مرکز ماهر

مرکز مدیریت امداد و هماهنگی
عملیات رخدادهای رایانه ای

دانشگاه محقق اردبیلی
۱۳۵۷

مرکز آپا دانشگاه محقق اردبیلی

کارگاه آموزشی
آشنایی با انواع بدافزار و
انواع تحلیل آن

شنبه ۱۸ فروردین - ساعت ۱۷-۱۵

دانشکده فنی مهندسی - سالن آمفی تئاتر

cert.uma.ac.ir cert@uma.ac.ir 045 31505718

فهرست مطالب

معرفی بدافزار

- بدافزار برنامه هایی است که بدون اجازه صاحب سیستم، قصد انجام کارهای ناخواسته یا خرابکارانه را در سیستم دارند.
- Malware : Malicious + Software
- هدف سازنده بدافزار:
  - آزمایش و سرگرمی
  - آزار و اذیت کاربر
  - ایجاد خسارت در سیستم رایانه، داده، سخت افزار
  - باگسترش اینترنت ← سود و منفعت

انواع بدافزارها

- بدافزارهای منتشر شونده
- بدافزارهای مخفی کار
- سایر بدافزارها

انواع بدافزارها

بدافزارهای منتشر شونده

ویروس (Virus)

برنامه هایی که نرم افزارهای قابل اجرا را آلوده کرده باشند و هنگامی که اجرا می شوند، سبب می شوند ویروس به فایل های قابل اجرای دیگر نیز منتقل شود.

- Melissa Virus
- Code Red Virus
- Sasser and Netsky Virus

انواع بدافزارها

- بدافزارهای منتشر شونده
  - کرم (Worm)

برنامه هایی که بطور فعالانه خود را بر روی شبکه منتقل می کنند تا رایانه ای دیگر را آلوده سازند.

❖ Stuxnet Worm

- تفاوت Virus و Worm :

۱. اندازه

۲. دخالت کاربر در شیوع

انواع بدافزارها

- بدافزارهای مخفی کار
  - اسب تروآ (Trojan horses)

برنامه هایی هستند که کاربر را ترغیب می کنند که آن را اجرا کند در حالی که قابلیت خرابکاری خود را مخفی می سازند. ابتدا وارد قسمت های مختلف شده و سپس راهی را برای آسیب زدن می یابند.

  - رد گم کن (Rootkit)

مجموعه ای از نرم افزارهاست که کنترل سیستم را در دست می گیرند در واقع هسته سیستم عامل را دور می زنند. بدین ترتیب توانایی تغییر تمامی تنظیمات به هکر داده می شود

رایانه ای که تحت کنترل Rootkit باشد Zombie گفته می شود.

انواع بدافزارها

- بدافزارهای مخفی کار
  - درب پشتی (Back door)

برنامه هایی هستند که راهی را برای پایداری نفوذ در سیستم قربانی ایجاد می کنند. یعنی علاوه بر نصب فایل بدافزار و شروع فعالیت مخرب راه دومی را نیز برای اتصال همیشگی در سیستم قربانی باز می کنند.

باز کردن پورت های TPC و UDP جهت گوش دادن به دستورات نفوذگر

انواع بدافزارها

- سایر بدافزارها
  - جاسوس افزار (Spyware)

بدافزارهایی که به قصد جمع آوری اطلاعات و بدون اطلاع قربانی در سیستم وی نصب می شوند.

  - آگهی افزار (Adware)

برنامه هایی که وظیفه بازکردن صفحات خاص اینترنتی جهت اهداف تجاری و تبلیغی را دارند.

  - جوک (Joke)

برنامه هایی که ادعا دارند در حال انجام عملیات تخریبی هستند اما در واقع این چنین نیست.

انواع بدافزارها

سایر بدافزارها

- کلک (Hoax)

این برنامه ها با سوء استفاده از کم بودن اطلاعات کاربران، آنها فریب داده و با دستورات اشتباه باعث می شوند که کاربر کار تخریبی بر روی سیستم خود انجام دهد.

- بارگیرها (Downloader)

این برنامه ها به دانلود کردن بدافزارها و اجرای آنها می پردازند.

- دزدگذرواژه (Password-Stealer)

این برنامه ها به دزدی گذرواژه از روی سیستم و ارسال آن به نفوذگر می پردازند.

انواع بدافزارها

سایر بدافزارها

- **Exploit**

کدهای مخربی هستند که از آسیب پذیری یک سیستم استفاده کرده و امکان دسترسی از راه دور به آن سیستم را فراهم می کنند.

- **ثبت کننده کلید (KeyLogger)**

برنامه هایی هستند که با قرار گرفتن در حافظه از کلیدهای زده شده توسط کاربر گزارش گرفته و در قالب یک فایل برای نفوذگر می فرستند.

- **کنترل از راه دور Remote Administrative Tool:**

یک بدافزار جامع جهت کنترل و گرفتن دسترسی از سیستم قربانی

انواع بدافزارها

- سایر بدافزارها
  - باج افزار (Ransomware)

باج افزارها با استفاده از الگوریتم های رمزنگاری خاص، شروع به جستجوی پسوندهای خاص فایل ها برروی سیستم قربانی می کنند و سپس آنها را رمز نموده و برای رمزگشایی درخواست باج می کنند.

- ❖ Cryptolocker
- ❖ Wannacry
- ❖ DoubleLocker

online Antivirus Scanner

- معرفی پویشگرهای online جهت شناسایی فایل های مخرب
  - Virustotal
  - Jotti
  - Drweb
  - Virscan
  - ویروس کاو

قابلیت اطمینان در آنتی ویروس ها

- آنتی ویروس ها قابل اطمینان هستند؟
  - بدافزارهای جدید
  - تکنیک های مبهم سازی

تکنیک های مبهم سازی

- Cryptor
- Binder
- Self FUD
- Binery Code Editing

تحلیل بدافزار

- هدف : بررسی رفتار فایل اجرایی
- انواع تحلیل
  - تحلیل ایستا
  - تحلیل پویا
  - تحلیل ترکیبی

انواع تحلیل

- تحلیل ایستا

بررسی ساختار و رفتار فایل اجرایی بدون اجرای آن

  - زمان کامپایل
  - نوع تکنیک مبهم سازی
  - کتابخانه ها و توابع استفاده شده

انواع تحلیل

- تحلیل پویا

بررسی ساختار و رفتار فایل اجرایی با اجرای فایل در محیط جعبه شنی

- فایل های باز شده
- تغییرات رجیستری
- فرایندهای ایجاد شده

انواع تحلیل

- تحلیل ترکیبی

ترکیبی از تحلیل پویا و تحلیل ایستا