أمن الحاسبات والمعلومات
الفصل السابع: البرمجيات الخبيثة Malware

إعداد الدكتور / أسامة حسام الدين

كلية علوم وهندسة الحاسبات بينبع
جامعة طيبة

محتوى الفصل السابع

- نقدم في هذا الفصل أنواع البرمجيات الخبيثة وطرق عملها
- نقدم للتركيب الداخلي للفيروس
- نقدم لطرق انتشار الديدان

تعريف البرمجيات الخبيثة

البرامج الضارة:

تعرف البرمجيات الضارة (الخبيثة) على أنها: " برنامج يتم ادخاله إلى النظام ، في الغالب يكون سرا ، الهدف منه التخريب او التدخل بسرية أو سلامة أو إتاحة بيانات الشخص المخترق جهازه، أو نظام التشغيل أو موضوع اخر يزعج الشخص المخترق جهازه أو يعطل له اعماله".

أنواع البرمجيات الخبيثة

التهديد المستمر المتقدم (APT)	هو التهديد الموجه إلى اشخاص الأعمال والسياسة ، يتم عن طريق استخدام مجموعة كبيرة من تقنيات الاقتحام والبرامج الضارة ، يتم تطبيقيها بشكل فعال وبصورة مستمره على أهداف معينة لفترة زمنية معينة وطويلة، بالعادة ما تُنسب إلى المنظمات التي تمتلكها الدولة.
أدوير (الإعلانات المزعجة)	الإعلان المدمج بالبرنامج المستخدم. يظهر عن طريق الاعلانات التي تظهر في البرنامج او عند النقر على رابط .يحدث اعاده توجيه المتصفح الى موقع تجاري اعلاني.
الباب الخلفي (Backdoor)	هي آلية تتخطى الحواجز الأمنية؛ وتتمكن من الوصول إلى وظائف في حاسب ما وهو غير مصرح لها أو تتمكن من الوصول إلى نظام وتخترقه وتنزل برمجية خبيثة به.

أنواع البرمجيات الخبيثة

هجوم قطع الخدمة (DOS)	يحدث هذه الهجوم من اجل توليد اعداد كبيرة من البيانات لإيصالها لنظام او انظمه الحاسوب المتصلة مع الشبكة ، ومن ثم قطع الخدمة عن المستخدمين الأبرياء، تسمى هذه الهجمة بهجمة قطع الخدمة (DoS).
الكود المتجول	يكون هجوم هذه النوع باستخدام احدى البرامج (على سبيل المثال ، برنامج محرر النصوص، به ما يمسمى ماكرو) وهو عبارة عن كود يستخدم في برنامج محرر النصوص ويمكن استبداله بكود خبيث.
كلمةrootkit مركبة من كلمتين **1. root و تعني جذر** **2. kit هو ممثل من تجميع عدة أجزاء**	هو هجوم يحدث عندما يستطيع الهاكر الوصول إلى نظام تشغيل عن بعد ويخترقه ومن ثم ينزل برمجيات خبيثة على الحاسب المضيف تصل إلى root بمعنى تتحكم بشكل كامل بالحاسب من مستوى الكرنل kernel وتحوله إلى بوت

أنواع البرمجيات الخبيثة

برامج التجسس Spyware	يكون هجومها على شكل برامج تقوم بجمع المعلومات من جهاز كمبيوتر ومن ثم ترسلها إلى نظام آخر عن طريق مراقبة نقرات لوحة المفاتيح وبيانات الشاشة أو حركة مرور الشبكة ؛ أو عن طريق مسح الملفات على النظام للحصول على معلومات حساسة.
حصان طروادة	هو برنامج حاسوبي يظهر ان له وظيفة مفيدة ، ولكنه سلاح متنكر، ايضا له وظيفة مخفية ويمكن ان تكون ضارة تستطيع تجاوز آليات الأمان ، وأيضا بمقدورها استغلال تراخيص متاحه ومشروعه باختراق النظام الأمني.

أنواع البرمجيات الخبيثة

فيروس Virus	هي عبارة عن برامج غير مفيدة تسبب ضرر بمجرد تنفيذها ، عن طريق إجراء نسخ متماثل لنفسها، وهي تحتاج إلى عائل وسيط تنتشر به. على عكس الديدان التي تنتشر بشكل مستقل. بمعنى انها "تركب" ظهر البرامج وتنتقل معها.
الدودة Worm	تعرف على انها برنامج حاسوبي من الامكان تفعيله بشكل مستقل او بالإمكان نشر نسخة كاملة لنفسه على انظمه آخرين على الشبكة بالغالب يقوم باستغلال ثغرات البرامج في النظام الذي تم استهدافه.
البوت Bot	هو عبارة عن برنامج يتم تفعيله على الجهاز المطلوب من اجل شن هجمات على اجهزه اخرى .

مراحل تنفيذ البرنامج الخبيث

المرحلة الأولى: مرحلة الانتشار

- تحدث آليه الانتشار عن طريق العدوى بالفيروسات التي تنتشر فيما بعد الى الأنظمة الاخرى. ممكن الانتقال عن طريق الشبكة أو وسائط التخزين.
- او عن طريق استغلال ثغرات البرامج المستهدفة
- أو باستخدام إحدى تقنيات **هجمات الهندسة الاجتماعية** التي تتمكن من اقناع المستخدمين بفتح ملف مرفقات البريد الإلكتروني بغرض تثبيت احد انواع الفيروسات مثل حصان طروادة.

مراحل تنفيذ البرنامج الخبيث

المرحلة الثانية: مرحلة التربص والكمون

- في هذه المرحلة يصيب الفيروس الملفات ولكن لا يفعل شيء.
- يستمر التربص حتى تأتي ساعة الصفر (وهو الوقت المحدد لتنفيذ الحمولة) والحمولة هو البرمجية الخبيثة التي يحملها الفيروس، كبرمجية التجسس وبرمجية مسح القرص الصلب أو برمجية قطع الخدمة.
- يمكن أن تكون ساعة الصفر (حدث ما) كالنقر على رابط أو فتح ملف ما أو ساعة معينة أو تاريخ معين.

مراحل تنفيذ البرنامج الخبيث

المرحلة الثالثة: مرحلة تنفيذ الحمولة

- عندما تأتي ساعة الصفر، تقوم البرمجية الخبيثة بتنفيذ الحمولة (مسح القرص الصلب، اظهار رسالة مزعجة، الخ)
- يستطيع الفيروس فعل اي شي او احداث اي خلل اذا تم ارفاقه ببرنامج قابل للتنفيذ, يتم تشغيله سراً عندما يتم تشغيل البرنامج المختص بنظام التشغيل والأجهزة ، ويستفيد من تفاصيلها وضعفها.

الفيروس Virus

مكونات الفيروس

المكونات التالية أساسية في أي فيروس:

- **آلية العدوى:** وهي الطريقة التي ينتشر بها الفيروس عن طريق تكرار نفسه. يشار إليها ايضا بآلية نقل العدى.

- **ضاغط الزناد (Trigger)** : وتفسر على انها الحدث أو الحالة التي بتحديد متى سيتم التنشيط والتي تعرف أحيانًا باسم القنبلة المنطقية.

- **الحمولة:** ويعرف بما يفعله الفيروس ، إلى جانب الانتشار. قد ينحصر عملها على انها ضرر أو نشاط حميد ولكن يمكن ملاحظته.

الفيروس | بنية الفيروس

الشفرة التالية توضح بنية الفيروس

```
    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:

}
```

آلية العدوى

الحمولة

ضاغط الزناد

البرنامج الرئيسي

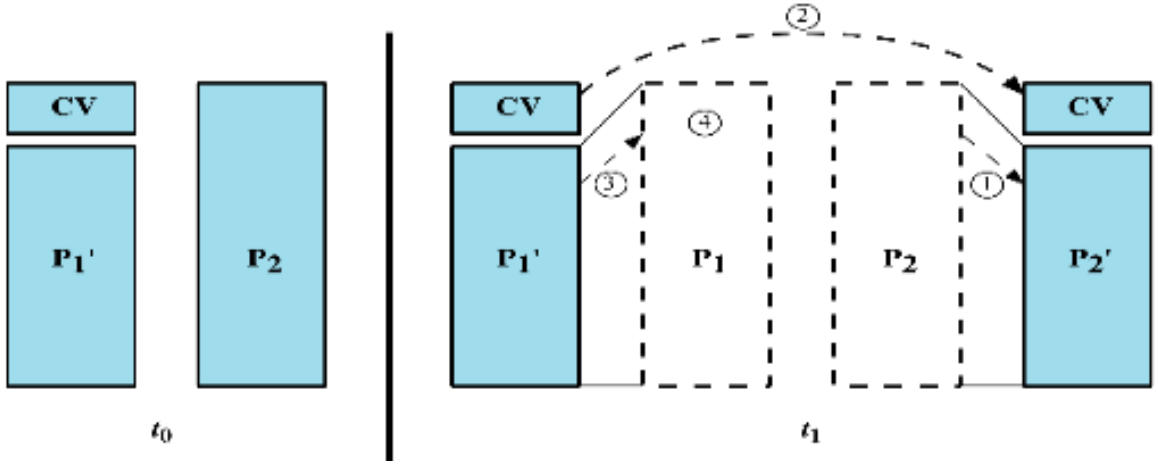
الفيروس | بنية الفيروس

شفرة الفيروس تعمل على النحو التالي:

- في آلية العدوى يقوم الفيروس بالبحث عن كل الملفات التي لا تبدأ بالرقم 1234567 إذا وجد واحدا يقوم بلصق الشفرة كلها في بداية الملف.
وإذا وجد ملفات تبدأ بالرقم 1234567 سيتجاهلها لأنها مصابة أصلا.
- يظل الفيروس كامنا حتى يتم تفعيل ضاغط الزناد، وحينها يتم تنفيذ الحمولة.
- يمكن معرفة كيف يتم عمل البرنامج بالنظر إلى البرنامج الرئيسي، حيث ينادي على الوظائف (آلية العدوى، والزناد، والحمولة)، بشكل عام فإن شفرته تقول، قم بعدوى الملفات حتى تنتهي من كل الملفات، وإذا تم ضغط الزناد قم بتنفيذ الحمولة.

الفيروس | اكتشاف الفيروس

يتم اكتشاف الفيروس مثل الفيروس الذي تم توضيحه بسهولة. لأن إصابة نسخه من الملف التنفيذي تزيد من حجم الملف بشكل واضح للنظام.



طريقة احباط مثل هذا الهجوم بوسيلة بسيطة للكشف عن فيروس هو ضغط الملف القابل للتنفيذ بحيث تكون كل من الإصدارات المصابة وغير المصابة ذات طول متطابق.

الفيروس | أنواع الفيروسات

الفيروس المشفر Encrypted virus: النموذج المعياري منه، انه يقوم جزء من الفيروس بإنشاء مفتاح تشفير عشوائي ويقوم بتشفير ما تبقى من الفيروس.

الفيروس المتخفي Stealth virus: نوع من الفيروسات المصممة لإخفاء نفسها من الكشف ببرنامج مكافحة الفيروسات. يتم إخفاء الفيروس بأكمله.

الفيروس المتشكل Polymorphic virus: يتغير هذا الفيروس مع كل إصابة ليكون شكله مختلف، ليكون الكشف عن "توقيع" الفيروس مستحيلاً.

الفيروس المتحول Metamorphic virus:يشبه الفيروس المتشكل في أنه يتغير شكله مع كل عدوى. والفرق هو أن الفيروس المتحول يعيد كتابة نفسه تمامًا عند كل عملية تكرار (يغير شكله ووظيفته بالكامل) ، مما يزيد من صعوبة الكشف. يمكن للفيروسات المتحولة تغير سلوكها وكذلك مظهرها.

الديدان worms

الديدان هو برنامج يقوم بالبحث بنشاط عن المزيد من الاجزاء للإصابة ، ومن ثم يعمل كل جزء مصاب بمثابة منصة إطلاق آلية للهجمات على الأجهزة الأخرى.

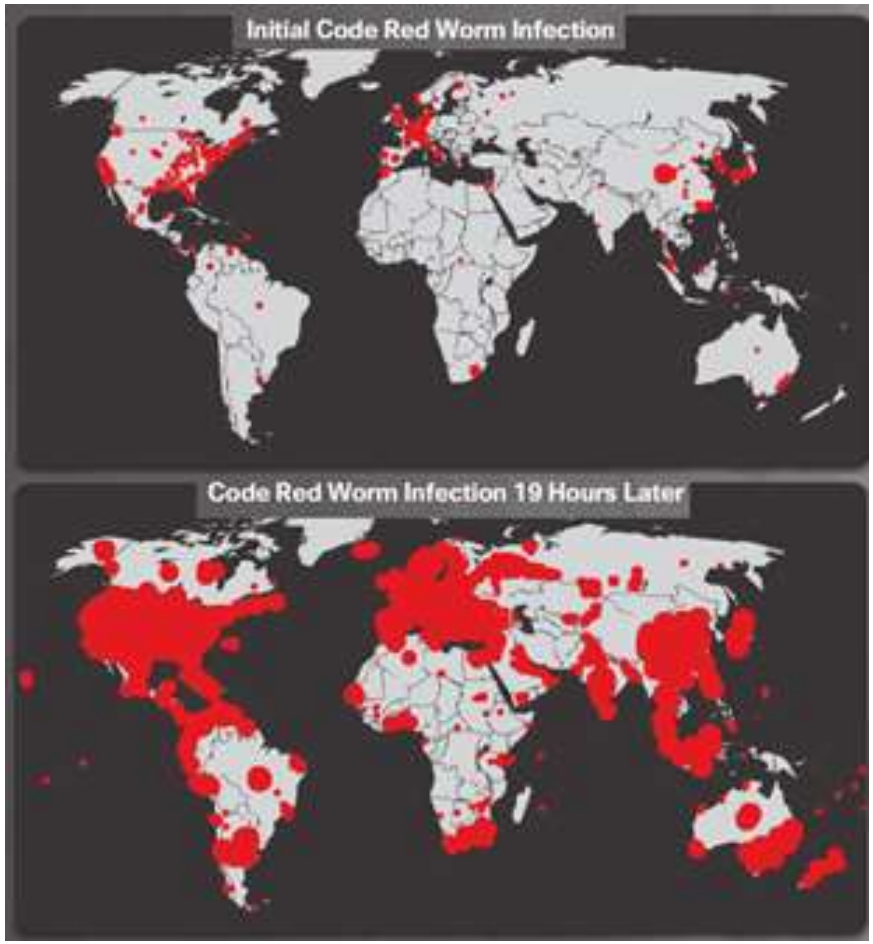
آلية الانتشار: تقوم الديدان باستغلال نقاط ضعف البرامج أو الخادم للوصول إلى كل نظام جديد. يمكنها الانتشار عبر الشبكات أو الوسائط المشتركة، مثل محركات أقراص USBأو أقراص سي دي. من الممكن أن تنتقل في التعليمات البرمجية للماكرو أو البرنامج النصي المضمنة في المستندات المرفقة بالبريد الإلكتروني.

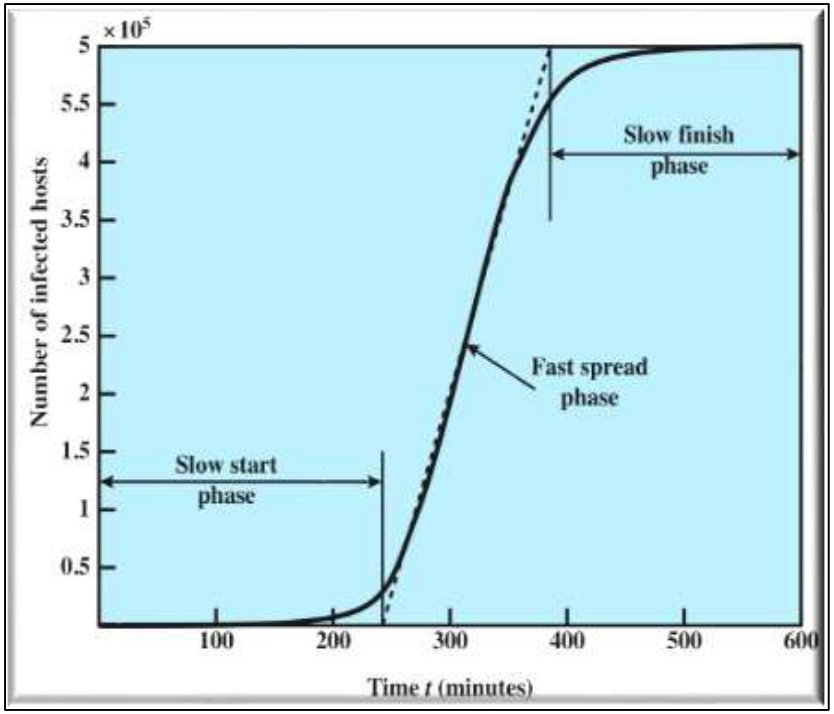
تتكاثر الدودة اثناء الانتشار !!!

ساعة الصفر: هو الوقت الذي يتم فيه ضغط الزناد وتفعيل حمولة الدودة قبل اكتشافها من قبل مكافحات الفيروسات أو الجدران النارية.

الديدان | نموذج التكاثر

تنتشر الديدان بسرعة جدا وتتكاثر في شكل تضاعفي exponential





تمرين عملي – إنشاء مستخدمين في ويندوز

– Open the User Account Tool

- **Create an Account**
- **Password Protect the Account**
- **Change the Account Type**
- **Delete the Account**
- Show the created account in MyPC-> Manage

الأسئلة