الفيروسات

يعتبر الفيروس أحد البرامج التخريبية التي تصنع لهدف غير قانوني وغير مشروع، ويقوم الفيروس بمهاجمة الملفات المحفوظة التي توجد في الأجهزة الالكترونية، حيث يتم صناعة هذه البرامج على يد المبرمجين المحترفين، وذلك بهدف إلحاق الضرر بالأجهزة الإلكترونية.

ولا يعرف السبب وراء صناعة هذه البرامج حتى اليوم، ومن أشهر الفيروسات الخبيثة التي استطاعت أن تخترق معظم أجهزة كمبيوتر العالم هو فيروس (روت كيت)، الذي وسع انتشاره بشكل سريع جدًا حين ظهوره.

هجمات توقف الخدمة

تتمثل هجمات توقف الخدمة في هجوم القرصنة الإلكترونين من خلال إمداد أعداد كبيرة وكميات هائلة من البيانات الغير هامة، التي تحمل الفيروسات وتنتشر داخل الموقع، فتبدأ هذه الفيروسات بتدمير المستخدمين المسجلين على الموقع، ويعتبر هذا النوع من أكثر الفيروسات خطورة لأن لا يمكن ملاحظته، بالإضافة إلى أنه يتدرج حتى يصل لنهايته.

هجمات المعلومة المرسلة

يعتمد هذا النوع من التهديدات على شن هجوم على المعلومات المرسلة، حيث يقف بمثابة حاجز لمنع وصول هذه المعلومات، وينتشر بسرعة كبيرة في برامج الدردشة والمحادثات مثل فايبر، ماسنجر، واتساب.

السيطرة على أجهزة الحاسب

عندما تقع الضحية لهذا النوع من التهديدات تكون تحت سيطرة المخترق بشكل كامل، حيث يتمكن من الحصول على كل ملفات الكمبيوتر، ويستطيع نسخها والتصرف فيها بكل يسر، وعلى الأغلب يقوم القرصنة بابتزاز الضحايا من خلال نشر البيانات والصور الهامة.

فيروسات الحاسوب

هو برنامج تخريبيّ يتم برمجته بأيدي مبرمجين محترفين، يحدث هذا البرنامج خللاً في خصائص الملفات التي يستهدفها ليجعلها تحت سيطرة المبرمج من خلال حذف جميع مستندات هذا الملف أو تخريبها أو التعديل عليها، وتكون الغاية من هذه البرامج تخريب أجهزة الحاسوب الخاصة بالمستخدمين، وكما قد يكون الهدف منه الحصول على ملفات وبيانات مهمة من جهاز مستخدم ما، ومن أكثر برامج الفيروسات ضرراً فيروس الروت كوت وذلك لعدم سهولة اكتشافه وسرعة تدميره للجهاز بكل سريّة، ويُنصح مستخدمو أجهزة الحاسوب عادة بالاحتفاظ بنسخ من مضادات الفيروس وتحديثها باستمرار.

تمتاز فيروسات الحاسوب بعدة صفات، منها:

- التلقائيّة في القدرة على التناسخ والانتشار.
- الربط الذاتيّ للفيروس مع برنامج يُطلق عليه الحاضن (Host).
- غير قابلة للنشأة من تلقاء ذاتها.
- فيروس الحاسوب انتقالي أي له القدرة لانتقال من حاسوب الى اخر.

مكونات الفيروس

تُصنّف مكونات برنامج فيروس الحاسوب إلى أربعة مكونات رئيسية وهي:

- **التناسخ (Replication):** وهو أحد أجزاء برنامج الفيروس الذي يمنحه خاصيّة التناسخ والانتشار بشكل تلقائيّ.
- **التخفي (Protection):** يضفي هذا الجزء على برنامج الحاسوب خاصيّة السريّة أي عدم القدرة على الكشف عن وجوده بسهولة.
- **التنشيط (The Trigger):** ويعطي هذا الجزء للفيروس خاصية القدرة على الانتشار قبل اكتشافه ويكون عادة ضمن توقيت معيّن كساعة معيّنة أو تاريخ معيّن، مثال على ذلك الفيروس الشهير الذي يمارس نشاطاته في السادس من شهر آذار من كل سنة وهو Michelangelo.
- **التنفيذ (The Payload)** وهو المهمة المناطة بالفيروس لتنفيذها عند بدء نشاطه وانتشاره.

طرق انتقال الفيروس

تنتقل الفيروسات في الحاسوب بطريقتين رئيسيّتين، وهما:

- **العدوى المباشرة (Direct Infector):** يغزو الفيروس ملفات الحاسوب وعندما يتم تشغيل أو استخدام أحد هذه الملفات فإن الفيروس يبدأ بنشاطه وانتشاره وينتقل بين الملفات الموجودة على جهاز الحاسوب، وفور انتقال العدوى لأي ملف فإنه يتم تحميله ونقله إلى الذاكرة تلقائياً ومن ثم تشغيله.
- **العدوى غير المباشرة (Indirect Infector):** يُنقل البرنامج المصاب بالفيروس إلى ذاكرة جهاز الحاسوب فور بدء تشغيل الملف المصاب وينفذ الحاسوب أوامر الملف الأصلي، وبعد ذلك تنتقل الإصابة بالفيروس لأي ملف يتم تحميله إلى الذاكرة، ويتوقف هذا النوع من الانتشار في حال فصل التيار الكهربائيّ عن جهاز الحاسوب أو إعادة التشغيل.

أنواع الملفات التي يغزوها الفيروس

يستهدف الفيروس الملفات القابلة للتنفيذ والتشفير، وهي:

- الملفات ذاتيّة التنفيذ، ويُقصد بها الملفات التي لها امتداد .EXE, .com. ELF
- سجلّات الملفات والبيانات (Volume Boot Record, Master Boot).
- ملفات الأغراض العامة (Script).
- أنظمة التشغيل وملفات الاستخدام المكتبيّ (MS-Office, Microsoft Windows).
- قواعد البيانات وملفات الأوتولوك (E-mails).
- الملفات ذات الامتداد PDF، ونصوص HTML.
- الملفات المضغوطة (RAR, ZIP).
- الملفات الصوتيّة MP3.

أنواع الفيروسات

تقسم فيروسات الحاسوب إلى أنواع، وهي على النحو التالي:

- **الفيروسات المخادعة (ذات قدرة تحويليّة متعددة):** وهي البرامج التخريبيّة التي تمتلك القدرة على الديناميكيّة في التحوّل والتخفي من خلال تغيير شفرتها عند بدء بانتقال عدوتها بين الملفات، وذلك لعدم الكشف عنها.

- **فيروسات قطاع التشغيل:** يتمركز هذا النوع من الفيروسات في المواقع التي يقرأها جهاز الحاسوب من خلال القرص الصلب، ويبدأ مفعولها التخريبي بالسريان عند بدء إقلاع القرص الصلب وتستقر في ذاكرة جهاز الحاسوب وتبدأ بفك شفرتها وتنفيذ الأوامر.

- **فيروسات الماكرو:** يعتبر هذا النوع من أكثر أنواع الفيروسات الحاسوبية حداثة، ويعتمد المبرمجون على برنامج معالجة النصوص Microsoft word في كتابته، ويغزو الملفات التي تحتوي على البيانات وبشكل أدق ملفات الأوفيس.

- **الفيروسات ذات الملفات المتعددة:** يدخل هذا النوع من الفيروسات إلى جهاز المستخدم بصيغة معيّنة وفور استقراره بالجهاز وتمكنه منه يبدأ بالتحوّل لأكثر من صيغة ليستهدف الملفات جميعها.

- **الفيروسات الخفيّة:** يستقر هذا النوع في ذاكرة جهاز الحاسوب، ويتولّى مهمة إعاقة فحص نظام التشغيل وقطاعه، ويرسل تقرير بسلامة الجهاز وعدم العثور على أي فيروسات.

- **فيروسات الملفات التنفيذيّة:** تجعل هذه الفيروسات من نفسها ملحقاً مع ملفات البرامج التنفيذيّة ومرافقاً لها باستمرار، ومن هذه البرامج التنفيذية Command.com.

- **فيروسات ذات مهام متعددة،** تغزو قطاع بدء التشغيل مع الملفات الموجودة على جهاز الحاسوب في آن واحد، أي أنّها تغزو جميع محتويات الحاسوب.

- **فيروسات قطاع التشغيل (Boot Sector):** يُعتبر هذا النوع من أكثر أنواع الفيروسات خطورة ويهدّد بشكل مباشر المقطع التشغيليّ في القرص الصلب ويصيبه.

- **الفيروسات الطفيليّة:** تتطفل هذه الفيروسات على الملفات التنفيذية وتتمركز في الذاكرة، وتبدأ عملها فور استخدام المستخدم لأي من البرامج المصابة، وتبدأ بعدها بغزو أي برنامج يتم تشغيله.

- **الفيروسات المتطوّرة:** لديها القدرة على الانتقال من جهاز حاسوب إلى آخر من خلال التحول من شفرة إلى أخرى.

تصنيفات الفيروسات

تصنف برامج فيروسات الحاسوب إلى عدة أنواع، وهي:

- **تصنيفات الفيروسات وفقاً للنوع:**

  - **الفيروس:** وهو عبارة عن برنامج تخريبي تنفيذي يحمل الامتداد (.com, .exe, .bat, .pif, .scr) يستهدف نظام الحاسوب ويلحق الضرر به.

  - **ديدان الحواسيب:** ينتقل هذا النوع بالاعتماد على الاتصال بالشبكة العنكبوتيّة العالمية ويكون عادة عبر البريد الإلكترونيّ.

- **أحصنة طروادة (Trojan Horse)**: يدخل هذا الفيروس برفقة أحد البرامج إلى جهاز الحاسوب بشكل سريّ، ويبدأ بعمله بعد أن يتم تنفيذ البرنامج الذي دخل برفقته ويمارس أعماله التخريبيّة.

- **تصنيفات الفيروسات وفقاً للسرعة:**
  - فيروسات سريعة الانتشار.
  - فيروسات بطيئة الانتشار.
  - فيروسات دائمة النشاط.
  - فيروسات مؤقتة النشاط.

تأثير الفيروسات في الحاسوب

- إبطاء عمل جهاز الحاسوب، وحدوث أخطاء مجهولة عند تشغيل البرامج وتنفيذ أوامرها.
- توسيع حجم الملفات وزيادتها، وكما يزيد من المدة التي يتم بها تحميل البرامج والملفات إلى ذاكرة جهاز الحاسوب.
- ملاحظة وجود تأثير غير مسبوق ورسائل على الشاشة.
- ظهور رسالة FATALI/o ERROR عند بدء قراءة الأقراص وزيادة المدة الزمنيّة في قراءتها في حال كانت محميّة.
- ملاحظة المستخدم صدور نغمات موسيقية غير مألوفة له.
- إحداث تغييرات في تواريخ تسجيل الملفات.
- اختلال عمل لوحة المفاتيح.
- تراجع المساحة المتوفرة في ذاكرة الجهاز، نظراً لما يشغله الفيروس من مساحة كبيرة.
- إظهار رسائل تكشف عن عدم وجود ذاكرة كافية لتحميل البرامج والملفات.
- عدم صلاحيّة بعض المساحات للتخزين في القرص الصلب.
- إلحاق الضرر بالنظام من خلال تعطيل BOOT Sector.
- تعرض البيانات والملفات للإتلاف.

الوقاية من فيروسات الحاسوب

يُنصح المستخدم عادةً بحماية جهازه من الفيروسات ووقايته منها، وذلك باتباع الخطوات التالية:

- عدم تحميل أي برامج دون إجراء فحص لها، وكذلك الأمر بالنسبة للملفات المحملة والمنقولة من الشبكة العنكبوتيّة فيتوجب الفحص قبل التشغيل.
- تحميل البرامج الخاصة للكشف عن وجود الفيروسات ومكافحتها في جهاز الحاسوب.
- الاحتفاظ بنسخ احتياطيّة (Backup) للملفات والبرامج.
- الاعتماد على برامج الجدار الناري التي تقف عائقاً في وجه الفيروسات.
- تنصيب أنظمة تشغيل أكثر أماناً كنظام التشغيل جنو/لينكس.
- عدم تشغيل ملفات وبرامج مجهولة المصدر.
- أخذ الحيطة والحذر من الرسائل التي تصل عبر البريد الإلكترونيّ والروابط المجهولة المصدر وفحصها قبل فتحها.

إزالة فيروسات الحاسوب

يُنصح المستخدم في حال اكتشافه وجود فيروسات بجهازه اتخاذ الإجراءات التالية:

- تنصيب برامج حماية من الفيروسات (Anti-Virus).
- البدء بعمل Scan لكل الملفات الموجودة.

وكما يمكن ذلك من خلال الاتصال بشبكة الإنترنت والولوج إلى مواقع الإنترنت والقيام بعملية الفحص، وتوفر Microsoft.com ذلك، إذ يتطلب ذلك من المستخدم الوصول إلى صفحة (برنامج مكافحة الفيروسات من MIcrosoft) على الشبكة العنكبوتيّة، واختيار "Download Now" التنزيل الآن، واتباع التعليمات لحين الانتهاء من التنزيل.