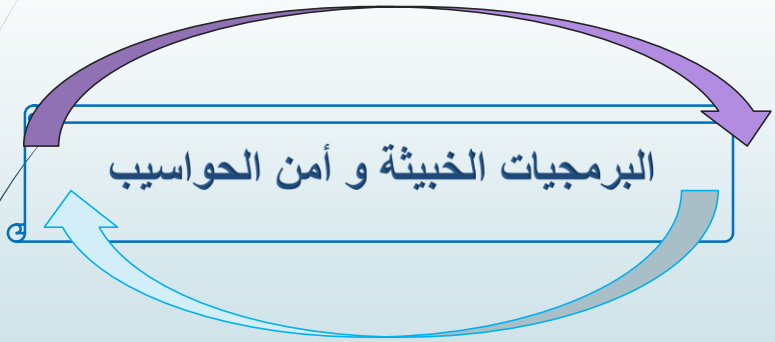
أمن المعلومات

GS224 - 8



أمن نظم المعلومات

- المقصود **بأمن الحواسيب** هو امن الكيان المادي (العتاد المادي)،
- في حين ان المقصد من **أمن البرمجيات** هو امن أنظمة التشغيل التي تتحكم بالأجهزة الحاسوبية وترابطها،
- اما **أمن التطبيقات** فهي البرامج التطبيقية المختلفة التي يتعامل معها المستخدم لأداء مهامه و اعماله،
- ويقصد **بأمن الملفات** هو أمن الملفات بنفسها كأوعية لتخزين المعلومات و البيانات، مثل: ملفات معالجة النصوص، الجداول الالكترونية، قواعد البيانات، رسائل البريد الالكتروني، وامن نظام الملفات الذى يتحكم بإدارة جميع الملفات.

التهديدات الرقمية على الحواسيب و البرمجيات و الملفات

يمكن **التهديد الرئيس للحواسيب** في وفرتها، فالحاسوب ماديا هو اكثر المناطق ضعفا في مواجهة الهجمات، وأكثرها طاعة لضوابط الرقابة التلقائية. و تشمل تهديدات الحواسيب السرقة وإلحاق الضرر بها سواء عن طريق الخطأ ام العمد. ان الزيادة المضطردة لاستخدام الحواسيب و انتشار شبكاتها، كذلك الاعتماد عليها في انجاز جميع الاعمال، زاد من احتمال فقدانها، لذلك فإن الاحتياطات الأمنية المادية و الإدارية أصبحت ضرورية جدا للتعامل مع هذه التهديدات.

ان **التهديد الرئيس للبرمجيات** يكمن في الهجمات على توفر البرمجيات وخاصة التطبيقية منها، حيث غالبا ما تكون سهلة الحذف. ومن التهديدات إمكانية تغيير البرامج التطبيقية او اتلافها؛ لتصبح غير مفيدة، كذلك التعديلات التي تحدث للبرنامج وهو لايزال يعمل ولكنها تجرى بطريقة مختلفة عن الطريقة السابقة مما يستلزم توزيعها بعناية عن طريق انشاء النسخ وفق إصدارات تدريجية و توزيع الاحدث منها. المشكلة الأخرى التي تواجه البرمجيات هي حقوق الملكية، فرغم اتخاذ المثير من الاحتياطات فلازالت مشكلة النسخ غير المرخص للبرامج بدون حل.

ان **التهديدات الأمنية على البيانات** واسعة جدا لدرجة انها تشمل تهديدات توفرها، وتهديدات سريتها، وتهديدات سلامتها و تكاملها (نزاهتها). ففي حالة التوفر تمكن التهديدات في اتلاف ملفات البيانات والتي قد تحدث عن طريق الخطأ او متعمدا. في حالة السرية، تكمن التهديدات في القراءة غير المسموح بها لملفات البيانات او قواعد البيانات. في حالة سلامة البيانات و تكاملها ، تكمن التهديدات في تغيير البيانات، إما بالحذف او إضافة او تعديل. وهناك تهديد أخر لكنها اقل ظهورا، وهو تحليل البيانات و تحليل تصاميم قواعد البيانات من اجل كسر حمايتها، و يمكن القول ان سلامة البيانات هي الهاجس الأكبر لمعظم المؤسسات؛ لان التعديلات التي قد تجرى على ملفات البيانات قد يترتب عليها نتائج تتراوح من المخاطر الصغيرة الى المخاطر الكارثية.

1- البرمجيات الخبيثة (Malware)

أكثر أنواع التهديدات تطورا لأنظمة الحاسب تتم من خلال البرامج التي تستغل نقاط الضعف في أنظمة الحوسبة من اجل اختراقها. ويشار إلى هذه التهديدات على أنها **برامج خبيثة أو ضارة (Malicious Software)**. مصطلح (Malware) اختصار الى (malicious software) والتي تعني البرمجيات الخبيثة. وهي البرمجيات التي صممت خصيصاً للتدمير أو التعطيل أو السرقة أو كسر السياسات الأمان وخططه، أو بشكل عام إحداث أنشطة سيئة أو غير شرعية على الأنظمة الحاسوبية. الفيروسات والدودة الحاسوبية وأحصنة طروادة والروبوتات الشبكية كلها أمثلة على البرمجيات الخبيثة. وقد ازداد وتضخم عدد البرمجيات الخبيثة بشكل كبير جدا تصل للملايين.

- يمكن تقسيم البرمجيات الخبيثة **حسب موقعها** إلى فئتين:
  - البرامج (او أجزاء من برنامج) التي تحتاج إلى **برامج مستضيفة :** أجزاء من البرنامج (او برنامج) لا يمكن أن توجد بشكل مستقل فعليا عن البرنامج التطبيقي، أو برنامج النظام. ومن الأمثلة على ذلك الفيروسات والقنابل المنطقية والأبواب الخلفية.
  - **برامج مستقلة** قائمة بذاتها : البرامج المستقلة هي التي يمكن جدولتها وتشغيلها بواسطة نظام التشغيل. من الأمثلة على ذلك برامج الديدان.
- وتقسم أيضًا بنأ على **الاضرار** التي تسببها البرامج الخبيثة فمنها التي لا تتضاعف وتلك التي تتضاعف.
  - الاضرار التي **لا تتضاعف** تسببها برامج أو أجزاء من البرامج التي يتم تنشيطها بواسطة مشغل. ومن الأمثلة القنابل المنطقية والأبواب الخلفية و الروبوتات.
  - الاضرار التي **تتضاعف** تسببها برامج مستقل أو أجزاء من البرامج قد ينتج عند تنفيذه نسخة واحدة أو أكثر من نفسه ليتم تفعيلها لاحقًا على نفس النظام أو على نظام آخر. من الأمثلة على ذلك الفيروسات والديدان.
- تعتبر تهديدات متطورة لأنظمة المعلومات .

1- البرمجيات الخبيثة (Malware) : السمات

بمرور الوقت ظهرت أنواع مختلفة من البرامج الخبيثة ونتيجة لأن الدفاعات الأمنية أصبحت أكثر تعقيدًا تدريجيا أصبحت الهجمات المقابلة أكثر تعقيدًا. ومع ذلك، لم يتم وضع معيار لتصنيف الأنواع المختلفة من البرامج الخبيثة. ونتيجة لذلك، غالبًا ما تكون تعريفات الأنواع المختلفة من البرامج الضارة مربكة وقد تتداخل. تتمثل إحدى طرق تصنيف الأنواع المختلفة من البرامج الخبيثة في استخدام السمات الأساسية التي تمتلكها هذه البرامج. وهذه السمات هي قدرات **الانتشار والعدوى والإخفاء والحمولة** :-

- **الانتشار** : تتمتع بعض البرامج الضارة بسمة أساسية تنتشر بسرعة إلى الأنظمة الأخرى من أجل التأثير على عدد كبير من المستخدمين. يمكن أن تنتشر البرامج الضارة عبر مجموعة متنوعة من الوسائل: باستخدام الشبكة التي تتصل بها جميع الأجهزة، من خلال فلاش (USB) محركات الأقراص المشتركة بين المستخدمين، أو عن طريق إرسال البرامج الضارة كمرفق بالبريد الإلكتروني. يمكن نشر البرامج الضارة تلقائيًا أو قد تتطلب اتخاذ إجراء من قبل المستخدم.

1- البرمجيات الخبيثة (Malware) : السمات

- **العدوى** : بمجرد وصول البرامج الضارة إلى النظام من خلال التداول، يجب أن "تصيب" هذا النظام أو تدمجه فيه. قد تعمل البرامج الضارة مرة واحدة فقط ثم تخزن نفسها في ذاكرة الحاسوب، أو قد تبقى على النظام ويتم إطلاقها لعدد لا نهائي من المرات من خلال ميزة التشغيل التلقائي. ترتبط بعض البرامج الضارة ببرنامج حميد بينما تعمل البرامج الضارة الأخرى كعملية قائمة بذاتها.
- **الإخفاء** : تتمتع بعض البرامج الضارة بسمة أساسية تتمثل في تجنب اكتشافها عن طريق إخفاء وجودها عن الماسحات الضوئية. تحاول البرامج الضارة متعددة الأشكال تجنب اكتشافها عن طريق تغيير نفسها، بينما يمكن للبرامج الضارة الأخرى تضمين نفسها في العمليات الحالية أو تعديل نظام التشغيل المضيف الأساسي.
- **الحمولة** : عندما تكون قدرات الحمولة هي محور التركيز الأساسي للبرامج الضارة، يكون التركيز على الإجراء (الإجراءات) الشائنة التي تقوم بها البرامج الضارة. هل يسرق كلمات المرور والبيانات القيمة الأخرى من نظام المستخدم؟ هل يقوم بحذف البرامج بحيث لا يتمكن الكمبيوتر من العمل بشكل صحيح؟ أم أن البرامج الضارة تقوم بتعديل إعدادات أمان النظام؟ في بعض الحالات، يكون غرض البرامج الضارة هو استخدام النظام المصاب لشن هجمات ضد أجهزة الكمبيوتر الأخرى.

مصطلحات البرمجيات الخبيثة

- **الفيروس** (Virus) : شفرة برمجية تلحق نفسها ببرنامج وينشر نسخًا منه على برامج أخرى.
- **الدودة الحاسوبية** (Worm) : برنامج ينشر نسخًا من نفسه على حواسيب أخرى عبر الشبكة.
- **القنبلة المنطقية** (Logic bomb) : تطلق فعل ما (تنفجر) عند حدوث شرط ما (استثارة).
- **حصان طروادة** (Trojan horse) : برنامج يحتوي على مهام إضافية غير متوقعة وغير معلنة.
- **الباب الخلفي** (Backdoor) : تعديل في برنامج شرعي يسمح بالوصول غير المصرح به إلى وظائفه.
- **برنامج متنقل** (Mobile code) : برنامج يمكن وضعه دون تغيير على مجموعة غير متجانسة من المنصات البرمجية وتنفيذه باستخدام دلالات متطابقة.
- **الادوات التلقائية** (مولد الفيروسات) (Auto-rooter Kit) : مجموعة من ادوات القرصنة الخبيثة لتوليد فيروسات جديدة تلقائيًا و تستخدم لاقتحام حواسيب جديدة عن بُعد.
- **برامج الرسائل الاقتحامية** (Spammer and flooder programs) : تُستخدم لإرسال كميات كبيرة من البريد الإلكتروني غير المرغوب فيه ، أو لمهاجمة الأنظمة التي تتضمن حركة المرور كبيرة وذلك لتنفيذ هجوم الحرمان من الخدمة.
- **مسجل المفاتيح** (Keyloggers) : يلتقط ضغطات مفاتيح لوحة الادخال على النظام المخترق.
- **الأدوات الجذرية** (Rootkit) : مجموعة من أدوات القرصنة المستخدمة بعد اختراق المهاجم لنظام حاسوب واكتسب وصولاً على مستوى الجذر/الأساس . وهى أدوات برمجية تعطي المستخدم وصولاً غير مصرح به إلى الجذر (root- الجذر هو الحساب التنفيذي في أنظمة التشغيل يونكس). كما تقوم هذه البرمجيات باستبدال أدوات النظام القائمة (مثل تلك الأدوات التي تستخدم لعرض العمليات ومحتويات المجلدات)، ومن ثم فإن النسخة المعدلة من النظام تقوم بإخفاء وجودُ المستخدم غير المصرح به. ويعد تثبيت (rootkits) في جهاز الضحية أحد أهداف البرمجيات الخبيثة.
- **الزومبي** (Zombie) : برنامج على حاسوب مصاب يتم تفعيله لشن هجمات على حواسيب أخرى.

مصطلحات البرمجيات الخبيثة

- **الحمولة** (Payload) : الأفعال الناتجة من تنفيذ الشفرة البرمجية للبرمجيات الخبيثة.
- **البرمجيات الاجرامية** (Crimeware) : مجموعات الأدوات لبناء وانتاج برمجيات الخبيثة ؛ تشمل آليات النشر والضرر المفتعل : Zeus, Sakura, Blackhole, Phoenix
- **التهديدات المستمرة المتقدمة** (APT) (Advanced Persistent Threats)

وهى هجوم بشري متواصل ومكثف يتم من خلاله رفع القدرات الكاملة لتقنيات التسلل للأنظمة الحاسوبية. ويهدف تصميم هذا النوع من التهديد لاختراق المؤسسات حتى لو كانت محمية بضوابط أمن معلومات مصممة ومصانة بشكل جيد. ولهذا السبب يتطلب هذا النوع من التهديد درجة عالية منً التخصيص حسب الهدف. مما يعني أن مجموعة ممولة تمويلا جيداً من المهاجمين مسؤولة عن هذا التهديد. وبسبب اختلاف التهديدات التي تندرج تحت هذا النوع فإن مصطلح (APT) يشير عادة الى فريق الهجوم بدلا من الهجوم نفسه. والهدف العام لهذا النوع من التهديد هو استخدام الهجوم للحصول على موطئ قدم داخل المؤسسة والمحافظة عليه من أجل الاستخدام والمراقبة المستمرة.

1- البرمجيات الخبيثة : أ – الفيروسات (Virus)

فيروس الحاسب الآلي هو برنامج يُعدُّ لينسخ وينشر نفسه، وينتشر ذاتيًّا دون علم وتعاون مع المالك أو المستخدم للجهاز، ولم يتم التوصل بعد لتعريف موحد للفيروسات متفق عليه من الباحثين كافّة، والتعريف العام هو تعريف فريد كوهين[1]، الذي يعرّف الفيروس بأنه: «برنامج يعدّل البرامج الأخرى لكي تحتوي نسخة معدّلة من نفسها» ورغم أنّ هذا التعريف يصف جُلّ الفيروسات، وأن كثيرًا من الباحثين ما زالوا يصرّون على استخدامه، إلّا أنّه يقتصر على البرامج التي تقحم نفسها بنفسها في البرامج الأخرى فقط، وهو بذلك يهمل كثيرًا من الفيروسات التي تقحم نفسها في الملفّات التي ليست برامج بطبيعتها، كالوثائق مثلًا. وعليه

" برنامج يتم إدراجه في نظام ، سرًا عادةً ، بقصد المساس بسرية أو نزاهة أو توفر بيانات الضحية أو تطبيقاته أو نظام تشغيله أو خلاف ذلك كإزعاج الضحية أو مضايقته."

وتنتشر الفيروسات بواسطة ملف «مضيف» يتطلب تفاعل بشري لتنشيطه. وقد يكون الملف المصاب موجوداً في القرص الصلب للحاسوب، لكن الحاسوب لن يصاب حتى يتم تشغيل الملف. وينتشر الفيروس عندما يقوم شخص ما بإرسال ذلك الملف المصاب ُ إلى حاسوب جديد، ويشغل ذلك الملف على المضيف الجديد.

1- البرمجيات الخبيثة : أ - الفيروسات

يمر الفيروس النموذجي خلال حياته بالمراحل الأربع التالية:

- **مرحلة الخمول**: يكون الفيروس خاملاً. ويتم تنشيط الفيروس من خلال حدث ما ، مثل تاريخ ، أو وجود برنامج أو ملف آخر ، أو تجاوز سعة القرص لحد ما. وليست كل الفيروسات لديها مثل هذه المرحلة.
- **مرحلة الانتشار**: يضع الفيروس نسخة متطابقة منه في برامج أخرى أو في مناطق معينة للنظام على القرص. سيحتوي كل برنامج مصاب الآن على نسخة من الفيروس ، والتي ستدخل بدورها مرحلة الانتشار.
- **مرحلة التحفيز**: يتم تنشيط الفيروس لأداء الوظيفة التي تم تصميمه من أجلها. كما هو الحال مع مرحلة الخمول ، يمكن أن تحدث مرحلة التحفيز بسبب مجموعة متنوعة من أحداث النظام ، بما في ذلك عدد المرات التي قامت فيها هذه النسخة من الفيروس من نسخ نفسها.
- **مرحلة التنفيذ**: يتم تنفيذ الوظيفة والتي قد تكون غير ضارة ، على سبيل المثال رسالة على الشاشة ، أو إتلاف ، على سبيل المثال إتلاف البرامج وملفات البيانات.

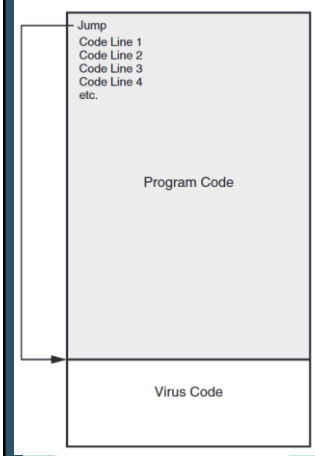
1- البرمجيات الخبيثة : أ - الفيروسات : البنية

- يتكون فيروس الحاسوب من ثلاثة مكونات:
  - **آلية العدوى**: الوسيلة التي ينتشر بها الفيروس بحيث يمكنه التكاثر. يشار إلى الآلية أيضًا باسم ناقل العدوى.
  - **التحفيز**: حدث أو حالة ما تحدد متى يتم تنشيط الحمولة أو توزيعها.
  - **الحمولة**: ما يفعله الفيروس إلى جانب انتشاره. قد تنطوي الحمولة على تلف أو قد تتضمن نشاطًا غير خطر ولكن ملحوظًا.
- **تواجد الفيروس يكون في المقدمة أو في النهاية** نسبة إلى البرنامج المنفذ ، أو يمكن تضمينه بطريقة أخرى. مفتاح تشغيله هو أن البرنامج المصاب عند استدعائه ، سيقوم أولاً بتنفيذ شفرة الفيروس ثم تنفيذ شفرة البرنامج المنفذ.
- بمجرد دخول الفيروس إلى النظام عن طريق إصابة برنامج ما بالنظام ، يكون في وضع يمكنه من **إصابة بعض أو جميع الملفات** القابلة للتنفيذ الأخرى على هذا النظام عند تنفيذ البرنامج المصاب. وبالتالي ، يمكن منع العدوى الفيروسية تمامًا عن طريق منع الفيروس من الدخول للنظام في المقام الأول.
- لسوء الحظ ، **الوقاية صعبة للغاية** لأن الفيروس يمكن أن يكون جزءًا من أي برنامج خارج النظام. وبالتالي ، ما لم يكتف المرء بكتابة جميع برامج النظام والتطبيق الخاصة به ، يكون المرء عرضة للخطر.
- يعد **الافتقار إلى ضوابط الوصول** على أجهزة الحاسوب القديمة أحد الأسباب الرئيسية للانتشار السريع للفيروسات التقليدية القائمة على شفرة الآلة على هذه الأنظمة. في المقابل ، في حين أنه من السهل كتابة فيروس شفرة الآلة لأنظمة يونيكس (UNIX)، إلا أنها غير فعالة تقريبًا عمليا نظرًا لوجود ضوابط في الوصول إلى هذه الأنظمة منعت الانتشار الفعال للفيروس.

1- البرمجيات الخبيثة : أ - الفيروسات : البنية

كانت الفيروسات الميكرة واضحة نسبيًا في كيفية إصابة الملفات. أحد الأنواع الأساسية للعدوى هو عدوى بطريقة الالحاق. يقوم الفيروس أولاً بإرفاق أو إلحاق نفسه بنهاية الملف المصاب. ثم يقوم بعد ذلك بإدراج تعليمات "الانتقال" في بداية الملف والتي تشير إلى نهاية الملف، وهي بداية الشفرة البرمجية للفيروس. عند تشغيل البرنامج، تقوم تعليمات الانتقال بإعادة توجيه التحكم إلى الفيروس. يوضح الشكل كيفية عمل **الاصابة بتقنية الإلحاق**. ومع ذلك، يمكن بسهولة اكتشاف هذه الأنواع من الفيروسات بواسطة برامج فحص الفيروسات. تبذل معظم الفيروسات اليوم جهودًا كبيرة لتجنب اكتشافها؛ ويسمى هذا النوع من الفيروسات **بالفيروسات المدرعة**. تتضمن بعض تقنيات الإصابة بالفيروسات المدرعة ما يلي:

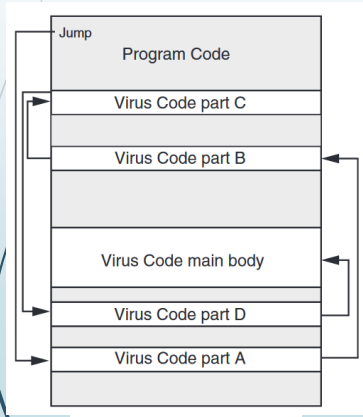
1) **تقنية الجبن السويسري**: بدلاً من وجود تعليمات "انتقال" واحدة إلى الشفرة البرمجية العادية للفيروس ، تقوم بعض الفيروسات المدرعة بإجراءين لجعل الكشف أكثر صعوبة. في البداية تقوم بـ "تشفير" (تشفير) الشفرة البرمجية للفيروس لجعل اكتشافه أكثر صعوبة. ثم تقوم بتقسيم المحرك "لتفكيك" (فك تشفير) رمز الفيروس إلى أجزاء مختلفة وحقن هذه القطع في جميع أنحاء شفرة البرنامج المصاب. عند إطلاق البرنامج، يتم ربط الأجزاء المختلفة معًا وتفكيك تشفير الفيروس. تظهر تقنية الجبن السويسري للإصابة في الشكل.



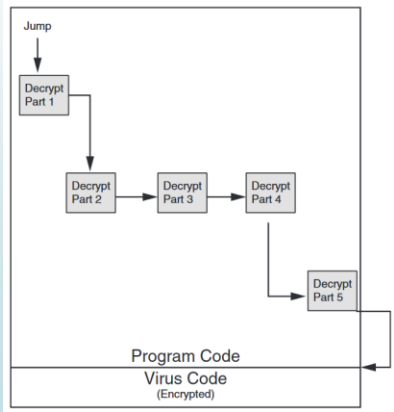
الإصابة بتقنية الالحاق

1- البرمجيات الخبيثة : أ - الفيروسات : البنية

2) **تقنية التقسيم**: بدلاً من إدخال أجزاء من محرك فك التشفير في جميع أنحاء شفرة البرنامج، تقوم بعض الفيروسات بتقسيم الشفرة الخبيثة نفسها إلى عدة أجزاء (مع نص رئيسي واحد من التعليمات البرمجية)، ثم يتم وضع هذه الأجزاء في مواضع عشوائية في جميع أنحاء البرنامج. ولجعل عملية الكشف أكثر صعوبة، قد تحتوي هذه الأجزاء على تعليمات برمجية "خردة" غير ضرورية لإخفاء غرضها الحقيقي. تظهر تقنية التقسيم للإصابة في الشكل .



الإصابة بتقنية التقسيم



الإصابة بتقنية الجبن السويسري

1- البرمجيات الخبيثة : أ - الفيروسات : البنية

```
    program V :=

{goto main;
    1234567;

    subroutine infect-executable :=
        {loop:
        file := get-random-executable-file;
        if (first-line-of-file = 1234567)
          then goto loop
          else prepend V to file; }

    subroutine do-damage :=
        {whatever damage is to be done}

    subroutine trigger-pulled :=
        {return true if some condition holds}

main:   main-program :=
        {infect-executable;
        if trigger-pulled then do-damage;
        goto next;}

next:

}
```

يوضح الشكل التصور العام لبنية الفيروس.

- في هذه الحالة ، شفرة الفيروس (V) ملحقة في مقدمة البرنامج المصاب ، ويُفترض أن نقطة الدخول إلى البرنامج ، عند استدعائه ، هي السطر الأول من البرنامج.

1- البرمجيات الخبيثة : أ - الفيروسات : البنية

- يبدأ البرنامج المصاب ببرنامج الفيروس ويعمل على النحو التالي. السطر الأول من التعليمات البرمجية هو القفزة إلى برنامج الفيروسات الرئيسي.
- السطر الثاني عبارة عن علامة خاصة يستخدمها الفيروس لتحديد ما إذا كان برنامج الضحية المحتمل قد أصيب بالفعل بهذا الفيروس أم لا. عندما يتم استدعاء البرنامج ، يتم نقل التحكم على الفور إلى برنامج الفيروسات الرئيسي. يبحث برنامج الفيروسات أولاً عن الملفات القابلة للتنفيذ غير المصابة ويصيبها.
- بعد ذلك ، قد يقوم الفيروس ببعض الإجراءات ، وعادة ما تكون ضارة بالنظام. يمكن تنفيذ هذا الإجراء في كل مرة يتم فيها استدعاء البرنامج ، أو يمكن أن يكون قنبلة منطقية لا يتم تشغيلها إلا في ظل ظروف معينة.
- أخيرًا ، ينقل الفيروس التحكم إلى البرنامج الأصلي. إذا كانت مرحلة إصابة البرنامج سريعة ، فمن غير المرجح أن يلاحظ المستخدم أي فرق بين تنفيذ برنامج مصاب وغير مصاب.

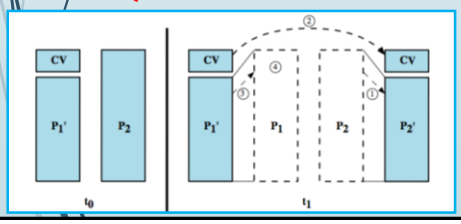
1- البرمجيات الخبيثة : أ - الفيروسات : البنية

```
    program CV :=

{goto main;
    01234567;

    subroutine infect-executable :=
          {loop:
               file := get-random-executable-file;
          if (first-line-of-file = 01234567) then goto loop;
       (1)     compress file;
       (2)     prepend CV to file;
       }

main:   main-program :=
          {if ask-permission then infect-executable;
       (3)     uncompress rest-of-file;
       (4)     run uncompressed file;}
       }
```

ضغط الفيروسات

- يمكن اكتشاف فيروس مثل الفيروس الموصوف سابقا بسهولة لأن النسخة المصابة من البرنامج أطول من النسخة غير المصابة.
- تتمثل إحدى طرق إحباط مثل هذه الوسيلة البسيطة لاكتشاف الفيروس في ضغط الملف القابل للتنفيذ بحيث يكون كل من النسختين المصابة وغير المصابة بطول متطابق. توضح الشفرة في الشكل التالي بشكل عام المنطق المطلوب.

P1 مصاب



1- البرمجيات الخبيثة : أ - الفيروسات : البنية

ضغط الفيروسات

تم ترقيم الخطوط الرئيسية في هذا الفيروس كما ان الشكل السابق يوضح العملية. في هذا المثال ، لا يقوم الفيروس بأي شيء سوى الانتشار. كما في المثال السابق ، قد يحتوي الفيروس على قنبلة منطقية. نفترض أن البرنامج (P1) مصاب بالفيروس (CV) ، وعند استدعاء هذا البرنامج ينتقل التحكم الى الفيروس المصاب به ، والذى سيقوم بالخطوات التالية:

1. كل ملف (P2) غير مصاب يتم العثور عليه ، يقوم الفيروس أولاً بضغط هذا الملف لإنتاج نسخة مضغوطة ، وهي أقصر من البرنامج الأصلي من حيث حجم الفيروس.
2. يتم وضع نسخة من الفيروس في مقدمة البرنامج المضغوط.
3. يفك ضغط النسخة المضغوطة من البرنامج الأصلي المصاب .
4. يتم تنفيذ البرنامج الأصلي غير المضغوط.

1- البرمجيات الخبيثة : أ - الفيروسات : التصنيف

كان هناك سباق تسلح مستمر بين كتاب الفيروسات وكتاب برامج مكافحة الفيروسات منذ ظهور الفيروسات لأول مرة. كلما تم تطوير إجراءات مضادة فعالة للأنواع الموجودة من الفيروسات تم تطوير أنواع جديدة من الفيروسات

يشمل تصنيف الفيروسات **حسب الهدف** ما يلي:

- **مصيبي قطاع الاقلاع**: يوجد لكل نظام تشغيل قطاع في القرص التخزين الصلب ، مخصص لبدء عملية التشغيل (الإقلاع) وهو القطاع الأول، في حالة اصابته فلا يتم تشغيل الحاسوب. فيروسات الإقلاع تصيب قطاع الإقلاع الرئيسي (Boot Sector Viruses)، وينتشر عند إقلاع نظام من القرص الذي يحتوي على الفيروس. وخطورتها تكمن في اصابتها لمكان مهم جدا يتم من خلاله توجيه الحاسوب لتنفيذ البرمجيات التي يجرى من خلالها استكمال تجهيز الحاسوب للعمل و بدلا من ذلك يوجه الفيروس الحاسوب لتنفيذ شفرة خاصة به ومن تم يفشل الحاسوب في عملية الإقلاع ولا يمكنه العمل.
- **مصيبي الملفات**: يصيب الملفات التي يعتبرها نظام التشغيل قابلة للتنفيذ. كذلك يمكن ان تصيب أنواع مختلفة من الملفات، وعادة ما ينتج عن هذه الفيروسات زيادة في احجام الملفات.
- **فيروس الجزئية المكررة (الماكرو)**: و تستخدم البرمجة الجزئية الخاصة بتطبيق معين، مثل معالج الكلمات ، لبدء تشغيلها. وتضرب هذه النوعية من الفيروسات ملفات البيانات، وتظل ساكنة او مقيمة في التطبيق نفسه عن طريق إصابة حقل التهيئة الخاص به. وهى خصوصا تصيب ملفات البيانات ذات التعليمات البرمجية الجزئية والتي يتم تفسيرها بواسطة أحد التطبيقات.
- **متعدد الأجزاء**: يصيب بطرقٍ متعددة، عادةً ما يكون الفيروس متعدد الأجزاء قادرًا على إصابة أنواع متعددة من الملفات ، لذلك يجب القضاء على الفيروس في جميع مواقع الإصابة المحتملة.

1- البرمجيات الخبيثة : أ - الفيروسات : التصنيف

يشمل تصنيف الفيروسات **حسب استراتيجية الإخفاء** ما يلي:

- **فيروس مشفر**: يقوم الفيروس بإنشاء مفتاح تشفير عشوائي ، يتم تخزينه مع الفيروس ، ويقوم بتشفير ما تبقى من الفيروس. عندما يتم استدعاء البرنامج المصاب ، يستخدم الفيروس المفتاح العشوائي المخزن لفك تشفير الفيروس. عندما يتكاثر الفيروس يتم تحديد مفتاح عشوائي مختلف. نظرًا لأن الجزء الأكبر من الفيروس يتم تشفيره بمفتاح مختلف لكل حالة ، فلا يوجد نمط خانات ثنائية ثابت يجب مراقبته.
- **فيروس متخفي**: نوع من الفيروسات مصمم بشكل يمكنه من إخفاء نفسه من الاكتشاف عن طريق برامج مكافحة الفيروسات. وبالتالي ، يتم إخفاء الفيروس بأكمله ، وليس مجرد حمولة. وقد تستخدم تقنيات مثل الضغط لتحقيق ذلك.
- **فيروس متعدد الأشكال**: نوع من الفيروسات يقوم بإنشاء نسخ أثناء التكاثر تكون متكافئة وظيفيًا ولكن لها أنماط خانات ثنائية مختلفة بشكل واضح (الشفرة البرمجية تتغير تمامًا عن شكلها الأصلي عند التنفيذ)، وذلك من أجل هزيمة البرامج التي تفحص الفيروسات. في هذه الحالة ، سيختلف "توقيع" الفيروس مع كل نسخة. لتحقيق هذا الاختلاف ، قد يعمل الفيروس داخليًا بإدراج تعليمات غير ضرورية أو تبادل ترتيب التعليمات المستقلة. الأسلوب الأكثر فعالية هو استخدام التشفير. يتم اتباع استراتيجية فيروس التشفير. يشار إلى جزء الفيروس المسؤول عن إنشاء المفاتيح وتنفيذ التشفير / فك التشفير باسم محرك الطفرات. يتم تغيير محرك الطفرة نفسه مع كل استخدام.
- **الفيروسات المتحولة**: الفيروس المتحول يعيد كتابة نفسه بالكامل عند كل تكرار ، حيث يمكن للفيروسات المتحولة أن تعيد كتابة التعليمات البرمجية الخاصة بها وبالتالي تظهر مختلفة في كل مرة يتم تنفيذها. وذلك عن طريق إنشاء مكافئ منطقي للتعليمات البرمجية الخاصة بها كلما تم تشغيلها. يتحور سلوك ومظهر الفيروس المتحول مع كل إصابة ، مما يزيد من صعوبة اكتشافه.

1- البرمجيات الخبيثة : أ - الفيروسات : الخصائص

هناك عدة خصائص للفيروسات الحاسوبية تميزها عن غيرها من البرمجيات الخبيثة، و تساعدها على الانتشار و إصابة الحواسيب دون علم مستخدميها وهي:

1) **التخفي**: وتعنى القدرة على الارتباط ببرمجيات او ملفات أخرى تبدو سليمة و مألوفة للمستخدم، بحيث يلحق الفيروس نفسه بالملف المصاب خفية ليصبح جزء ا منه، ومن اشهر طرق تخفى الفيروسات ما يلى:
   - التخفي في مرفقات البريد الالكتروني
   - التخفي في الملفات التي يجرى تحميلها من مواقع الانترنت، خاصة تلك التي تشغل ملفات الصوتيات و الفيديو و تتبادلها.
   - التخفي وراء الروابط و الاوامر الموجودة في صفحات الانترنت و البريد الالكتروني.
   - التخفي وراء الروابط و ملفات الإعلانات و البريد الدعائي.
   - التخفي مع البرامج المنسوخة بشكل غير قانوني.
2) **التضاعف**: ويعني ذلك ان ينسخ الفيروس نفسه عدة نسخ تصل الى الملايين في بعض الأحيان، بمعني انه يتكاثر ليصيب اكبر قدر ممكن من الملفات و البرمجيات داخل الحواسيب نفسها و او الأجهزة الأخرى المرتبطة بها. وتبدأ عملية التضاعف عندما يتم تحميل برنامج الفيروس الى ذاكرة الحاسوب و ينفذه المعالج .
3) **الانتشار**: ويعنى انتقال الفيروس من جهاز الى اخر عبر شبكات الحاسوب او وسائط التخزين المختلفة، ومعنى ذلك ان لدى الفيروس القدرة على نقل نفسه عند استثارته او تحفيزه، كتشغيل امر النسخ او عند اكتشاف اتصل الحاسوب المصاب بحاسوب اخر، و من اشهر طرق انتشار الفيروسات ما يلي:
   - تحميل ملفات مصابة من موقع شبكة الانترنت او زيارة مواقع تنشر الفيروسات بشكل تلقائي.
   - فتح مرفقات بريد الكتروني مصابة.
   - ان ينسخ المستخدم ملفات مصابة دون علمه، ويخزنها على وسائط تخزين خارجية تنتشر معها، او يرسلها عبر الشبكة المحلية (كاستخدام المجلدات المشتركة)، فتنتشر عبرها.

1- البرمجيات الخبيثة : أ - الفيروسات : الأعراض

عندما يصاب حاسوب بفيروس فإنه قد تظهر عليه بعض الاعراض الاتية :

- البطء الشديد: يعمل الحاسوب ببطء ملحوظ، و تصبح سرعة البرمجيات المشغلة عليه ابطأ من المعتاد، ومن ذلك ان نظام التشغيل يعمل ببطء شديد عند بداية التشغيل، او عند إيقاف التشغيل، وقد يكون سبب هذا البطء هو النقص الشديد في الذاكرة العشوائية (RAM).
- تعليق (تجميد) الحاسوب: يدخل الحاسوب في حالة من الجمود وعدم الاستجابة لأى امر؛ فلا يمكن في هذه الحالة تشغيل أي برنامج، او حتى إيقاف عمل الجهاز.
- انهيار الحاسوب: في اغلب الأحيان حالات الانهيار تظهر شاشة غريبة (كالشاشات الزرقاء في نظام التشغيل ويندوز)، وعندئذ يتوقف الحاسوب عن العمل.
- إضاءة مصباح القرص الصلب بشكل عشوائي ومتصل وبدون سبب منطقي.
- زيادة احجام الملفات و زيادة الزمن اللازم لفتح الملفات او تشغيل البرمجيات.
- وجود بيانات تالفة كانت صالحة سابقا.
- ظهور رسائل خطأ، ومربعات حوار غير مألوفة و غير متوقعة.
- إعادة تشغيل الحاسوب بشكل تلقائي و مستمر بدون تدخل المستخدم.

1- البرمجيات الخبيثة : ب - الدودة الحاسوبية (Worm)

بينما تعتمد الإصابة بالفيروسات وانتشارها على التدخل البشري، تستخدم دودة الحاسوب ثغرات نظام التشغيل أو التطبيقات للدخول عبر الشبكة واستغلال نقاط الضعف نفسها الموجودة في الأجهزة الأخرى. ودودة موريس (Morris Worm) هي الدودة الحاسوبية الأولى التي ظهرت في عام 1988. وعلى الرغم من أن هذه الدودة تشبه الفيروس، لكن بسبب خطأ في كتابة التعليمات البرمجية أصبح للبرنامج فرصة ثابتة في التكاثر وإنتاج نسخ ُمتعددة من نفسه في الجهاز المصاب ما يؤدي إلى زيادة حمل الجهاز المضيف، وفي نهاية المطاف يؤدي أحياناً إلى تعطل الجهاز المضيف.

فالدودة الحاسوبية هي عبارة عن برنامج مستقل بذاته، وله ملف خاص به، ويعد برنامجا تطبيقيا متكاملا يمكن ان يعمل لوحده و لا يحتاج لان يضيف نفسه لملف اخر. ويمكن للدودة ان تعمل بمفردها و تحمل نفسها الى ذاكرة الحاسوب و تبدأ بالعمل بشكل تلقائي. تم تصميم الدودة لدخول الحاسوب عبر الشبكة ومن ثم الاستفادة من الثغرات الأمنية في أحد التطبيقات أو نظام التشغيل الموجود على الحاسوب المضيف. بمجرد أن تستغل الدودة الثغرة الأمنية في أحد الأنظمة، فإنها تبحث على الفور عن حاسوب آخر على الشبكة لديه نفس الثغرة الأمنية.

ومن الفوارق الاساسية، هي ان الديدان تستخدم الشبكات وروابط الاتصالات لكى تنتشر(تسمى الديدان أحيانًا بالفيروسات الشبكية)، وخلافا للفيروسات لا تلتحم مباشرة بالملفات القابلة للتنفيذ. وهى تصيب الحواسيب المرتبطة بالشبكات المصابة دون تدخل المستخدم او قيامه باستثارتها كفتح ملف معين او تشغيل برنامج، وقد تنتقل الى الحاسوب بمجرد تصفح بعض مواقع الانترنت او بمجرد فتح بريد اليكتروني. برنامج الدودة يتكون من أجزاء تعمل في الحواسيب متفرقة، تتواصل فيما بينها عبر الشبكة، فيمكن ان تجد بدية البرنامج في حاسوب و نهايته في حاسوب اخر بعيد.

والمشكلة هنا ليست الإصابة بالدودة نفسها بل السرعة المرعبة التي تحاول الدودة أن تنشر نفسها. إن إصابة جهاز واحد تؤدي إلى إغراق الشبكة في غضون دقائق مما يؤدي وبشكل فعال إلى خلق **هجوم الحرمان من الخدمة** (Denial of Service Attack) باستخدام كل النطاق الترددي المتاح للشبكة. وتشير التقديرات إلى أنه يمكن إصابة 90% من الخوادم ذات الثغرات على الإنترنت في غضون 10 دقائق من انطلاق الدودة.

1- البرمجيات الخبيثة : ب - الدودة الحاسوبية : الخصائص

لتكرار نفسها و الانتشار، تستخدم الدودة بعض الوسائل للوصول إلى الأنظمة البعيدة عبر الاتصال بالشبكات. وهي تشمل الوسائل التالية، والتي لا يزال معظمها قيد الاستخدام النشط :

- مرفقة بالبريد الإلكتروني أو المراسلة الفورية: تقوم الدودة بإرسال نسخة من نفسها إلى أنظمة أخرى عبر البريد الإلكتروني، أو ترسل نفسها كمرفق عبر خدمة الرسائل الفورية ، بحيث يتم تشغيل الشفرة البرمجية الخاص بها عند استلام البريد الإلكتروني أو مرفقاته أو عرضه.
- مشاركة الملفات: تقوم الدودة بإنشاء نسخة من نفسها أو تصيب ملفات أخرى مناسبة كفيروس على وسائط قابلة للإزالة مثل مشغل (USB)؛ ثم يتم تنفيذه عند توصيل المشغل بنظام آخر باستخدام آلية التشغيل التلقائي عن طريق استغلال بعض نقاط الضعف البرامجية ، أو عندما يفتح المستخدم الملف المصاب على النظام الهدف.
- قدرة التنفيذ عن بعد: تنفذ الدودة نسخة من نفسها على نظام آخر ، إما عن طريق استخدام وسيلة تنفيذ صريحة عن بعد أو عن طريق استغلال خلل برمجي في خدمات الشبكة لتخريب عملياتها.
- إمكانية الوصول إلى الملفات أو نقلها عن بُعد: تستخدم الدودة خدمة الوصول إلى الملفات عن بُعد أو خدمة النقل إلى نظام آخر لنسخ نفسها من نظام إلى آخر ، حيث يمكن للمستخدمين على هذا النظام تنفيذه بعد ذلك.
- إمكانية تسجيل الدخول عن بُعد: تقوم الدودة بتسجيل الدخول إلى نظام بعيد كمستخدم ثم تستخدم أوامر لنسخ نفسها من نظام إلى آخر ، حيث يتم تنفيذها بعد ذلك.

1- البرمجيات الخبيثة : ب - الدودة الحاسوبية : الخصائص

يتم بعد ذلك تشغيل النسخة الجديدة من برنامج الدودة على النظام البعيد حيث يستمر في الانتشار بالإضافة إلى أي مهام اخرى يقوم بها البرنامج على هذا النظام.

تستخدم الدودة عادةً نفس مراحل فيروس الحاسوبية: الخمول ، والانتشار ، والتحفيز ، والتنفيذ. تؤدي مرحلة الانتشار عمومًا الوظائف التالية:

- البحث عن آليات وصول مناسبة للأنظمة الأخرى للإصابة وذلك عن طريق فحص جداول المضيف ، ودفاتر العناوين ، وقوائم الأصدقاء ، والأقران الموثوق بهم ، والمستودعات الأخرى المماثلة لتفاصيل الوصول إلى الانظمة البعيدة؛ من ثم مسح عناوين المستهدفة المحتملة ؛ أو بالبحث عن أجهزة وسائط قابلة للإزالة مناسبة للاستخدام.
- استخدم آليات الوصول التي تم العثور عليها لنقل نسخة منها إلى النظام البعيد ، والتسبب في تشغيل النسخة.

قد تحاول الدودة أيضًا تحديد ما إذا كان النظام قد أصيب مسبقًا قبل نسخ نفسها على النظام. في النظام المتعدد البرامج ، يمكنها أيضًا إخفاء وجودها من خلال تسمية نفسها كعملية نظام أو استخدام اسم آخر قد لا يلاحظه مشغل النظام. يمكن للديدان الأكثر حداثة أن تحقن شفرتها البرمجية في العمليات الحالية على النظام، وتنفذ باستخدام محاور إضافية في تلك العملية ، لإخفاء وجودها بشكل أكبر.

1- البرمجيات الخبيثة : ب - الدودة الحاسوبية : الاستهداف

تتمثل المهمة الأولى في مرحلة الانتشار للدودة الحاسوبية هي البحث عن أنظمة أخرى للإصابة ، وهي عملية تُعرف باسم **المسح**. بالنسبة للديدان المتنقلة ، فهي تستغل الثغرات البرمجية في الخدمات الشبكية التي يمكن الوصول إليها عن بُعد ، لذلك يجب عليها أولا تحديد الأنظمة المحتملة التي تشغل الخدمة التي بها الثغرة، ثم تصيبها. بعد ذلك، عادةً ما تكرر الشفرة البرمجية للدودة المثبت الآن على الأجهزة المصابة نفس عملية المسح ، حتى يتم إنشاء شبكة كبيرة موزعة من الأجهزة المصابة.

هناك عدة انواع من استراتيجيات فحص عناوين الشبكة التي يمكن لمثل هذه الدودة استخدامها، مثل :

- **عشوائي:** يقوم كل مضيف مخترق بالتحقق من عناوين عشوائية لحزمة من عنوانين (IP)، باستخدام بداية مختلفة. تنتج هذه التقنية حجمًا كبيرًا من حركة المرور على الإنترنت، والتي قد تسبب اضطرابًا عامًا حتى قبل بدء الهجوم الفعلي.
- **قائمة الإصابة:** يقوم المهاجم أولاً بتجميع قائمة طويلة من الأجهزة المعرضة للثغرة المحتملة. يمكن أن تكون هذه العملية البطيئة وان تتم على مدى فترة طويلة لتجنب اكتشاف ان هجوم قيد الاعداد. بمجرد تجميع القائمة، يبدأ المهاجم في إصابة الأجهزة الموجودة بالقائمة. يتم تزويد كل جهاز مصاب بجزء من القائمة للمسح. تؤدي هذه الاستراتيجية إلى فترة مسح قصيرة جدًا ، مما قد يجعل من الصعب اكتشاف حدوث العدوى.
- **طوبولوجي:** تستخدم هذه الطريقة المعلومات الموجودة على الجهاز المصاب للعثور على المزيد من الأجهزة المضيفة للمسح.
- **الشبكة الفرعية المحلية:** إذا كان من الممكن إصابة مضيف خلف جدار حماية ، فسيبحث هذا المضيف بعد ذلك عن أهداف في شبكته المحلية. يستخدم المضيف بنية عنوان الشبكة الفرعية للعثور على مضيفين آخرين ممكن ان يكونوا محميين بواسطة جدار الحماية.

1- البرمجيات الخبيثة : ب - الدودة الحاسوبية : التقنيات

التقنيات الحديثة للدودة الحاسوبية : تشمل أحدث تقنيات الدودة ما يلي:

- **متعددة المنصات**: لا تقتصر الفيروسات المتنقلة الحديثة على أجهزة الويندوز لكنها تستطيع مهاجمة مجموعة متنوعة من المنصات ، وخاصة الأنواع الشائعة من يونيكس (UNIX)؛ أو استغلال لغات الماكرو أو البرمجة النصية المدعومة من أنواع شائعة من المستندات.
- **متعددة الاستغلال**: تخترق الديدان الحديثة الأنظمة بعدة طرق ، باستخدام عمليات ضد خوادم الويب والمتصفحات والبريد الإلكتروني ومشاركة الملفات والتطبيقات الأخرى المعتمدة على الشبكات ؛ أو عبر الوسائط المشتركة.
- **فائقة الانتشار**: استغلال التقنيات المختلفة لتحسين معدل انتشار الدودة وذلك بزيادة القدرة على تحديد أكبر عدد ممكن من الأجهزة القابلة للإصابة في فترة زمنية قصيرة.
- **متعددة الأشكال**: لتفادي الاكتشاف وتخطي المرشحات و خداع التحليل في الوقت الحقيقي ، تعتمد الديدان تقنيات متعددة الأشكال للفيروسات. تحتوي كل نسخة من الدودة على شفرة برمجية جديدة يتم إنشاؤها بسرعة باستخدام تعليمات وتقنيات تشفير متكافئة وظيفيًا.
- **المتحولة**: بالإضافة إلى تغيير مظهرها ، تمتلك الديدان المتحولة ذخيرة من أنماط السلوك التي يتم إطلاقها في مراحل مختلفة من التكاثر.
- **الناقلة**: نظرًا لأن الديدان يمكنها اختراق عدد كبير من الأنظمة بسرعة ، فهي مثالية لنشر مجموعة متنوعة من الحمولات الضارة ، مثل روبوتات رفض الخدمة الموزعة ، ومولدات البريد الإلكتروني العشوائي ، وبرامج التجسس.
- **الاستغلال الفوري**: لتحقيق أقصى قدر من المفاجأة والتوزيع ، يجب أن تستغل الدودة ثغرة غير معروفة لم يكتشفها مجتمع الشبكات إلا عند إطلاق الدودة.

1- البرمجيات الخبيثة : ج – برامج احصنة طروادة (Trojan horse)

حصان طروادة هو برنامج مفيد (يرئ ظاهريًا)، أو أداة مساعدة تحتوي على تعليمات برمجية مخفية قابلة للتنفيذ تؤدي عند استدعائها، بعض المهام غير المرغوب فيها أو الضارة.

يمكن استخدام برامج حصان طروادة لإنجاز مهام بشكل غير مباشر حيث لا يستطيع المهاجم إنجازها بشكل مباشر. على سبيل المثال، للوصول إلى معلومات شخصية حساسة مخزنة في ملفات المستخدم ، يمكن للمهاجم إنشاء برنامج حصان طروادة يقوم، عند تنفيذه، بمسح ملفات المستخدم بحثًا عن المعلومات الحساسة المطلوبة وإرسال نسخة منها إلى المهاجم عبر نموذج ويب أو بريد إلكتروني أو رسالة نصية او حتى تدمير عمل الحاسوب المصاب به. يمكن للمهاجم (مؤلف الشفرة البرمجية) بإغراء المستخدمين بتشغيل البرنامج من خلال دمجه في لعبة أو برنامج مساعد مفيد ، وإتاحته عبر موقع توزيع برمجيات معروف أو متجر التطبيقات. فحصان طروادة عبارة عن برنامج قابل للتنفيذ يتنكر في هيئة أداء نشاط حميد ولكنه يقوم أيضًا بنشاط خبيث. مثلا، قد يقوم المستخدم بتنزيل ما تم الإعلان عنه كبرنامج تقويم، ولكن عند تثبيته، بالإضافة إلى تثبيت التقويم، فإنه يقوم أيضًا بتثبيت برامج ضارة تقوم بمسح النظام بحثًا عن أرقام بطاقات الائتمان وكلمات المرور، وتتصل عبر الشبكة بنظام بعيد ، ثم تنقل هذه المعلومات إلى المهاجم.

تم استخدام مثل هذا النهج مؤخرًا مع التطبيقات المساعدة التي "تدعي" أنها أحدث ماسح لمكافحة الفيروسات ، أو تحديث أمني للأنظمة، ولكنها في الواقع عبارة عن أحصنة طروادة ضارة ، وغالبًا ما تحمل حمولات مثل برمجيات التجسس التي تبحث عن بيانات الاعتماد المصرفية. ومن ثم يحتاج المستخدمون إلى اتخاذ الاحتياطات للتحقق من صحة مصدر أي برنامج يقومون بتثبيته.

1- البرمجيات الخبيثة : ج – برامج احصنة طروادة

احصنة طروادة تكون من أحد النماذج الثلاثة:

- الاستمرار في أداء وظيفة البرنامج الأصلي و بالإضافة إلى ذلك تنفيذ نشاط ضار منفصل.
- الاستمرار في أداء وظيفة البرنامج الأصلي مع تعديل وظيفته لأداء نشاط ضار (على سبيل المثال، إصدار برنامج حصان طروادة لبرنامج تسجيل الدخول يجمع كلمات المرور) أو لإخفاء نشاط ضار آخر (على سبيل المثال ، إصدار لبرنامج حصان طروادة لبرنامج استعراض عمليات النظام لا يعرض عمليات معينة ضارة).
- تنفيذ وظيفة ضارة تحل محل وظيفة البرنامج الأصلي تمامًا.

تتجنب بعض أحصنة طروادة تدخل المستخدم من خلال استغلال بعض الثغرات البرامجية وذلك لتثبيت نفسها والتنفيذ التلقائي. وبهذا هي تشترك مع بعض ميزات الدودة الحاسوبية ، لكن عكسها، لا تتضاعف.

من الأمثلة البارزة على مثل هذا الهجوم هو حصان طروادة (Hydraq) المستخدم في عملية (Aurora) في 2009 وأوائل 2010 . استغل هذا الهجوم ثغرة أمنية في (Internet Explorer) لتثبيت نفسه ، واستهدف العديد من الشركات البارزة وتم توزيعه عادةً باستخدام البريد الإلكتروني العشوائي أو عبر موقع ويب مخترق.

مقارنة بالاختلافات بين الفيروسات والدودة الحاسوبية وأحصنة طروادة

الفعل	الفيروس	الدودة الحاسوبية	حصان طروادة
ماذا يعمل ؟	يقوم بإدراج تعليمات برمجية ضارة في برنامج أو ملف بيانات	يستغل ثغرة أمنية في التطبيق أو نظام التشغيل	يتنكر بأداء عمل شرعي وحميد لكنه يقوم أيضًا بعمل شيء خبيث
كيف ينتشر في الحواسيب الأخرى ؟	يقوم المستخدم بنقل الملفات المصابة إلى الأجهزة الأخرى	يستخدم شبكة للانتشار من جهاز حاسوب إلى آخر	المستخدم ينقل ملف الطروادة إلى الحواسيب الأخرى
هل يصيب الملفات ؟	نعم	لا	يمكن
هل يجب أن يكون هناك دور للمستخدم من أجل انتشاره؟	نعم	لا	نعم

1- البرمجيات الخبيثة : هـ – البرامج الدعائية (Adware)

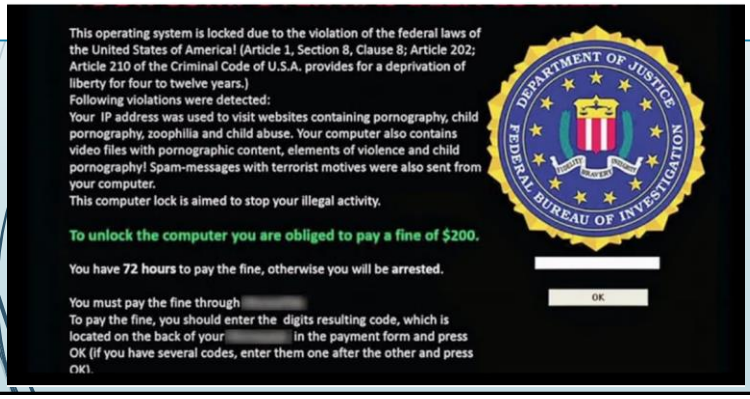
تقدم برامج الإعلانات المتسللة محتوى إعلانيًا بطريقة غير متوقعة وغير مرغوب فيها من قبل المستخدم. بمجرد تثبيت البرامج الضارة، فإنها عادةً ما تعرض لافتات إعلانية أو إعلانات منبثقة أو تفتح نوافذ متصفح ويب جديدة على فترات عشوائية. يرفض المستخدمون عمومًا برامج الإعلانات المتسللة للأسباب التالية:

- قد تعرض برامج الإعلانات المتسللة محتوى غير مرغوب فيه، مثل مواقع المقامرة أو المواد الغير مشروعة.
- يمكن أن تتداخل الإعلانات المنبثقة المتكررة مع إنتاجية المستخدم.
- يمكن أن تؤدي الإعلانات المنبثقة إلى إبطاء الحاسوب و حتى التسبب في حدوث أعطال وفقدان البيانات.
- الإعلانات غير المرغوب فيها يمكن أن تكون مصدر إزعاج.

تتجاوز بعض برامج الإعلانات المتسللة التأثير على عمل المستخدم الخاص على الحاسوب. وذلك لأن برامج الإعلانات المتسللة يمكنها أيضًا أداء وظيفة التتبع، والتي تراقب وتتتبع أنشطة المستخدم عبر الإنترنت ثم ترسل سجلاً بهذه الأنشطة إلى أطراف ثالثة دون إذن المستخدم أو علمه. على سبيل المثال، يمكن تتبع المستخدم الذي يزور مواقع السيارات عبر الإنترنت لعرض أنواع معينة من السيارات بواسطة برامج الإعلانات المتسللة وتصنيفه على أنه شخص مهتم بشراء سيارة جديدة. واستنادًا إلى تسلسل مواقع الويب التي تمت زيارتها ونوعها، يمكن لبرامج الإعلانات المتسللة أيضًا تحديد ما إذا كان سلوك المتصفحين يشير إلى أنهم على وشك إجراء عملية شراء أو أنهم ينظرون أيضًا إلى سيارات المنافسين. يتم جمع هذه المعلومات عن طريق برامج الإعلانات المتسللة ومن ثم بيعها إلى المعلنين عن السيارات، الذين يرسلون للمستخدمين إعلانات عبر البريد العادي حول سياراتهم أو حتى يتصلون بالمستخدم عبر الهاتف.

1- البرمجيات الخبيثة : هـ – برامج الفدية (Ransomware)

أحد أحدث أنواع البرامج الضارة وأسرعها نموًا هو برنامج الفدية. تمنع برامج الفدية جهاز المستخدم من العمل بشكل صحيح حتى يتم دفع الرسوم. يقوم أحد أنواع برامج الفدية بإغلاق الحاسوب الخاص بالمستخدم ثم يعرض رسالة يُزعم أنها واردة من إحدى وكالات إنفاذ القانون. تنص هذه الرسالة، التي تستخدم صورًا ذات مظهر رسمي، على أن المستخدم قام بإجراء غير قانوني مثل تنزيل مواد غير مشروعة ويجب عليه دفع غرامة عبر الإنترنت على الفور عن طريق إدخال رقم بطاقة الائتمان. يظل الحاسوب "رهينة" ومغلقًا (باستثناء المفاتيح الرقمية الموجودة على لوحة المفاتيح) حتى يتم دفع الفدية. يوضح الشكل رسالة برنامج فدية من مركز الاستجابة الأمنية الخاص بموقع (Symantec) الإلكتروني.



1- البرمجيات الخبيثة : هـ – برامج الفدية (Ransomware)

تعد برامج الفدية الضارة مربحة للغاية. ووفقاً لأحد التقديرات، فإن ما يقرب من 3% من هؤلاء المستخدمين المصابين يدفعون الفدية دون أدنى شك، مما يدر ما يقرب من 5 ملايين دولار سنوياً من الضحايا الذين يتم ابتزازهم. نظرًا لمعدل نجاحها المرتفع، بدأ المهاجمون في توسيع قدرات هذه البرامج الضارة. بدلاً من مجرد عرض رسالة على الشاشة، يقوم أحد الأشكال الجديدة لبرامج الفدية بتشغيل رسالة مسجلة من خلال مكبرات صوت الحاسوب باستخدام رسالة صوتية محلية وشبه شخصية.

شكل آخر يعرض تحذيرًا وهميًا بوجود مشكلة في الحاسوب مثل الإصابة بالبرامج الضارة أو فشل وشيك في محرك الأقراص الثابتة. بغض النظر عن حالة الحاسوب، فإن برامج الفدية دائمًا تشير إلى وجود مشكلة. يخبر هذا النوع من برامج الفدية المستخدمين أنه يجب عليهم شراء برامج إضافية عبر الإنترنت على الفور لإصلاح المشكلة التي لا وجود لها في الواقع. يبدو التحذير مشروعًا لأنه يحاكي مظهر البرامج الأصلية ويستخدم علامات تجارية أو أيقونات مشروعة - بشكل غير قانوني. يستخدم مثال برنامج الفدية الموضح في الشكل أنظمة ألوان وأيقونات مشابهة لتلك الموجودة في برامج ويندوز الشرعية. يجد المستخدمون الذين يقدمون رقم بطاقة الائتمان الخاصة بهم لإجراء عملية الشراء أن المهاجمين ببساطة يلتقطون تلك المعلومات ثم يستخدمون رقم البطاقة لأغراضهم الخاصة.

1- البرمجيات الخبيثة : و – القنبلة المنطقية (Logic bomb)

القنبلة المنطقية هي رمز حاسوبي يُضاف عادةً إلى برنامج شرعي ولكنه يظل خاملًا حتى يتم تشغيله بواسطة حدث منطقي محدد. بمجرد تشغيله، يقوم البرنامج بعد ذلك بحذف البيانات أو تنفيذ أنشطة ضارة أخرى. في أحد الأمثلة، حاول أحد موظفي حكومة ولاية ماريلاند تدمير محتويات أكثر من 4000 خادم عن طريق زرع نص قنبلة منطقية كان من المقرر تفعيله بعد 90 يومًا من فصله عن العمل. وهناك امثلة لقنابل منطقية حديثة أخرى رفيعة المستوى كما في الجدول التالي.

من الصعب اكتشاف القنابل المنطقية قبل إطلاقها. وذلك لأن القنابل المنطقية غالبًا ما تكون مضمنة في برنامج حاسوبي كبيرة جدًا، يحتوي بعضها على عشرات الآلاف من أسطر التعليمات البرمجية، ويمكن للموظف الموثوق به بسهولة إدخال بضعة أسطر من تعليمات برمجية في برنامج طويل دون أن يكتشفها أحد. بالإضافة إلى ذلك، لا يتم فحص هذه البرامج بشكل روتيني بحثًا عن احتوائها على إجراءات ضارة.

1- البرمجيات الخبيثة : و – القنبلة المنطقية (Logic bomb)

الوصف	سبب الهجوم	النتائج
قنبلة منطقية تمت زرعتها في شبكة خدمات مالية تسببت بحذف معلومات حساسة في 1000 حاسوب	وقد اعتمد أحد الموظفين الساخطين على هذا الهجوم للتسبب في انخفاض سعر سهم الشركة؛ لقد خطط لاستخدام هذا الحدث لكسب المال.	انفجرت القنبلة المنطقية ولكن تم القبض على الموظف وحكم عليه بالسجن لمدة 8 سنوات وأمر بدفع 3.1 مليون دولار كتعويض.
تم تصميم قنبلة منطقية من قبل أحد مقاولي وزارة الدفاع لحذف بيانات مهمة لمشروع صاروخي.	كانت خطة الموظف هي تعيينه كمستشار بأجر مرتفع لإصلاح المشكلة.	تم اكتشاف القنبلة المنطقية وتعطيلها قبل أن يتم تفعيلها. تم اتهام الموظف بالتلاعب بالحاسوب ومحاولة الاحتيال وتم تغريمه 5000 دولار.
تم إعداد قنبلة منطقية في إحدى شركات الخدمات الصحية للانفجار في عيد ميلاد موظف.	كان الموظف غاضبًا من احتمال تسريحه من وظيفته (رغم أنه لم يحدث ذلك).	حُكم على الموظف بالسجن لمدة 30 شهرًا في سجن فيدرالي ودفع 81200 دولار كتعويض للشركة.

1- البرمجيات الخبيثة : ي – الروبوتات الشبكية (Bots)

الروبوتات الشبكية هي برمجيات ذات استخدام عام، وتكون مثل القشور الخارجية الفارغة، تتصل بخادم الأوامر والتحكم (Command and Control server) من أجل تنفيذ أوامره. ويستخدم الروبوت الشبكي (ZeroAccess) الشبكات المشابهة لشبكة النظراء (peer-to-peer) لتنزيل الإضافات من خوادم الأوامر والتحكم . وتقوم هذه الإضافات بتنفيذ المهام المصممة لمنفعة مشغلي الروبوتات. ومن اشهر هذه المهام : احتيال النقر(Click Fraud)، والتنقيب عن عملة بت كوين (Bitcoin Mining). أحد أشهر ألروبوتات الشبكية التي تم اكتشافها تعرف باسم (ZeroAccess). وتشير التقديرات في عام 2012 إلى أن البرمجيات الخبيثة المعروفة باسم (ZeroAccess) قد جرى تحمليها ملايين المرات.

ويحدث احتيال النقر عند الارتباط بالأعمال التي تستخدم نموذج الاعلانات المعروف بالدفع حسب عدد النقرات (Pay Per Click). وبشكل عام الدوافع تختلف. وعادة ما يتم توظيف قراصنة الحاسب الآلي في محاولة لتجفيف ميزانية الدعاية للمنافسين. والجناة الأكثر شيوعاً هم الناشرون الذين نجحوا في السابق في إدارة هذا النوع من الاحتيال.

ويمكن وصف عملة الإنترنت بت كوين بأنها العملة الافتراضية الجديدة التي تحل محل النقود في شبكة الإنترنت. وبشكل مشابه للبنك المركزي المسؤول عن تنظيم العملة النقدية فإنه يتم تفويض تنظيم عملة البت كوين إلى شبكة النظراء والتي تتألف من أجُهزة حاسب آلي تعمل كعميل البت كوين، أو ما يعرف (تنقيب البت كوين) وعندما تقوم بتثبيت (عميل البت كوين) على جهازك فإن الجهاز يعمل بشكل أساسي كأنه بنك بت كوين (Bitcoin bank) يقوم بإصدار العملة والتأكد من صحة المعاملات وغيرها. ويصبح الأفراد عادة جزءاً من مجموعة التنقيب (mining pool) ويحصلون على تعويضات بت كوين (payout bitcoins) كجزء من سدادهم للمدفوعات. ومن الواضح أن الروبوتات الشبكية مناسبة جداً لهذا النشاط.

1- البرمجيات الخبيثة : ي – الروبوتات الشبكية : الاستخدامات

للروبوتات استخدامات عديدة اخرى، منها:

1) هجمات الحرمان من الخدمة الموزع (DDoS): هجوم (DDoS) هو عبارة عن هجوم على نظام حاسوبي أو شبكة يؤدي إلى فقدان الخدمة للمستخدمين.
2) البريد الإلكتروني العشوائي: بمساعدة الروبوتات والآلاف من الروبوتات، يستطيع المهاجم إرسال كميات هائلة من البريد الإلكتروني الجماعي (البريد العشوائي).
3) تقصي حركة المرور: يمكن للروبوتات أيضًا استخدام أداة لتشمم حزم البيانات ومشاهدة بيانات نصية واضحة ومثيرة للاهتمام تمر عبر الجهاز المخترق. يتم استخدام التشمم في الغالب لاستراق المعلومات الحساسة مثل أسماء المستخدمين وكلمات المرور.
4) تسجيل نقرات المفاتيح (الازرار): إذا كان الجهاز المخترق يستخدم قنوات اتصال مشفرة (مثل (HTTPS) أو (POP3S)) فإن مجرد التقاط حزم الشبكة على حاسوب الضحية يكون عديم الفائدة لأن المفتاح المناسب لفك تشفير الحزم مفقود. ولكن باستخدام برنامج تسجيل نقرات المفاتيح ، الذي يلتقط ضغطات المفاتيح على الجهاز المصاب ، يمكن للمهاجم استراق المعلومات الحساسة.
5) نشر برامج خبيثة جديدة: تُستخدم شبكات الروبوت لنشر برامج روبوت جديدة. هذا سهل للغاية نظرًا لأن جميع برامج الروبوت تنفذ آليات لتنزيل ملف وتنفيذه عبر (HTTP) أو (FTP). وتسمح شبكة الروبوتات التي تحتوي على 10000 مضيف وتعمل كقاعدة بداية لدودة أو فيروس بريدي بالانتشار بسرعة كبيرة وبالتالي تسبب المزيد من الضرر.

1- البرمجيات الخبيثة : ي – الروبوتات الشبكية : الاستخدامات

6) تثبيت الوظائف الإضافية للإعلان وكائنات مساعدة للمستعرض: يمكن أيضًا استخدام شبكات الروبوت للحصول على مزايا مالية. يعمل هذا عن طريق إنشاء موقع ويب مزيف مع بعض الإعلانات: يقوم مشغل موقع الويب هذا بالتفاوض بشأن صفقة مع بعض شركات الاستضافة التي تدفع مقابل النقرات على الإعلانات. بمساعدة الروبوتات ، يمكن أن تكون هذه النقرات "تلقائية" بحيث تنقر على الفور بضعة آلاف من الروبوتات على النوافذ المنبثقة. يمكن تحسين هذه العملية بشكل أكبر إذا قام الروبوت باختطاف صفحة البداية لجهاز مخترق بحيث يتم تنفيذ "النقرات" في كل مرة يستخدم فيها الضحية المتصفح.
7) مهاجمة شبكات دردشة (IRC) : تُستخدم شبكات الروبوتات أيضًا لشن هجمات ضد شبكات الدردشة (Internet Relay Chat). يعتبر ما يسمى بهجوم الاستنساخ شائعًا بين المهاجمين بشكل خاص؛ في هذا النوع من الهجوم ، يأمر جهاز التحكم كل روبوت بربط عدد كبير من النسخ بشبكة الدردشة للضحية. تغمر الضحية طلبات الخدمة من آلاف الروبوتات أو الآلاف من القنوات التي تنضم إليها هذه الروبوتات المستنسخة. بهذه الطريقة ، يتم إسقاط شبكة الدردشة الخاصة بالضحية ، على غرار هجوم (DDoS).
8) التلاعب في استطلاعات الرأي / الألعاب عبر الإنترنت: تحظى استطلاعات الرأي / الألعاب عبر الإنترنت باهتمام متزايد ومن السهل إلى حد ما التلاعب بها باستخدام شبكات الروبوت. نظرًا لأن كل روبوت له عنوان (IP) مميز ، فسيكون لكل صوت نفس مصداقية التصويت الذي يدلي به شخص حقيقي. يمكن التلاعب بالألعاب عبر الإنترنت بطريقة مماثلة.

1- البرمجيات الخبيثة : د – المكافحة : اساليب الإجراءات المضادة

الحل الأمثل لتهديد البرامج الخبيثة هو الوقاية: لا تسمح للبرامج الخبيثة بالدخول إلى النظام في المقام الأول ، أو تمنع قدرتها على تعديل النظام. وبشكل عام هذا الهدف يكاد يكون من المستحيل تحقيقه، على الرغم من أن اتخاذ الإجراءات المضادة المناسبة لتقوية الأنظمة والمستخدمين في منع الإصابة يمكن أن يقلل بشكل كبير من عدد هجمات البرامج الخبيثة الناجحة. ويقترح أربعة عناصر رئيسية للوقاية: **السياسة ، والتوعية ، وتقليل الثغرات ، وتقليل التهديدات.**

ان توفر سياسة مناسبة لمنع البرامج الخبيثة يعتبر أساسًا لتنفيذ الإجراءات الوقائية المناسبة.

أحد الإجراءات المضادة الأولى التي يجب استخدامها هو التأكد من أن جميع الأنظمة محدثة قدر الإمكان، مع تطبيق جميع التصحيحات و ذلك من أجل تقليل عدد الثغرات الأمنية التي يمكن استغلالها على النظام.

الخطوة التالية هي وضع ضوابط وصول مناسبة على التطبيقات والبيانات المخزنة على النظام ، لتقليل عدد الملفات التي يمكن لأي مستخدم الوصول إليها ، وبالتالي من المحتمل أن تتسبب في إصابة أو تلف نتيجة تنفيذ بعض شفرات البرمجيات الخبيثة. وتستهدف هذه الإجراءات بشكل مباشر آليات الانتشار الرئيسية التي تستخدمها الديدان والفيروسات وبعض أحصنة طروادة.

ثالثا، يمكن مواجهة آلية الانتشار الشائعة والتي تستهدف المستخدمين في هجوم الهندسة الاجتماعية باستخدام التوعية و التدريب المناسبين للمستخدمين. يهدف هذا إلى اعداد المستخدمين ليكونوا أكثر وعياً بهذه الهجمات، وأقل احتمالية لاتخاذ إجراءات تؤدي إلى تسوية غير مشروعة.

1- البرمجيات الخبيثة : د – المكافحة : اساليب الإجراءات المضادة

في حالة فشل المنع ، يمكن استخدام الآليات التقنية التالية لدعم خيارات التقليل من حدة التهديدات :

- **الكشف**: بمجرد حدوث الإصابة ، حدد الاصابة وحدد موقع البرنامج الخبيث.
- **التعرف**: بمجرد تحقيق الاكتشاف ، حدد نوع البرامج الخبيثة التي أصابت النظام.
- **الإزالة**: بمجرد التعرف على البرامج الخبيثة وتحديدها ، قم بإزالة جميع آثار فيروسات البرامج الخبيثة من جميع الأنظمة المصابة حتى لا تنتشر أكثر. إذا نجح الاكتشاف ولكن لم يتم تحديد الهوية أو الإزالة ، فإن البديل هو تجاهل أي ملفات مصابة أو ضارة وإعادة تحميل نسخة احتياطية نظيفة. في حالة بعض الإصابات السيئة بشكل خاص، قد يتطلب ذلك مسحًا كاملاً لكل وسائط التخزين ، وإعادة بناء النظام المصاب من الوسائط النظيفة معروفة.

بعض **متطلبات الإجراءات الفعالة لمكافحة البرامج الخبيثة**:

- **العمومية**: يجب أن يكون الاسلوب المتبع قادرًا على التعامل مع مجموعة متنوعة من الهجمات.
- **حسن التوقيت**: يجب أن يستجيب الاسلوب بسرعة للحد من عدد البرامج أو الأنظمة المصابة وما يترتب على ذلك من نشاط .
- **المرونة**: يجب أن يكون الأسلوب مقاومًا لتقنيات التهرب التي يستخدمها المهاجمون لإخفاء وجود برامجهم الضارة.
- **الحد الأدنى من تكاليف تعطيل الخدمة**: يجب أن يؤدي هذا الاسلوب إلى الحد الأدنى من تقليل السعة أو الخدمة بسبب إجراءات برنامج الإجراءات المضادة ، ويجب ألا يؤدي إلى تعطيل التشغيل العادي بشكل كبير.
- **الشفافية**: يجب ألا تتطلب برامج وأجهزة الإجراء المضاد تعديل أنظمة التشغيل (القديمة) والتطبيقات البرمجية والأجهزة.
- **التغطية العالمية والمحلية**: يجب أن يكون الاسلوب قادرًا على التعامل مع مصادر الهجوم من خارج شبكة المؤسسة وداخلها.

غالبًا ما يتطلب تحقيق كل هذه المتطلبات استخدام اساليب متعددة في استراتيجية دفاعية متعمقة.

يمكن أن يحدث الكشف عن وجود برامج خبيثة في عدة مواقع. فقد يحدث ذلك في النظام المصاب ، حيث يتم تشغيل بعض برامج "مكافحة الفيروسات"، ومراقبة البيانات المستوردة إلى النظام ومراقبة تنفيذ البرامج التي تعمل على النظام. أو قد يحدث ذلك كجزء من آليات الأمن المحيط المستخدمة في أنظمة جدار الحماية وكشف التسلل (IDS) للمؤسسة. أخيرًا ، قد يستخدم الاكتشاف الآليات الموزعة التي تجمع البيانات من كل من أجهزة الاستشعار على المضيف والمستشعرات المحيطية، على الأرجح عبر عدد كبير من الشبكات والمؤسسات ، من أجل الحصول على عرض أوسع نطاق لحركة البرامج الضارة.

1- البرمجيات الخبيثة : د – المكافحة : التقنيات

يمكن مكافحة البرامج الضارّة باستخدام حزمة برامج واحدة لمكافحة كل من الفيروسات والديدان وأحصنة طروادة في آن واحد؛ لذا لا بدّ من تثبيت برنامج مكافحة جيّد وتحديثه دوريًّا لتوفير الحماية المطلوبة. ولا بدّ أن تشتمل برامج الحماية ليس فقط على كشف الإصابات فقط، وإنّما إزالتها أيضًا، وهناك عدّة برامج(أو حزم) مشهورة لمكافحة البرامج الضارّة يمكن الاعتماد عليها، ومن أشهرها:

- حزمة برامج مكافي(McAfee).
- حزمة برامج سيمانتك(Symantec).
- حزمة برامج كاسبر سكاي(Kasper SKY).
- حزمة برامج نورتون(NORTON).
- وفي جميع الحالات لا بدّ من اتّباع الخطوات الآتية للحصول على مكافحة جيدة:
- تحديث برنامج المكافحة آليًّا ودوريًّا لضمان كشف الفيروسات والديدان وأحصنة طروادة الحديثة ومنعها.
- تحديث نظام التشغيل آليًّا ودوريًّا عن طريق تنشيط خاصية التحديث التلقائي لسد الثغرات الأمنيّة عند ظهورها.

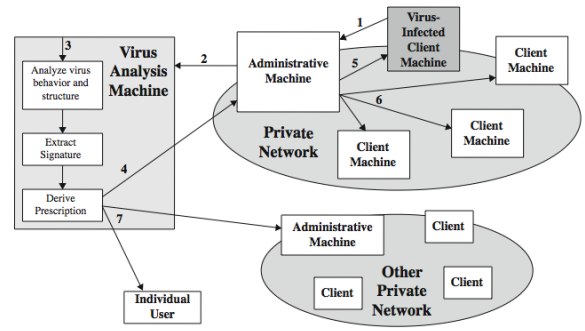
1- البرمجيات الخبيثة : د – المكافحة : التقنيات

- تحميل ملفات الإصلاح الأمنيّة الخاصة بأنظمة التشغيل وبعض البرامج التطبيقيّة الأخرى،(كحزمة برامج الأوفيس) التي تصدرها الشركات المصنّعة(كشركة مايكروسوفت) بشكل مستقلّ لسدّ ثغرة أمنيّة خاصّة لم يتم سدها من خلال التحديث التلقائي، وكذلك تحميل حزم الخدمة(Service Pack) الجديدة حال ظهورها.
- عدم فتح مرفقات البريد الإلكتروني التي لها الامتدادات التشغيليّة مثل:(scr) (exe vbs)، أو التي لها أكثر من امتداد مثل(txt.vbs).
- ويمكن أن تعمل برامج المكافحة بإحدى الطرق الآتية أو جميعها:
- باستخدام جدول زمني معيّن يحدّد من خلاله عمل برنامج المكافحة؛ ليبدأ بفحص جميع مكوّنات الجهاز عند أوقات محدّدة(عند منتصف الليل من كل يوم مثلًا).
- عند الطلب من قبل المستخدم، ويمكن أن يكون ذلك في أيّ وقت.
- عند تشغيل البرامج أو فتح الملفّات أيًّا كان نوعها، وفي هذه الحالة يفحص برنامج المكافحة الملف المراد فتحة قبل أن تتم عمليّة الفتح الفعليّة؛ للتأكد من خلوّه من الفيروسات والديدان وأحصنة طروادة، ومن الأفضل تفعيل جميع هذه الطرق لتوفير حماية أفضل وأشمل.

1- البرمجيات الخبيثة : نظام المناعة الرقمي

نظام المناعة الرقمي هو نهج شامل للحماية من الفيروسات طورته شركة IBM وصقلته لاحقًا شركة (Symantec). الهدف من هذا النظام هو توفير وقت استجابة سريع بحيث يمكن القضاء على الفيروسات بمجرد دخولها.

عندما يدخل فيروس جديد إلى نظام ما ، يلتقطه النظام المناعي تلقائيًا ويحلله ويضيف الكشف والوقاية منه ويزيله ويمرر معلومات حول هذا الفيروس إلى أنظمة أخرى بحيث يمكن اكتشافه قبل السماح له بالعمل في مكان آخر ، كما يوضح الشكل:



IBM/Symantec Project

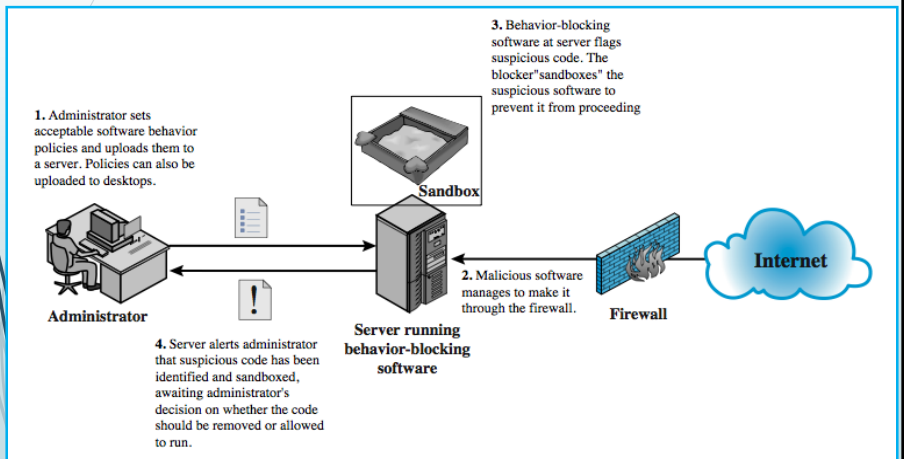
1- البرمجيات الخبيثة : نظام المناعة الرقمي

1. يستخدم برنامج المراقبة على كل حاسوب مجموعة متنوعة من الأساليب التجريبية لاستنتاج وجود فيروس ، ويعيد توجيه نسخة إلى جهاز مشرف النظام.
2. يقوم حاسوب مشرف النظام بتشفير الفيروس وإرساله إلى حاسوب تحليل الفيروسات المركزي.
3. ينشئ هذا الجهاز بيئة يمكن فيها تشغيل البرنامج المصاب بأمان للتحليل. ثم يصدر حاسوب تحليل الفيروسات وصفة طبية لتحديد الفيروس وإزالته.
4. يتم إرسال الوصفة الطبية الناتجة إلى حاسوب المشرف.
5. يقوم حاسوب المشرف بإرسال الوصفة الطبية إلى العميل المصاب.
6. يتم إرسال الوصفة الطبية أيضًا إلى عملاء آخرين في النظام.
7. يتلقى المشتركون في جميع أنحاء العالم تحديثات منتظمة لمكافحة الفيروسات لحمايتهم من الفيروسات الجديدة.

يعتمد نجاح جهاز المناعة الرقمي على قدرة حاسوب تحليل الفيروسات على اكتشاف سلالات فيروسية جديدة ومبتكرة. من خلال التحليل المستمر للفيروسات الموجودة في بيئة العمل ومراقبتها ، يجب أن تكون هناك امكانية تحديث برمجيات المناعة الرقمية باستمرار لمواكبة التهديدات.

1- البرمجيات الخبيثة : برنامج حظر السلوك

برنامج حظر السلوك هو متكامل مع نظام تشغيل الحاسب المضيف ويراقب سلوك البرنامج في الوقت الفعلي بحثًا عن الإجراءات الضارة. يقوم برنامج حظر السلوك بعد ذلك بحظر الإجراءات التي يحتمل أن تكون ضارة قبل أن تؤثر على النظام.



1- البرمجيات الخبيثة : برنامج حظر السلوك

يمكن أن تشمل السلوكيات المراقبة

- محاولات فتح الملفات وعرضها وحذفها و / أو تعديلها ؛
- محاولات تهيئة محركات الأقراص وعمليات القرص الأخرى غير القابلة للاسترداد ؛
- تعديلات على منطق تنفيذ الملفات أو وحدات الماكرو ؛
- تعديل إعدادات النظام الهامة ، مثل إعدادات بدء التشغيل ؛
- برمجة عملاء البريد الإلكتروني والمراسلة الفورية لإرسال محتوى قابل للتنفيذ ؛
- بدء اتصالات الشبكة.

يوضح الشكل عملها. يتم تشغيل برنامج حظر السلوك على أجهزة حاسوب الخادم وسطح المكتب ويتم توجيهه من خلال السياسات التي وضعها مسؤول الشبكة للسماح بتنفيذ الإجراءات الحميدة ولكن للتدخل عند حدوث إجراءات غير مصرح بها أو مشبوهة. تمنع الوحدة أي برامج مشبوهة من التنفيذ. يعزل برنامج الحظر البرنامج المنفذ في وضع الحماية ، مما يقيد وصوله ال إلى موارد وتطبيقات نظام التشغيل المختلفة. ثم يرسل برنامج الحظر التنبيه. نظرًا لأن أداة حظر السلوك يمكنها حظر البرامج المشبوهة في الوقت الفعلي ، فإنها تتمتع بميزة على تقنيات الكشف عن الفيروسات الراسخة مثل البصمات أو الاستدلال. حظر السلوك وحده له حدود. نظرًا لأنه يجب تشغيل الشفرة الخبيثة على الجهاز الهدف قبل التعرف على جميع سلوكياتها ، فقد تتسبب في حدوث ضرر قبل اكتشافها وحظرها.

2 - برمجيات التجسس:- (Spyware)

لقد عُرفت فيروسات الحاسب الآلي بصـورة موسعة في أواخر الثمانينيّات. فهي كائنات غريبة ولافتة للنظر، وفي كل مرة يوجّه الفيروس ضرباته يكـون هو موضوع الأخبار، خاصّة إذا انتشـر بسرعة. وخلال السنوات القليلة الماضية ظهرت فئـة جديدة من البرامج الماكرة هي برامج التجسّس، وبرنامج التجسّس ليس بفيروس، لكن فعله أقوى وأخطر من الفيروسات والديدان وأحصنة طروادة. فبالرغم من عدم تسببه في تلف البيانات، إلا أنه يفعل فعله من وراء الكواليس بكل هدوء، ودون علم المستخدم، وينقل المعلومات لمالكه. وبرنامج التجسّس هو عبارة عن خدعة ماكرة، مثله في ذلك مثل الفيروس، لكنه عمومًا أقل شهرة.

على الرغم من الجدل الذي يكتنف تعريف برنامج التجسّـس الدقيق، إلا أنّه في النهاية كائن(إلكتروني) يتجسّس عليك، ونتيجة لذلك يتركز الجانب المهم من موضوع برنامج التجسّس عادةً حول مسألة الخصوصيّة. ويُعـدُّ تعريف ويبوديا[٢] لبرنامج التجسّـس أفضل التعريفات الموجودة، حيث عرّفه بأنه: «أيّ برنامج يحصل –سرًّا– على معلومات عن المستخدم عن طريق الربط بالإنترنت، وخاصة بدعاوى دعائية وإعلانيـة». عادةً ما يتم تضمين برامج التجسّس في شكل مكوّنات مجانيّة خفية، أو برامج مشاركة يمكن تنـزيلها من شبكة الإنترنت، وبمجرّد تركيب برنامج التجسّس يبدأ بمراقبة حركة المستخدم علـى الإنترنت، وينقل المعلومات من وراء الكواليس لجهة أخرى.

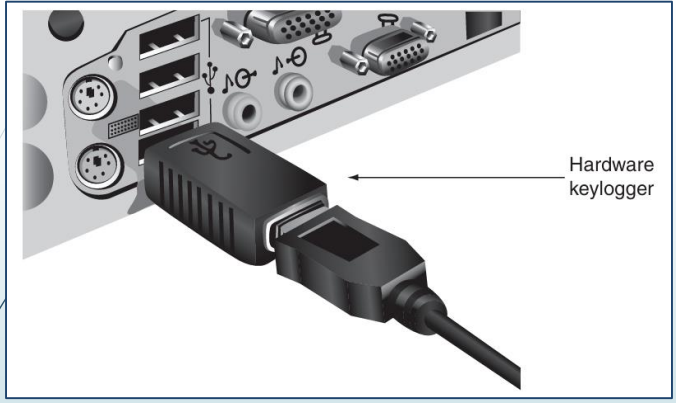
2 – برامج التجسس (Spyware)

برامج التجسس هو مصطلح عام يستخدم لوصف البرامج التي تتجسس سرًا على المستخدمين من خلال جمع المعلومات دون موافقتهم. يُعرّف برامج التجسس بأنها برامج تتبع يتم نشرها دون إشعار أو موافقة أو سيطرة كافية من قبل المستخدم. يستخدم هذا البرنامج موارد الحاسوب، بما في ذلك البرامج المثبتة بالفعل على الحاسوب، بغرض جمع وتوزيع المعلومات الشخصية أو الحساسة.

أحد أنواع برامج التجسس الشائعة هو برنامج **مسجل المفاتيح** (Keylogger) الذي يلتقط ويخزن بصمت كل ضغطة مفتاح يضغطها المستخدم على لوحة مفاتيح الحاسوب. يقوم المهاجم بعد ذلك بالبحث في النص الذي تم التقاطه عن أي معلومات مفيدة مثل كلمات المرور أو أرقام بطاقات الائتمان أو المعلومات الشخصية.

يمكن أن يكون برنامج **مسجل المفاتيح** عبارة عن جهاز صغير (مادي) أو برنامج، **مسجل المفاتيح المادي** (**كمحول** مثلا)، يتم إدخال برنامج مسجل المفاتيح المادي بين اتصال لوحة مفاتيح الحاسوب ومنفذ USB ، كما هو موضح في الشكل. ونظرًا لأن المحول يشبه قابس لوحة مفاتيح عاديًا، كما أن منفذ USB للوحة مفاتيح الحاسوب غالبًا ما يكون موجودًا في الجزء الخلفي من الحاسوب، فمن الممكن بسهولة عدم اكتشاف مسجل المفاتيح المادي. بالإضافة إلى ذلك، فإن المحول بعيدًا عن متناول برنامج فحص البرامج الضارة للحاسوب، وبالتالي لا يثير أي إنذارات. يعود المهاجم الذي قام بتثبيت برنامج مسجل المفاتيح المادي في وقت لاحق ويقوم بإزالة الجهاز فعليًا من أجل الوصول إلى المعلومات التي جمعها.

2 – برامج التجسس (Spyware)



مسجل المفاتيح البرمجي هو برامج مثبتة على الحاسوب يلتقط المعلومات الحساسة بصمت. يعمل مسجل المفاتيح البرمجي مثل الجذور الخفية وتخفي نفسها بحيث لا يمكن للمستخدم اكتشافها. تتمثل ميزة مسجل المفاتيح البرمجي في أنها لا تتطلب الوصول الفعلي إلى حاسوب المستخدم كما هو الحال مع مسجل المفاتيح المادي (المحول). يمكن للبرنامج، الذي يتم تثبيته غالبًا على شكل حصان طروادة أو عن طريق فيروس، إرسال المعلومات التي تم التقاطها بشكل روتيني إلى المهاجم من خلال اتصال الكمبيوتر بالشبكة (الانترنت).

2 - برمجيات التجسس:- الانواع

كما رأينا في تعريف برامج التجسّس، فهي برامج خطيرة تتسلل إلى الحواسيب وتعرف المعلومات الخاصة والسِّريّة المخزّنة بها، وربما ترسلها إلى أجهزة أخرى بمجرد توفر خط الاتصال، وبناءً على طريقة عملها، يمكن تصنيف برامج التجسّس إلى نوعين رئيسين: برامج رصد وتسجيل، وبرامج تتبع.

النوع المعروف من برامج الرصد والتسجيل هو مسجل أو راصد المفاتيح (من لوحة المفاتيح) وحركات الفأرة. فهو يعمل في صمت في الخلف ويقوم بتسجيل ضغطات المفاتيح وحركات الفأرة لكي يعيد ترتيب وتكوين ما يفعله المستخدم، وهذه الطريقة شديدة الخطورة، إذ يمكن من خلالها معرفة الأرقام السِّريّة أو الأرقام الخاصة التي يُدخلها المستخدم عبر لوحة المفاتيح. وخلافًا لراصد عمل المفاتيح، هناك أيضًا راصدات ومسجلّات للبريد الإلكتروني والدردشة. وراصدات عمل المفاتيح مشهورة؛ لأنّها هي أكثر الأنواع شيوعًا وإزعاجًا في عمليّة سرقة كلمات السر وأرقام بطاقات الائتمان.

أمّا المتتبّعات فتراقب عادات الاستخدام وأنماطه وتخزّنها كبيانات إحصائيّة بهدف إعداد التقارير بناءً عليها. وقد تكون البيانات عبارة عن عادات التصفح للشخص المستهدف، مثل استخدام برنامج معيّن أو خاصية محدّدة في ذلك البرنامج. ويتم تجميع هذه المعلومات عن الشخص الضحية ثم تحليلها واستخدامها في الهجوم عليه أو سرقة معلوماته.

2 - برامج التجسس:- التقنيات المستخدمة

التقنية	الوصف	التأثير
برامج التحميل التلقائي	تستخدم لتنزيل البرامج وتثبيتها دون تدخل المستخدم.	ربما تستخدم لتثبيت التطبيقات غير المصرح بها.
تقنيات التتبع السلبي	تستخدم لجمع معلومات حول أنشطة المستخدم دون تثبيت أي برنامج.	قد تجمع معلومات خاصة مثل مواقع الويب التي زارها المستخدم.
برامج تعديل النظام	تعديل أو تغيير تكوينات المستخدم، مثل الصفحة الرئيسية لمتصفح الويب أو صفحة البحث أو مشغل الوسائط الافتراضي أو وظائف النظام ذات المستوى الأدنى.	يقوم بتغيير التكوينات إلى الإعدادات التي لم يوافق عليها المستخدم.
برامج التتبع	يُستخدم لرصد ومراقبة سلوك المستخدم أو جمع معلومات عنه، بما في ذلك في بعض الأحيان معلومات تعريف شخصية أو معلومات حساسة أخرى.	قد تجمع معلومات شخصية يمكن مشاركتها على نطاق واسع أو سرقتها، مما يؤدي إلى الاحتيال أو سرقة الهوية.

2 - برمجيات التجسس:- طريقة العمل

فنيًّا لا يصنف برنامج التجسّس كفيروس، ولذلك لا يمكن مكافحته بشكل كامل من خلال البرامج المصمّمة لمكافحة الفيروسات. وعلى وجه التحديد تُتلف الفيروسات البيانات على جهاز الحاسب الآلي وتنسخ نفسها ذاتيًّا، في حين تعمل برامج التجسّس خلسة، ولا تتلف البيانات، بل تتجسّس عليها. ويمكن لبرامج التجسّس أن تنسخ نفسها على الجهاز وتعمل كمهمة خلفية، ثم تنقل المعلومات السِّريّة الخاصة بالمستخدم لمالكها دون علم المستخدم.

لدى برنامج التجسّس مكوّنان أساسيّان: ففي الواجهة الأمامية هو برنامج عادي يعمل في العلن، ويوفر وظائف مفيدة، بينما هو في الخلف برنامج تجسّس يراقب وينقل المعلومات. ويمكن لبرنامج التجسّس البقاء في أيّ صورة أو شكل من أشكال البرامج القابلة للتنفيذ، بما في ذلك التطبيقات مثل (ActiveX. Plug-in)، أو أكواد (Applets).

عادة لا تجمع برامج التجسّس المعلومات الشخصيّة فقط، لكن بالإضافة إلى ذلك تجمّع المعلومات الديموغرافية وعادات التصفح. ومن المحتمل أن تباع هذه المعلومات المتحصل عليها، أو أن تضاف لقواعد البيانات الأخرى لبناء سجلّات عن المستخدم وعادات استخدامه، وعن طريق ربطها بالبيانات الشخصية، مثل: الاسم والعنوان وعنوان البريد الإلكتروني والعمر والجنس والدخل وتاريخ الائتمان، قد تكون من أقوى وسائل التسويق. ومن الطبيعي أن يكون

2 - برمجيات التجسس:- طريقة العمل

لها بعض الأعراض، ومنها:

- نشاط أعلى من الحد المعتاد: ويتضح ذلك أكثر عندما يرسل الحاسب الآلي ويستقبل كميّات كبيرة من البيانات عبر الشبكة أو الإنترنت، في حين أن المستخدم لا يستخدم أيّ برامج تستوجب ذلك، ويمكن ملاحظة ذلك عن طريق مراقبة عمل جهاز المودم وعرض كميّة البيانات التي أرسلها واستقبلها.
- طلب الاتصال بالإنترنت تلقائيًا: وتظهر هذه الحالة في الأجهزة التي لا يوجد بها جهاز مودم (Digital Subscriber Line-DSL)، حيث يشغّل برنامج التجسّس طلب الاتصال الهاتفي من أجل الارتباط بالإنترنت.
- ظهور أشرطة أدوات غير مألوفة تُضاف إلى متصفّح الإنترنت.
- اختيار صفحة بداية لمتصفّح الإنترنت خلاف الصفحة التي تم ضبط المتصفّح عليها من قبل المستخدم.

ومن أشهر الطرق التي تنتقل بها برامج التجسّس طريقتان، هما:

- تظهر كأنها برامج عادية حتى يتم تثبيتها من قبل المستخدم وبعلمه.
- الاختفاء في برامج أخرى، بحيث يجري تثبيتها مع هذه البرنامج دون علم المستخدم.

2 - برامج التجسس:- المكافحة

من أخطر ما تفعله برامج التجسّس هو أنها تُزيل برامج مكافحة التجسّس. ويمكن القول إنّه ليس هناك برنامج يحمي من برامج التجسّس بدرجة كاملة، لكن يمكن أخذ بعض التدابير الوقائية، ومنها:

- مصفيات خاصية استرجاع البيانات
- حاجبات الاعلانات و النوافذ المنبثقة
- استخدام مضادات برامج التجسس
- استخدام جدار النار الشخصي و برامج كشف التطفل
- تأمين متصفح الانترنت
- تأمين ادخال كلمات المرور

3 – أمن انظمة التشغيل و الملفات

هناك أربعة عناصر رئيسة يمكن من خلالها تحقيق الحد الأدنى لأمن أنظمة التشغيل والملفّات، وهي:

١. التحقّق من الهُوِيّة: يتطلب ذلك أن تكون أصول أجهزة الحاسب الآلي(أنظمة التشغيل، والملفّات، والأجهزة نفسها) قادرة على التحقّق من هويّة المستخدم، ومن هويّة البرامج والبيانات.

٢. السِّريّة: وتتطلب أن يكون الدخول إلى أنظمة الحاسب الآلي والبيانات المخزّنة بها من قبل الجهات المصرّح لها فقط، وأن تبقى البيانات والمعلومات سرّيّة(غير مقروءة) لمن ليس له حق الاطّلاع عليها. وفي أنظمة التشغيل تكون المعلومات السِّريّة للقراءة فقط من قبل الجهات المصرّح لها بذلك فقط، وهذا النوع من الدخول يشمل: الطباعة، والعرض، وأنواع الاستعراض(التصفح) الأخرى، وكذلك يشمل إمكانية الكشف عن وجود العنصر(ملف أو مجلد مثلًا).

٣. السلامة والتكاملية: ويتطلب ذلك إمكانية تعديل أصول أنظمة الحاسب الآلي بوساطة الجهات المصرّح لها بذلك فقط، والتعديل يشمل: الكتابة، والتغيير، وتغيير الوضع، والحذف والإنشاء.

٤. التوافر: يتطلب ذلك أن تكون أصول أنظمة الحاسب الآلي متوافرة للجهات المخول لها باستخدامها.

3 – أمن انظمة التشغيل و الملفات

وتهدف هـذه العناصر في مجملها إلى تحقيق الغايات الآتية، التي تُعدُّ هي جوهر أمن أي نظام تشغيل:

- ضبط الدخول: ويهتم هذا بتنظيم دخول المستخدم إلى كامل نظام التشغيل، والأنظمة الفرعية والبيانات، وينظّم عمليّة الدخول إلى مختلف الموارد في النظام.
- ضبط تدفق المعلومات: ينظّم تدفق البيانات في النظام وتسليمها إلى المستخدمين .
- التأكيد: يتعلّق بإثبات أنّ الدخول وآليات ضبط التدفق تعمل وفقًا لمواصفاتها، وأنّها تفرض الحماية المطلوبة والسياسات الأمنيّة.

4 – أمن الحواسيب : اساءة الاستخدام

إساءة الاستخدام يتضمن الاستخدام غير المصرح به للأصول. وفي معظم الحالات فإن إساءة الاستخدام تأتي نتيجة لغياب مبدأ الأمن العام المعروف باسم "المعرفة حسب الحاجة". واستناداً إلى هذا المبدأ فإن الفرد لا يكون لديه حق الوصول إلى الأصول إلا إذا كان يحتاج إلى ذلك لأداء وظيفته. وهذا المبدأ ينطبق بشكل مستقل عن الوظيفة التي يشغلها الشخص في المؤسسة.

إساءة استخدام الامتيازات: يحدث إساءة استخدام الامتيازات عندما يستخدم الموظف منصبه و/أو الوصول إلى الأصول بطريقة غير سليمة مما يتسبب في الضرر للأصول و/أو المؤسسة. وكشخص متخصص في تقنية المعلومات، أول ما يتبادر إلى الذهن هو إساءة استخدام مسؤولي النظم لامتيازاتهم. لنأخذ على سبيل المثال قضية "ستيفن بارنز" احد متعهدي تقنية المعلومات. عمل ستيف لشركة (Blue Falcon Networks) والمعروفة الآن باسم (Systems Akimbo) . ففي عام 2008 صدر حكم من محكمة في ولاية كاليفورنيا على ستيفن بدفع 54 ألف دولار كتعويضات لشركة (Systems Akimbo)، كما حكم عليه بقضاء سنة ويوم في السجن. والسبب أن ستيفن استخدم صلاحياته للدخول على خادم البريد الإلكتروني للشركة لإزالة القيود التي وضعتُ لحماية الخادم من مرسلي البريد المزعج ومن ثم جرى استخدام الخادم كبروكسي للرسائل غير المرغوب فيها. وكانت النتيجة مشابهة لهجمات الحرمان من الخدمة حيث تعطل نظام البريد الإلكتروني لشركة (Systems Akimbo) وذلك عندما وجد مرسلو البريد المزعج المنافذ مفتوحة. ووفقاً لستيفن فإنه فتح المنافذ انتقاماً من زملاء العمل في الشركة والذين جاؤوا إلى منزله وأخذوا أجهزة الحاسب الآلي الخاصة به بالقوة.

4 – أمن الحواسيب : اساءة الاستخدام

الاحتيال والاختلاس: تعد قوانين الاحتيال وإساءة الاستخدام والوصول المزيف لأجهزة الحاسب الآلي محاولة من قبل الحكومات للتعامل مع قضية الاحتيال في مجال تقنية المعلومات. حيث يجرم القانون استخدام أجهزة الحاسب الآلي لإلحاق الضرر بأنظمة الحاسب الآلي، متضمناً ذلك الأجهزة والبرمجيات الخاصة بها. وهي موجهة في المقام الأول نحو قراصنة الحاسب الآلي. وتستخدم هذه القوانين لمقاضاة الموظفين الذين يستغلون مناصبهم للوصول إلى أصول المنظمة بهدف الاحتيال واختلاس الأموال من المنظمات وعملائها.

إن حالات الاحتيال والاختلاس باستخدام موارد تقنية المعلومات كثيرة، وخصوصاً عندما يجد الأفراد أنفسهم في ضائقة مالية. وقد أدى ذلك إلى قيام الشركات بالتحقق من الرصيد الدائن للموظفين الذين لديهم امتياز الوصول إلى أصول قد ترتبط بها عمليات الاحتيال.

ففي عام 2012 بدأت امرأة من نيوكسفيل بقضاء خمس سنوات تحت المراقبة بعد اعترافها بارتكاب عملية احتيال باستخدام أجهزة حاسب آلي . وذلك أثناء عملها مديرة لعمليات التجزئة في مصرف صن ترست، وكانت وظيفتها التأكد من أن الفروع في منطقتها تمتثل لممارسات الأمن الداخلي، وفقاً للقضية، كان لديها إمكانية الوصول إلى السجلات المالية لعملاء صن ترست من خلال جهاز الحاسب الآلي المخصص لعملها. وفيما يلي أمثلة على الاحتيال باستخدام الحواسيب:

- الخداع عبر البريد الإلكتروني بهدف تخويف الناس (البرمجيات المثيرة للقلق، وبرمجيات الفدية).
- استخدام جهاز الحاسب الآلي لشخص آخر بطريقة غير شرعية أو "التظاهر" بأنه شخص آخر على الإنترنت.
- استخدام أي نوع من البرمجيات الخبيثة أو رسائل البريد الإلكتروني لجمع المعلومات من منظمة أو شركة بقصد استخدامها لتحقيق مكاسب مالية.
- استخدام أجهزة الحاسب الآلي لإغواء الاخرين في علاقات غير مشروعة.
- انتهاك قوانين حقوق التأليف والنشر عن طريق تحميل وتبادل مواد محفوظة الحقوق دون إذن صاحبها.
- استخدام أجهزة الحاسب الآلي لتغيير المعلومات، مثل الدرجات، وتقارير العمل، وغيرها.

4 – أمن الحواسيب : اساءة الاستخدام

استخدام البرمجيات غير المعتمدة: قد يصبح الموظفون وسطاء تهديد عندما يقومون بعمل لا يتفق مع سياسة المؤسسة كتثبيت تطبيقات برمجية على أجهزة الحاسب الآلي. البرامج المثبتة في أجهزة الحاسب المكتبية أو الهواتف الذكية قد توفر لقراصنة الحاسب وسيلة للوصول إلى الأصول المقيدة للمؤسسة. ويعد السماح للمستخدمين بتثبيت البرمجيات على الحواسيب المكتبية قضية إشكالية خصوصاً بالنسبة للجامعات. وبشكل تلقائي يجب أن تكون الجامعات مفتوحة وغير مقيدة لأنها المكان الذي يجتمع فيه حب الاستطلاع والبحوث لتشجيع الإبداع. من جهة أخرىً يمكن ان الانفتاح نفسه يعرض البيانات البحثية وغيرها من الأصول المعلوماتية على وسطاءُ تهديد ما يؤدي إلى عواقب وخيمة على المؤسسة والأفراد.

وخير مثال على القضايا المرتبطة بتثبيت البرمجيات هو برنامج (Bonzi Buddy) والذي ظهر في أواخر التسعينيات، كان الغوريلا الأرجواني (Bonzi) اللطيف والرائع مُفضلا لدى كثر من المستخدمين في الحرم الجامعي، وكان يتجول على سطح مكتب الحاسوب وكان يسلي المستخدمين. ولسوء الحظ كان أيضاً يجمع معلومات عن عادات التصفح الخاصة بالمستخدم، ومحلات التسوق المفضلة للمستخدم (برنامج تجسس- spyware)، من ثم يعرض الإعلانات ذات الصلة على الشاشة (برنامج إعلانات تطفلي – adware). وأخيراً فإنه يستخدم الكثير من طاقة وحدة المعالجة المركزية (CPU) ما يؤدي إلى بطء شديد في جميع التطبيقات الأخرى.

وبسبب انفتاح الجامعات على العالم الخارجي فإنها لا تملك سياسة حظر المستخدمين من تثبيت البرمجيات على الحواسيب، ولكن العديد من المؤسسات الأخرى تقوم بذلك. ففي عام 2012 قررت المحكمة الجزئية الأمريكية للمنطقة الغربية من ولاية أوكلاهوما أن الموظف الذي يقوم بتحميل برمجيات من الإنترنت في انتهاك لسياسة المؤسسة قد يكون مسؤولاً بموجب قانون (CFAA) عن قيام البرمجياتُ المَحملة بالحصول على وثائق المؤسسة السرية. ففي القضية التي كانت بين شركة (Musket Corp) وشركة (Star Fuel of Oklahoma LLC)، رأت المحكمة أن أي شخص مخول لاستخدام جهاز الحاسب الآلي لأغراض معينة ولكنه يتعدى تلك الحدود، فإنه يعد قد "تجاوز الوصول المسموح" وفقاً لقانون (CFAA) .

4 – أمن الحواسيب : الهندسة الاجتماعية

تعتمد العديد من هجمات الهندسة الاجتماعية على علم النفس، وهو النهج العقلي والعاطفي وليس المادي. تعتمد الهندسة الاجتماعية في جوهرها على تلاعب المهاجم الذكي بالطبيعة البشرية من أجل إقناع الضحية بتقديم المعلومات أو اتخاذ الإجراءات. هناك العديد من "المبادئ" أو الأسباب الأساسية التي تجعل الهندسة الاجتماعية النفسية فعالة. تم إدراجها في الجدول التالي مع مثال مهاجم يتظاهر بأنه الرئيس التنفيذي (CEO) ويتصل بمكتب المساعدة الخاص بالمؤسسة لإعادة تعيين كلمة المرور.

الهجمات الاجتماعية تشمل محادثات أو حوار مع مستخدمين بهدف إقناعهم أن يفعلوا شيئاً ما يقومون عادة بفعله. وفي ظروف معينة حتى مستخدمو الحاسب الآلي الأذكياء قد يكونون عرضة لهجمات الهندسة الاجتماعية.

التحجج الاحتيالي (Pretexting) : وهي التقنية التي يستخدم فيها المهاجم سيناريو وهمي للتأثير في شخص ما لإنجاز عمل ما أو بهدف إفشاء معلومات. ويعرف (التحجج الاحتيالي) خارج المنطقة التقنية باسم **"الاحتيال"** (scam).

وأحد أنواع التحجج الاحتيالي هو **التصيد** (phishing) والذي يستخدم فيه المهاجم البريد الإلكتروني في محاولة لجعل متلقي الرسالة الإلكترونية يفصح عن بعض المعلومات. ويمكن أن تكون رسائل الانتحال الإلكترونية مقنعة وجميلة وجذابة بشكل كبير، كما يمكن أن يأخذ المرسل دور شخصية ذات سلطة، أو يأخذ دور شخص يعرفه المستخدم. ويقرن التصيد عادة برسائل البريد الإلكتروني غير المرغوب فيها (spamming) وهي التي يقوم فيها المهاجم بإرسال آلاف وآلاف من الرسائل الإلكترونية على أمل إقناع نسبة صغيرة من المتلقين بفتح ملف مصاب ببرمجيات خبيثة، أو الرد برقم الحساب أو كلمة المرور.

ومع توجه الاتصالات الهاتفية بما يعرف بالتواصل الصوتي عبر شبكة الإنترنت أو اختصاراً (VOIP)، ظهرت طريقة جديدة لهجمات التحجج الاحتيالي . تعرف هذه الطريقة اختصاراً (SPIT) وهي عبارة عن مجموعة من المكالمات الهاتفية المسجلة مسبقاً باستخدام شبكة مخترقة من شبكات (VOIP). ومن خلال هذه الطريقة يتم توجيه الشخص الذي يرد على المكالمة "بالبقاء على الخط" أو الإجابة عن أسئلة والتي يتم تسجيلها ونقلها لقراصنة الحاسب. وبعكس تسليم البريد الإلكتروني حيث يوجد عناصر للتحكم لإيقاف معظم الرسائل غير المرغوب فيها والتي تصل للمستخدم، لا يوجد طريقة للتحكم في المكالمات الهاتفية التي تصل إلى هاتف شخص ما. وبينما كان لدى بعض شركات الهاتف "قوائم سوداء" متاحة للعملاء (مقابل رسوم رمزية)، إلا أن الوضع يكون خارج السيطرة عندما يتغير مصدر المكالمات بشكل دوري.

4 – أمن الحواسيب : الهندسة الاجتماعية

الهندسة الاجتماعية هي وسيلة لجمع المعلومات للهجوم من خلال الاعتماد على نقاط الضعف لدى الأفراد. يمكن أن تتضمن هجمات الهندسة الاجتماعية أساليب نفسية بالإضافة إلى إجراءات جسدية. أحد أكثر أشكال الهندسة الاجتماعية شيوعًا هو **التصيد الاحتيالي**. التصيد الاحتيالي هو إرسال بريد إلكتروني، أو عرض إعلان على الويب، أو تسجيل مكالمة هاتفية تدعي كذبًا أنها من مؤسسة شرعية في محاولة لخداع المستخدم لتسليم معلومات خاصة. يتم تنفيذ التصيد الاحتيالي في أغلب الأحيان عن طريق إرسال رسائل غير مرغوب فيها، وهي رسائل بريد إلكتروني غير مرغوب فيها مزعجة ومزعجة ويمكن أن تشكل أيضًا خطرًا أمنيًا خطيرًا.

يمكن للمهاجمين استخدام الخدع كخطوة أولى في الهجوم، وهو تحذير كاذب، غالبًا ما يتم تضمينه في رسالة بريد إلكتروني تدعي أنها واردة من قسم تقنية المعلومات. يتم إخبار المستلمين أنه يجب عليهم مسح ملفات معينة أو تغيير تكوينات الأمان، ثم إعادة توجيه الرسالة إلى مستخدمين آخرين. يستفيد وضع **الخطأ المطبعي** من الأخطاء الإملائية للمستخدم لتوجيهه إلى مواقع الويب المزيفة. يتم توجيه هجوم **حوض الشرب** نحو مجموعة أصغر من أفراد محددين، مثل المديرين التنفيذيين الرئيسيين الذين يعملون في شركة تصنيع.

تعتمد بعض هجمات الهندسة الاجتماعية على الأفعال المادية. يتضمن تفتيش القمامة التفتيش في أوعية القمامة للعثور على معلومات يمكن أن تكون مفيدة في الهجوم. كما تستثمر المؤسسات مبالغ كبيرة لتركيب أبواب متخصصة لا تسمح بالدخول إلا للمستخدمين المصرح لهم الذين يمتلكون بطاقة خاصة أو الذين يمكنهم إدخال رمز معين، إلا أنها لا تتحكم دائمًا في عدد الأشخاص الذين يدخلون المبنى عندما يُسمح بالدخول. يُعرف اتباع الشخص المرخص له من خلال باب مفتوح باسم "الملاحقة". إذا لم يتمكن أحد المهاجمين من دخول المبنى دون إثارة الشكوك، فإن البديل هو مشاهدة فرد يدخل رمز الأمان على لوحة المفاتيح. يُعرف هذا باسم تصفح الكتف، ويمكن استخدامه في أي مكان يتجسس فيه المستخدم على شخص يقوم بإدخال رمز مصرح به على لوحة المفاتيح.

4 – أمن الحواسيب : الهندسة الاجتماعية

المبدئ	الوصف	مثال
السلطة	يتم توجيهه من قبل شخص ينتحل شخصية ذات مسؤولية عالية أو يستشهد زورًا بسلطته	"المتصل الرئيس التنفيذي."
التخويف/التهديد	التخويف والإكراه بالتهديد	"إذا لم تقم بإعادة تعيين كلمة المرور الخاصة بي، سأتصل بمديرك المباشر."
الإجماع / التأثير الاجتماعي	يتأثر بما يفعله الآخرون	"اتصلت الأسبوع الماضي وقام زميلك بإعادة تعيين كلمة المرور الخاصة بي."
النقص	هناك نقص في شيء ما	"لا أستطيع إضاعة الوقت هنا."
الاستعجال	هناك حاجة إلى اتخاذ إجراءات فورية	"اجتماعي مع مجلس الإدارة سيبدأ بعد 5 دقائق."
الألفة / الإعجاب	الضحية معروفة ومقبولة جدًا	"أتذكر أنني قرأت تقييمًا جيدًا عليك."
يثق	ثقة	"أنت تعرف من أكون."

4 – أمن الحواسيب : الهندسة الاجتماعية

نظرًا لأن العديد من الأساليب النفسية تتضمن الاتصال الشخصي، يستخدم المهاجمون مجموعة متنوعة من التقنيات لكسب الثقة بدون التحرك بسرعة حتى لا يصبحوا مشبوهين.

على سبيل المثال:

- لن يطلب المهاجم الكثير من المعلومات في وقت واحد، ولكنه بدلاً من ذلك سيجمع كميات صغيرة - حتى من عدة ضحايا مختلفين - من أجل الحفاظ على مظهر المصداقية.
- يجب أن يكون طلب المهاجم قابلاً للتصديق. إن مطالبة الضحية بالذهاب إلى مكتب المدير المالي للحصول على مستند قد يثير الشكوك، لكن السؤال عما إذا كان المدير المالي في إجازة لن يثير الشكوك.
- يمكن أن يكون التملق أو المغازلة البسيطة مفيدًا في "إقناع" الضحية بالتعاون.
- يعمل المهاجم على "دفع الظرف" إلى مسافة كافية عند البحث عن معلومات قبل أن تشك الضحية في أي شيء غير عادي.
- ابتسامة وسؤال بسيط مثل "أنا في حيرة من أمري، هل يمكنك مساعدتي؟" أو كلمة "شكرًا" يمكنها عادةً "حسم الامر".
- غالبًا ما تتضمن الأساليب النفسية للهندسة الاجتماعية انتحال الهوية، والتصيد الاحتيالي، والبريد العشوائي، والخدع، والأخطاء المطبعية، وهجمات الحفرة المائية.

4 – أمن الحواسيب : التهديد المادي

نشاط التهديد المادي (Physical) وهذا يتضمن الجانب المادي أو الجانب الملموس للأصل. ولسوء الحظ فإن العديد من المؤسسات لا تأخذ نشاط التهديد المادي بعين الاعتبار بما فيه الكفاية لتبرير تكاليف الحماية ضد تلك الأنشطة التهديدية.

الدخول غير المرخص: وهذا تهديد شائع حيث تتطلب العديد من المؤسسات وجود بعض المناطق المحمية بآلية الدخول بالبطاقة. لكن وفي محاولة ليصبح الموظفون مهذبين وديين، يقوم الموظفون بإبقاء الباب مفتوحاً عند رؤيتهم لشخص ما يركض لاستغلال هذه الفرصة لدخول المبنى دون البحث عن بطاقته الخاصة بالدخول. وفي كثير من الأحيان لا يقوم الموظفون بتحدي الأفراد الآخرين خصوصاً إذا كانوا يعاملون أنفسهم بثقة وإيمان انطلاقاً من مبدأ "يفترض أن أتجول هنا بدون بطاقتي الخاصة بالدخول".

نعيش في عصر تحول فيه الإرهاب من وسيط تهديد غير معروف نسبياً إلى مشكلة كبرى، لذا فإن التحكم في الدخول غير المصرح به إلى المناطق والأنظمة المتعلقة بالبنية التحتية مثل المطارات ومحطات توليد الطاقة وحتى محطات الكهرباء التي تخدم منطقة محدودة أصبح قضية حرجة. وفي حين أن الأسوار وضوابط الوصول الأخرى كانت مبدئياً تهدف في المقام الأول منع الناس من الوصول وإصابتهم بصعقة كهربائية، لكن ما يثر القلق الآن هو أن الوصول غير المصرح به سيؤدي إلى نقص حاد في خدمات البنية التحتية الحرجة. والمؤسسات الآن تراجع المبادئ التوجيهية والمعايير لحماية الأصول، مثل معهد مهندسي الكهرباء و الالكترونيات (IEEE) ومعاييرهم الخاصة بالأمن المادي لمحطات التوليد الكهربائية، وذلك للتركيز على وسطاء التهديد الجديدة والتي تم تجاهلها سابقا.

السرقة: عند التجول في الحرم الجامعي أو مكتبة الجامعة أو منطقة دراسية أخرى، ستلاحظ أنه من السهل أن تأخذ جهاز الحاسب الآلي المحمول لشخص ما عندما يخرج بسرعة للذهاب إلى دورة المياه. سيكون لديك متسع من الوقت لإغلاق غطاء الحاسب المحمول، وتفصل الكهرباء من المقبس، وتنطلق بالجهاز الجديد.

4 – أمن الحواسيب : الأخطاء

الأخطاء (Error) : هذه الفئة من أنشطة الوسطاء تشمل كل عمل غير صحيح وغير مقصود. وتشمل الإهمال، والحوادث، والعثرات، وأعطال الأجهزة والبرمجيات، وغيرها. والأخطاء لا تشمل الأشياء التي تركت دون إتمامها، أو الأشياء التي تم إتمامها عمدا بشكل غير صحيح.

أخطاء إدخال البيانات (Data entry errors) : أخطاء ادخال البيانات تأتي على نوعين: الحذف والزيادة. ومع وجود أخطاء الحذف لا يتم إدخال القيمة بطريقة مناسبة. أما أخطاء الزيادة فتؤثر في سلامة إدخال البيانات.

وللأسف فإن أخطاء إدخال البيانات شائعة لكنها خطرة خاصة في مجال الصحة. وتم وضع السجلات الصحية الإلكترونية للعمل بها في المستشفيات ومكاتب الأطباء في جميع أنحاء البلاد بهدف تسهيل تبادل البيانات بين الجهات الطبية وغيرها من نقاط الرعاية. لكن تبادل البيانات بهذه الطريقة من شأنه أن يشارك أي خطأ في إدخال البيانات نفسها. وفي حين أن التكنولوجيا نفسها قد تكون مهمة، إلا أن ًكلا من التدريب المناسب، واختبارات قابلية الاستخدام ضروريان لعمل هذه الأنظمة بالشكل الصحيح.

أخطاء التهيئة (Misconfiguration) : يجب على مسؤولي النظام توخي الحذر عند تعاملهم مع الخوادم التي تحتوي على معلومات شخصية. وللأسف فإن تحديث البرمجيات والأجهزة تتم عادة تحت ضغط هائل لإعادة توافر النظام بأسرع ما يمكن وذلك يؤثر في تكامل النظام وسلامته. ويبدو أن حوادث أخطاء التهيئة الأكثر شيوعاً تكون ذات علاقة بتلك التحديثات. ففي عام 2012 وفي جامعة نورث كارولينا في مدينة شارلوت أصبحت المعلومات الشخصية لأكثر من 350 الف شخص مكشوفة بسبب فشل المسؤولين في ترحيل إعدادات الأمان بشكل صحيح من الخادم القديم الذي توقف عن العمل للانتقال إلى خادم جديد. والشيء نفسه حدث مع كلية نورث ويست في ولاية فلوريدا بعد هذه الحادثة ببضعة أشهر.

البيئة (Environment) : أنشطة التهديد التي تندرج تحت تصنيف البيئة تشمل ما يلي:

- الكوارث الطبيعية مثل الأعاصير، والعواصف، والفيضانات.
- فشل الضوابط البيئية المخصصة لدعم الأصول التقنية للمعلومات، مثل انقطاع التيار الكهربائي، وتسرب المياه، وتعطل تكييف الهواء، وغيرها.

4 – أمن الحواسيب : الثغرات

الثغرات هي نقاط الضعف في نظم المعلومات والتي تعطي التهديدات الفرصة لاختراق الأصول. وغالباً يستخدم التعبيران: الثغرات والتهديدات، بالتبادل في هذه الصناعة خصوصاً من قبل الموردين. ومع ذلك فإنه من المهم التمييز بن هذين التعبيرين. وفي حد ذاتها فإن الثغرة لا تشكل خطراً على الأصول. وبالطريقة نفسها فإن التهديد لا يشكل خطراً مالم يكن هناك ثغرة في النظام يمكن استغلالها من قبل التهديد.

ليس كل ثغرة تسب تهديداً للشبكة، ولا يجب تصحيح جميع الثغرات على الفور. الثغرات التي يمكن استغلالها فقط هي التي تمثل تهديداً على عمليات المؤسسة والأصول المعلوماتية. ومن الشائع للفرق الإدارية استلام تقارير عن الثغرات مع طلبات اتخاذ إجراءات فورية للقضاء عليها. وأحد مصادر هذه الطلبات هو فريق التدقيق الداخلي للمؤسسة. والمصدر الشائع الآخر للرسائل (أصلحه الآن، لأن الصحافة أو الموردين يعتقدون بأهميته) هو الإدارة بما في ذلك العديد من مديري نظم المعلومات. لكن هل ينبغي النظر إلى جميع الثغرات بأنها حالات طارئة؟ وهل جميع الثغرات تستحق التكاليف المالية من الميزانية الأمنية؟.

ويستخدم وسطاء التهديد معرفتهم بالثغرات لإنتاج تهديدات جديدة ضد أحد الأصول. وبالنسبة لأصول المعلوماتية فإن التعديل على شفرة البرمجيات لمعالجة الثغرات يعرف "التصحيح الأمني" (security patch). وأفادت إدارة الأمن الداخلي لقاعدة بيانات الثغرات الوطنية الامريكية بوجود 3532 ثغرة في عام 2011 أي بمعدل 10 ثغرات جديدة تكتشف كل يوم. وهذا في الواقع يعد تحسناً مقارنة بأرقام عام 2009 وعام 2010.