأفراد زود الفيروسات بطريقة سريعة وواسعة للإنتشار إلى كل مكان في العالم . خاصة مع تطوير الوسائل القياسية لإرسال المرفقات مع البريد الالكتروني . ويرسل الفيروس أو الملف المصاب بالفيروس إلى الضحية كمرفق مع رسالة البريد الالكتروني, وعادة ما تتضمن رسالة البريد الالكتروني التي تحمل فيروس عبارات تغري المستلم بفتح الملف المرفق بها والذي يحتوي على فيروس , مثل الفوز بجائزة أو منحة أو مساعدة , أو الوعد بالحصول على أموال أو مشاريع , أو أي شيء هام آخر يمكنه جذب وخداع المستلم , وبمجرد أن يفتح المستلم المرفقات ينشط فيروس البريد الالكتروني, وينتشر داخل الجهاز الخاص به , ثم يستولي على دفتر عناوين البريد الالكتروني الخاص بالمستلم ويرسل نسخ من نفسه إلى جميع العناوين التي حصل عليها . وبذلك ينتشر بسرعة فائقة إلى أكبر عدد من الأجهزة والحواسيب عبر العالم .

1. **التراسل الفوري :**

الرسائل الفورية هي أسلوب للتواصل بين المستخدمين عن طريق رسائل تتم بينهم في نفس اللحظة التي يكون الطرفين فيها متواجدين على الانترنت . وهي تشبه البريد الالكتروني من حيث أنها تتيح تبادل الرسائل النصية ولكن الاختلاف بينهما في أن نظام الرسائل الفورية يسمح بتبادل الرسائل بين المستخدمين الذين يكونون على الخط في الانترنت في نفس الوقت , فلا تخزن الرسائل للاسترجاع والقراءة في وقت لاحق كالبريد الالكتروني , بل تعرض الرسائل على كمبيوتر المستلم في نفس اللحظة التي ارسلت فيها , فإذا كان الشخص الذي ارسلت اليه غير متصل بالانترنت , فإن الرسالة لا تصل اليه , ومن تطبيقات هذا النظام برنامج ويندوز لا يف ماسنجر , وبرنامج المحادثة الشهير ICQ وبرنامج سكايب وبرنامج البالتوك , وبرنامج ميبو .

تتضمن برامج التراسل الفوري خدمات نقل الملفات والبرامج والصور , وهذه الخدمات تشكل ثغرات تسمح بنقل الفيروسات والملفات والبرامج المصابة بالفيروسات . بل إن بعض الفيروسات وأحصنة طروادة تم كتابتها خصيصا لهذا النوع من التطبيقات وهي تحاول استغلال أي نقطة ضعف في برامج التراسل الفوري لكي تتمكن من ارسال نفسها إليك بدون معرفتك أو موافقتك .

1. **المستندات , الوورد والأكسل والانواع الأخرى :**

هناك بعض الخطوات التي يجب تكرار عملها في الوورد أو الأكسل في بعض الأعمال التي يقوم بها المستخدم , وبدلا من أن يقوم المستخدم بتكرار القيام بهذه الخطوات واحدة تلو الأخرى , فإنه يتم اتمتة جميع هذه الخطوات في زر واحد في لوحة المفاتيح , وهذا يفيد المستخدمين في تبسيط وتسهيل القيام بالمهام المكررة على وورد أو اكسل . وتسمى الخطوات التي يتم جمعها وأتمتتها تحت زر أو اجراء واحد ( الماكرو ) .

ومن أمثلة وحدات الماكرو ؛ علبة الأوامر التي تطبق الهوامش تلقائيا على المستندات , أو الوحدة التي تطبق الوظائف الحسابية على خلايا جدول بيانات معين .

تتكون المستندات في الاصدار الحديث من برامج الوورد والاكسل مع وحدات الماكرو الخاصة بها , بعض وحدات الماكرو تندرج داخل برنامج الوورد أو الاكسل , وبعضها الآخر يمكن أن توضع داخل المستندات نفسها , وقد هدفت شركة مايكروسوفت من وحدات الماكرو تقديم خدمات ومميزات للمستخدم , غير أن كتاب الفيروسات يحولون هذه الميزات والخدمات إلى طرق أخرى لنشر الفيروسات على أجهزة الكمبيوتر . على سبيل المثال , يستطيع فيروس الماكرو تضمين نفسه داخل المستندات التي في جهاز الكمبيوتر الخاص بك , وعندما تقوم بارسال هذه المستندات إلى شخص آخر عبر الانترنت , فإنك ترسل له الفيروس ايضا بدون ان تعلم .

وينشط فيروس الماكرو بمجرد فتح المستند الذي يحتوي عليه , ثم يصيب المستندات الأخرى وينتشر في الجهاز , كما يقوم بتدمير البيانات وبإحداث أي اضرار أخرى يحددها له كاتب الفيروس .

1. **مواقع الويب :**

هناك العديد من مواقع الانترنت التي تحتوي على برامج وملفات مصابة بالفيروسات , خاصة البرامج المجانية والتجريبية , وعندما يقوم المستخدم بتحميل هذه البرامج والملفات فإن الفيروسات تنتقل إلى حاسوبه معها .

1. **مجموعات الأخبار:**

مجموعات الأخبار أو مجموعات المناقشة هي عبارة عن مجموعات اخبارية مصنفة حسب الموضوع , فهناك مجموعة خاصة بالعلوم , وأخرى بالتكنولوجيا , بالمنوعات , وبالمجتمع , وبالكمبيوتر .... الخ , وتتوزع هذه المجموعات على آلاف المواقع على الانترنت . وتتيح هذه المجموعات تبادل الأفكار والخبرات ووجهات النظر بين الأشخاص في جميع انحاء العالم . ويستطيع المستخدم المشاركة في أي مجموعة من خلال ارسال مقالة لعرضها عليها , وتقنية رسائل المقالات في مجموعات الأخبار تشبه تماما تقنية رسائل البريد الالكتروني , سواء من حيث شكل الرسالة , أو نظام المرفقات , ولذلك فإن أي شخص يمكنه ان يثبت أي فيروسات أو أحصنة طروادة بالمرفقات الخاصة بالمقالة التي يرسلها كما يفعل في رسالة البريد الالكتروني , وقد يقع الشخص الذي يقرأ المقالة في أي مكان في العالم ضحية فيروس من هذا النوع عندما يفتح الملفات المصابة بالفيروس المرفقة بالمقالة . وقد يتضمن المقال رابط إلى موقع ويب يتضمن برمجيات خبيثة وفيروسات , وعندما يقوم المستخدم بالدخول على الرابط , فإنه يمكن للفيروسات والبرامج الخبيثة أن تنتقل الى جهازه وتلحق به ,

1. **البرامج المقرصنة :**

البرنامج المقرصن هو برنامج ينشر ويوزع بشكل غير قانوني مما يؤدي إلى حرمان صانع البرنامج الأصلي من الدخل أو الربح الذي يحصل عليه بواسطة بيعه , و البرامج المقرصنة يتم توزيعها بدرجة منخفضة من الشروط والمعايير الأمنية مما يسمح للفيروسات بالتسلل إليها , كما أن بعض الأشخاص الذين يقومون بتوزيع البرامج المقرصنة يتعمدون وضع الفيروسات فيها بقصد إلحاق أضرار بالأشخاص الذين يشترونها .

* **أشهر فيروسات الحاسب الآلي :**

1-الفيروس الاسرائيلي : اكتشف هذا الفيروس لاول مرة طالب في الجامعة العبرية في القدس , وقد وضع هذا الفيروس بحيث ينفذ في تاريخ 13 من كل شهر اذا صادف هذا التاريخ يوم جمعة , وعندما يتوافر هذان الشرطان , أي 13 + يوم جمعة , فإن الفيروس ينفذ ويدمر كل ما تحتويه اسطوانة الاقراص الصلبة من برامج وبيانات او يدمر البرنامج الذي يتم تشغيله [[11]](#footnote-11) .

2-فيروس ميليسا Melissa : وقد تميز هذا الفيروس بأنه يقوم بالبحث عن دفتر عناوين البريد الالكتروني الخاص بك , ثم يقوم بارسال نسخة من نفسه الى عناوين اصدقائك ومعارفك الموجودة في هذا الدفتر , وعندما يفتح احد الاصدقاء او المعارف الرسالة فإنه ينتقل الى معارفه واصدقائه وهكذا .

وقد ساعدت هذه الطريقة الفيروس على الانتشار الى انحاء العالم اكثر من أي فيروس اخر , ومع ان هذا الفيروس لا يسبب اضرارا تدميرية للبرامج والبيانات , إلا أنه تسبب في ارسال مئات الآلاف من رسائل البريد الالكتروني التي ادت الى بطء الخدمة واغلاق انظمة البريد الالكتروني , كما كلفت ازالته والتخلص منه خسائر مادية باهضة [[12]](#footnote-12) .
3-فيرس تشرنوبل 1998 : وهو واحد من أشد الفيروسات تدميرا ، وسمي "تشرنوبل" نسبة إلى  "حادثة  تشرنوبل" التى وقعت فى أوكرانيا عام 1986 بسبب انفجار فى أحد المفاعلات النووية .
يصيب فيرس تشيرنوبيل القرص الصلب فيجعل الجهاز غير قادر على الإقلاع. ويقوم في نفس الوقت بمحاولة مسح البيوس مما يتطلب إعادة تنصيب البيوس ، وهو امر صعب لذلك فإن الناس الذين أصيبوا بهذا الفيروس قاموا بتغيير أجهزتهم [[13]](#footnote-13).

4-فيرس مايكل أنجلو – 1991 : تم اكتشاف فيرس مايكل أنجلو لأول مرة فى أبريل 1991 فى نيوزلندا ، انتشر فيرس مايكل أنجلو على الأجهزة التى تعمل بنظام MS Dos لكنه يبقى ساكنا فى الجهاز غير محدث لأية أضرار حتى مجىء يوم 6 مارس – ذكرى ميلاد الفنان مايكل أنجلو – حيث يحدث أكبر قدر ممكن من التدمير [[14]](#footnote-14).

5-فيروس الحب 2000 م : يأتي هذا الفيروس على هيئة بريد الكتروني من احد الاصدقاء أو المعارف مثل فيروس ميليسا , ولكن عنوان الرسالة كان هو I love you , مما ادى الى انتشار الفيروس بسرعة كبيرة عبر انحاء العالم حيث اصاب خمسة عشر مليون جهاز كمبيوتر من اجمالي ثلاثمائة مليون جهاز في انحاء العالم , وتميز الفيروس بأنه يدمر الملفات الغير تجارية مثل ملفات الموسيقى والجرافيك ونحوها وتسبب في خسائر بلغت ما بين 5 الى 10 مليار دولار [[15]](#footnote-15).

6-دودة سانتي Santy 2005 م :
 تطلب دودة سانتي من محرك البحث مثل جوجل وياهو إنشاء قائمة بأسماء المواقع الموجودة بها الثغرة التى تنفذ من خلالها ، ثم تدمر جميع محتويات الموقع ، تاركة رسالة تفيد بأن الموقع قد تم تشويهه بواسطتها . وقد قامت بتدمير أكثر من 40 ألف موقع فى أقل من 24 ساعة فقط ! [[16]](#footnote-16).

7- دودة ستاكس نت Stuxnet 2010 م :
ضربت دودة ستاكس نت Stuxnet عدة منشآت صناعية هامة كمفاعل بوشهر النووى بإيران فضلا عن 15 مؤسسة صناعية أخرى ، الجدير بالذكر أن إيران  تحملت 60% من إجمالى الخسائر التى سببها [Stuxnet](http://itwadi.com/node/1423) مما يبين أن الهدف من وراء [Stuxnet](http://itwadi.com/node/1423) كانت أهداف سياسية تقف وراءها قوى دولية [[17]](#footnote-17).

* **دوافع مجرمي الفيروسات :**

كان الاعتقاد الشائع يذهب الى ان صانعي الفيروسات هم من المراهقين , وقد رسخ هذا الاعتقاد ان الفيروسات الاولى قام بصناعتها طلاب ومراهقون مثل الفيروس الباكستاني ودودة موريس , لكن مع دخول تقنيات جديدة في صناعة الفيروسات فإن هذا الاعتقاد بدأ يتلاشى , إذ ان صناعة الفيروسات اصبحت مهمة صعبة لم يعد يكفي لها ان يكون الشخص مبرمجا جيدا , بل اصبحت صناعة الفيروس تتطلب الماما بانظمة الحاسب الحديثة وكيفية عملها وتقنياتها المختلفة , وهو الامر الذي ادى الى دخول المتخصصين في تكنولوجيا المعلومات الى الساحة ومشاركتهم في صناعة برامج الفيروسات [[18]](#footnote-18).

وتتعدد دوافع كتاب او صانعي الفيروسات الا أنه يمكن اجمال اهمها فيما يلي :

1-عدم وجود احترام كبير للسلطات : لا يحمل كتاب الفيروسات اي احترام او تقدير للسلطات , ولا يحترمون ويقدرون الا انفسهم وما لديهم من مهارات وقدرات , بل انهم يفاخرون باختراق القوانين والانظمة التي تجرم وتحظر انشطتهم .

2-عدم احترام ملكية الآخرين وأموالهم : كتاب الفيروسات لديهم استهتار واستهانة بممتلكات الآخرين وأموالهم , وهم يتنافسون على عرض مهاراتهم وبرهنة ذواتهم من خلال تدمير اموال الآخرين وممتلكاتهم بالفيروسات , والاستمتاع بمشاهدة آثار التخريب والتدمير الذي احدثوه بواسطة هذه الفيروسات , ولذلك فإنه يمكن القول بأن لديهم نوع من الأنانية المرضية , والافتقار الى القيم الاخلاقية التي يتسم بها افراد المجتمع [[19]](#footnote-19).

3-الانتقام : قد يكون دافع كاتب الفيروس هو الانتقام , كأن ينتقم الموظف من صاحب العمل بسبب فصله أو تعرضه لأي شكل من اشكال الظلم , فيقوم بزرع فيروس في اجهزة الحاسب التابعة للشركة التي كان يعمل بها مستغلا معرفته بنظام الشركة والثغرات الموجودة فيه , مما يؤدي الى تدمير بيانات وبرامج الشركة ويسبب لها خسائر فادحة .

مثال ذلك قيام مبرمج فرنسي بدافع الانتقام من فصله من العمل بوضع فيروس من نوع القنبلة المنطقية على شبكة المنشأة التي كان يعمل بها , بحيث تنفجر بعد مضي ستة اشهر من رحيله عن المنشأة , الامر الذي ادى الى اتلاف كل البيانات المتعلقة به [[20]](#footnote-20).

4-الهدف التجاري : قد يتم عمل وصنع الفيروسات من أجل بيع برامج مضادات الفيروسات لانة بعمل الفيروس يصبح المستخدمون بحاجة إلى برامج مضادة للفيروسات ويضطرون للشراء . معظم شركات مضادات الفيروسات تقوم بصناعة الفيروسات وتقوم بعمل مضادات لها وذلك لتسويق منتجاتها وبرامجها لدى مستخدمي الكمبيوتر [[21]](#footnote-21).

1. راجع : Peter Szor, The art of computer virus research and defens ,Symantec Press,Addison Wesley Professional, 2005 , 2.3

حجار , فادي , تشريح الفيروسات , شعاع للنشر والعلوم , دمشق , 2003 م , ص9 . [↑](#footnote-ref-1)
2. Computer virus – from an Annoyance to a serious threat , p2 [↑](#footnote-ref-2)
3. Mark A. Ludwig , The Little Black Book of computer Virus , p12 [↑](#footnote-ref-3)
4. حجار , فادي , تشريح الفيروسات , ص 9 , 10 . [↑](#footnote-ref-4)
5. Computer virus – from an Annoyance to a serious threat , p3 [↑](#footnote-ref-5)
6. Jhon Aycock, Computer virus and malwar p 14 [↑](#footnote-ref-6)
7. Computer virus – from an Annoyance to a serious threat, USA ,F-secure Corporation , p4 [↑](#footnote-ref-7)
8. أبو الفتوح , خالد , فيروس الكمبيوتر مرض التكنولوجيا الحديثة , دار الكتب العلمية للنشر والتوزيع , مصر , 1990 م , ص 52 , 53 . [↑](#footnote-ref-8)
9. Mark A. Ludwig , The Little Black Book of computer Virus, p15 [↑](#footnote-ref-9)
10. Peter Gregory , Computer virus for Dummies,wiley publishing , p 238-244 [↑](#footnote-ref-10)
11. ابو الفتوح , خالد , فيروسات الحاسب الآلي مرض التكنولوجيا الحديثة , ص 114 . [↑](#footnote-ref-11)
12. ريتشارد ما نسفيلد , حيل واساليب الهاكرز, دار الفاروق للنشر والتوزيع , مصر , 2001 م , ص 256 , 257 . [↑](#footnote-ref-12)
13. أخطر 10 فيروسات فى التاريخ \_ وادي التقنية.htm [↑](#footnote-ref-13)
14. أخطر 10 فيروسات فى التاريخ \_ وادي التقنية.htm [↑](#footnote-ref-14)
15. ريتشارد مانسفيلد , حيل واساليب الهاكرز , ص 264 , 265 . [↑](#footnote-ref-15)
16. أخطر 10 فيروسات فى التاريخ \_ وادي التقنية.htm [↑](#footnote-ref-16)
17. أخطر 10 فيروسات فى التاريخ \_ وادي التقنية.htm [↑](#footnote-ref-17)
18. Computer virus – from an Annoyance to a serious threat ,p15 [↑](#footnote-ref-18)
19. راجع فيما تقدم :

 Peter Gregory , Computer virus for Dummies , p 217,218,219 . [↑](#footnote-ref-19)
20. الملط , أحمد خليفة , الجرائم المعلوماتية , دار الفكر الجامعي , الاسكندرية , ط2 , 2006 م , ص 546 . [↑](#footnote-ref-20)
21. فيروس الحاسوب , ويكيديا . [↑](#footnote-ref-21)