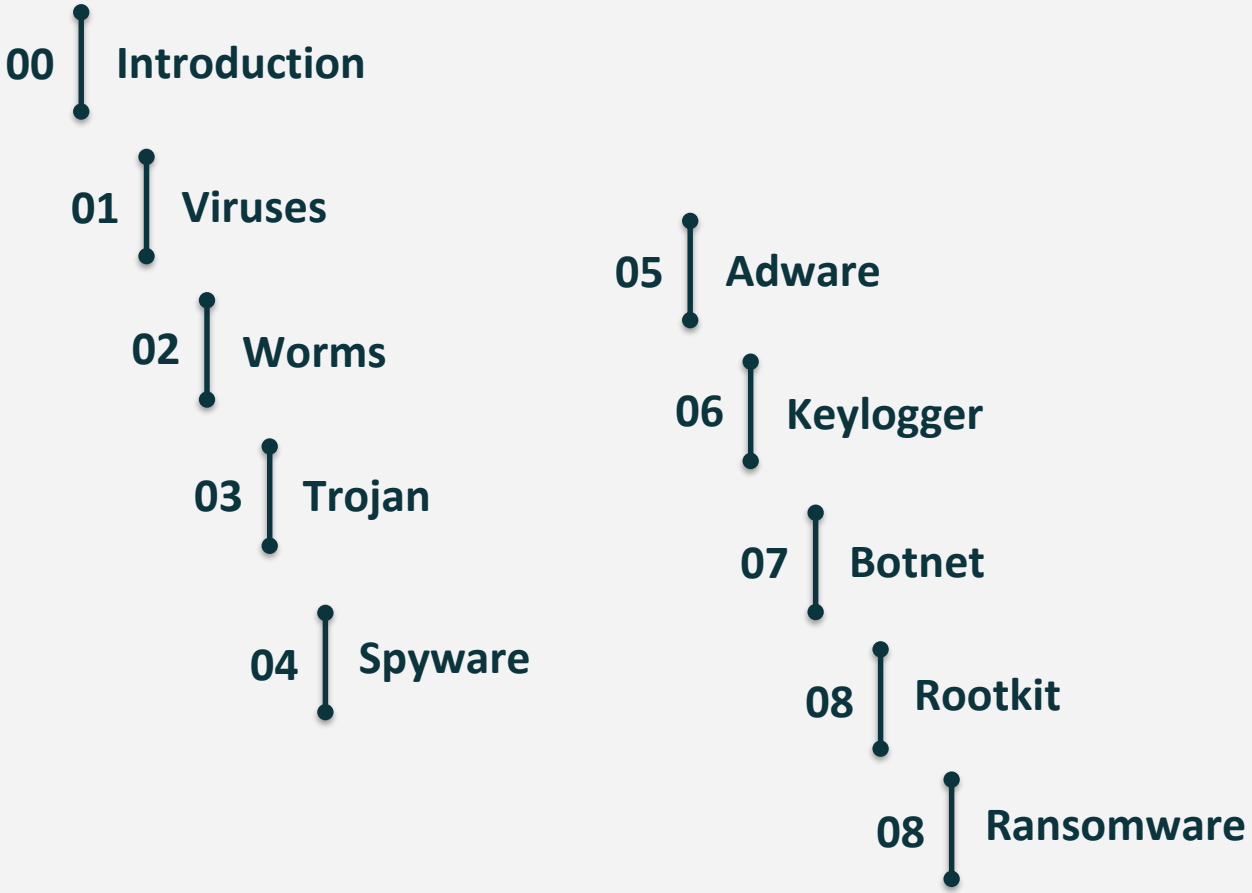
Advanced Network Security

Malware

Dr. Yaeghoobi
PhD. Computer Science & Engineering, Networking, India
dr.yaeghoobi@gmail.com


00 Introduction
01 Viruses
02 Worms
03 Trojan
04 Spyware
05 Adware
06 Keylogger
07 Botnet
08 Rootkit
08 Ransomware

Introduction 00

Introduction

- Most people seem to call **every type of malware a "virus"**, but that isn't technically accurate.
- There are many more terms beyond virus: malware, worm, Trojan, rootkit, keylogger, spyware, and more.
- But what do all these terms mean?

Ways Malware Enters a System

Intentional عمدی / هدفمند

- Malware which is purposefully **used** or **made** with the intention to **damage or alter a system**.
- Intentional internal and external

Unintentional غیرعمد / بدون اطلاع

- Malware which is **injected into a system without knowledge**.
- Unintentional internal and external

Internal داخلی

- Malware which **infects a system from within**.

External خارجی

- Malware which **infects a system from outside.**

Malware

The word “malware” is short for ***“malicious software”***

The word “malware” encompasses ***all harmful software****.*

کلمه "بدافزار" شامل همه نرم افزارهای مضر است .

Viruses

01

Viruses

*Are malicious tools, fragments and software which **spread themselves** by human intervention to **infect files or systems of a network**.*

ابزار ها، قطعات و نرم افزار های مخرب هستند که با مداخله انسان برای آلوده کردن پرونده ها یا سیستم های یک شبکه گسترش می یابند .

Viruses …

- A virus can do many different things:
  - watch in the background and steal your passwords
  - display advertisements
  - or just crash your computer
  - در پس زمینه اجرا و رمزهای عبور را سرقت می‌کند
  - نمایش تبلیغات
  - یا فقط کامپیوتر را خراب می‌کند
- But the key thing that makes it a virus is **how it spreads**.
- اما نکته اصلی که آن را ویروس می کند نحوه شیوع آن است.

Viruses …

- When you **run a virus**, it will infect programs on your computer.
- When you **run the program on another computer**, the virus will infect programs on that computer, **and so on**.

- For example: **infect program files on a USB stick.**

Types of Viruses

Polymorphic	*Stealth*	*Retro*	*Multipartite*
Armored	*Companion*	*Phage*	*Macro*

Polymorphic Viruses

خود را اصلاح می‌کند تا از شناسایی توسط نرم‌افزارهای ضد ویروس جلوگیری کند.

Modify themselves to avoid detection from anti-virus software

Anti-Virus software **searches for viruses by their signature** database and when virus mutates **signatures don't match.**

Can attack **servers, hosts, systems**

Will **delete files**

Will **mutate** and **encrypt** itself making it harder to detect and remove from a system.

Stealth Viruses

ویروس‌هایی که برای جلوگیری از شناسایی، خود را در فایل‌ها و پوشه‌های مهم مخفی می کنند

Viruses that hide themselves in critical files and folders to avoid detection

Can attach themselves to **boot sectors of hard drives**.

When system utilities or applications run the stealth virus will **redirect commands around itself**.

Will **change file and folder size** to avoid detection. Anti-virus signature databases include file size of suspected viruses.

Retro Viruses

ویروس هایی که بطور کامل نرم افزار ضد ویروس را دور می زنند، تغییر داده و از بین می برند

Viruses that completely bypass, alter and destroy anti-virus software

Changes and corrupts anti-virus signature or definition database

Will cause anti-virus **software to name critical files as viruses**

Can make your **operating system inoperable**

Multipartite Viruses

ویروس هایی که به چندین روش به سیستم حمله می کنند

Viruses which attack a system in multiple ways

Can **infect all executable files** and in the process **destroy application files**

May infect **boot sector** of a **hard drive**

Attacks on a **large scale** to make sure if parts are detected and deleted **at least one will remain**

Armored Viruses

ویروس هایی که کاربران را از شناسایی سریع و حذف آنها از سیستم جلوگیری می‌کنند و سیستم را در مقابل حملات دیگر آسیب پذیر می کند

Viruses which prevent users from quickly identifying and removing them from systems leaving the system vulnerable to other attacks

- **Difficult to detect and analyse**
- Have **multiple layers** of protected code
- Virus is used as a **decoy** to penetrate a vulnerable system
- Will **rapidly spread**
- Can be very **complex** and **hard to establish an origin** of the virus
- **Virus of choice for Hackers**

Companion Viruses

ویروس هایی که خود را به برنامه های معتبر متصل می کنند

Viruses which attach themselves to legitimate programs

Will **create files with a different extension** from the infected program

Usually reside in the **temporary folder** on a computer

Virus will run in **place of legitimate program if typed in RUN**

Attack the **windows registry** and **windows configuration database**

Phage Viruses

ویروس‌هایی که برنامه‌ها و پایگاه داده‌ها را تغییر داده و تغییر می دهند

Viruses which alter and modify programs and databases

Will infect all databases on a system

To remove the entire infected program must be uninstalled and all instances of that application need to be removed

Once small trace will trigger the spread again

Macro Viruses

ویروس‌های هوشمند در نرم افزارهایی اجرا می‌شوند که از ماکرو استفاده می‌کنند

Intelligent viruses that run in software which utilize macros (word, excel)

Heavily exploited because they can be easily made and distributed

Hard to detect and analyse

Can spread onto a system by opening a dirty word or excel file

Newer productivity software will disable macros by default

Worms

02

Worms

*The goal of a worm is to **infect other hosts and systems** from the infected system so they can **spread to system to system** without human intervention.*

هدف از کرم آلوده کردن میزبان‌ها و سیستم‌های دیگر توسط میزبان آلوده است

بنابراین آنها می توانند بدون دخالت انسان از سیستم به سیستم دیگر گسترش یابند.

Worms …

- They typically **travel across a computer network,** rather than through software downloads.
- A worm won't corrupt your files or break your computer.
- A worm will **slow down** a computer or network by **sucking up hardware resources or internet bandwidth**.
  - آنها معمولاً به جای دانلود با نرم افزار ، در شبکه حرکت می کنند.
  - کرم نمی تواند فایل‌های و یا کامپیوتر شما را خراب کند.
  - کرم با استفاده منابع سخت افزاری یا پهنای باند اینترنت، کامپیوتر یا شبکه را کند می کند.

Worms …

- Hackers rarely create payload-less worms -> find OS vulnerability exists
- Large-scale payload attacks -> DDOS attack

Worms …

- You can pick up a worm through a software download, or even by **opening an infected email attachment**.
  - می توانید از طریق دانلود نرم افزار یا حتی با باز کردن پیوست ایمیل آلوده، کرم را دانلود کنید.
- Because of frequent system updates and built-in anti-virus software, you don’t have to worry too much about worms.
  - به دلیل بروزرسانی‌های مکرر سیستم و نرم افزار ضد ویروس ، لازم نیست نگران کرم ها باشید.

Viruses Vs. Worms

Viruses

- Spread through Human intervention
- Destroy and alter programs, files and folders.
- Do not install backdoors

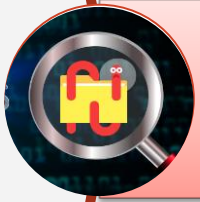
Worms

- Execute malicious code
- Do not attach themselves to system files and programs.
- Consume resources but do not corrupt or delete files.
- Install backdoors
- Can release a virus
- Denial of Service Attack

Worms …

Enabling Vulnerability آسیب پذیری را فعال می کند

- Installs itself to a vulnerable system



Propagation Mechanism مکانیسم انتشار

- Once gains access will begin to replicate
- Finds new targets to attack

Payload ظرفیت

- Once in, it will release a virus or let a hacker gain access

Trojan

03

Trojan

Masks malware as **legitimate applications.**
When this malware is installed into a system they **release malicious code** and **infect the whole system**.

ماسکی برای بدافزارها.
زمانی که نصب شوند، کد مخرب آزاد می‌شود و کل سیستم را آلوده می نماید.

Trojan (or Trojan Horse)

- When you **download and run** the program, the Trojan horse will **run in the background**, **allowing third-parties to access your computer.**
  - to **monitor** activity on your computer
  - to **join** your computer to a **botnet**
  - to open the **floodgates** and **download many other types of malware** onto your computer

- هنگامی که برنامه را بارگیری و اجرا می کنید، Trojan در پس زمینه اجرا می شود و به اشخاص ثالث نیز امکان دسترسی به رایانه شما را می دهد.
  - برای نظارت بر فعالیت ها روی رایانه
  - برای پیوستن رایانه به یک botnet
  - برای ایجاد flood و بارگیری انواع دیگر بدافزارها بر روی رایانه

How Trojan Arrives?

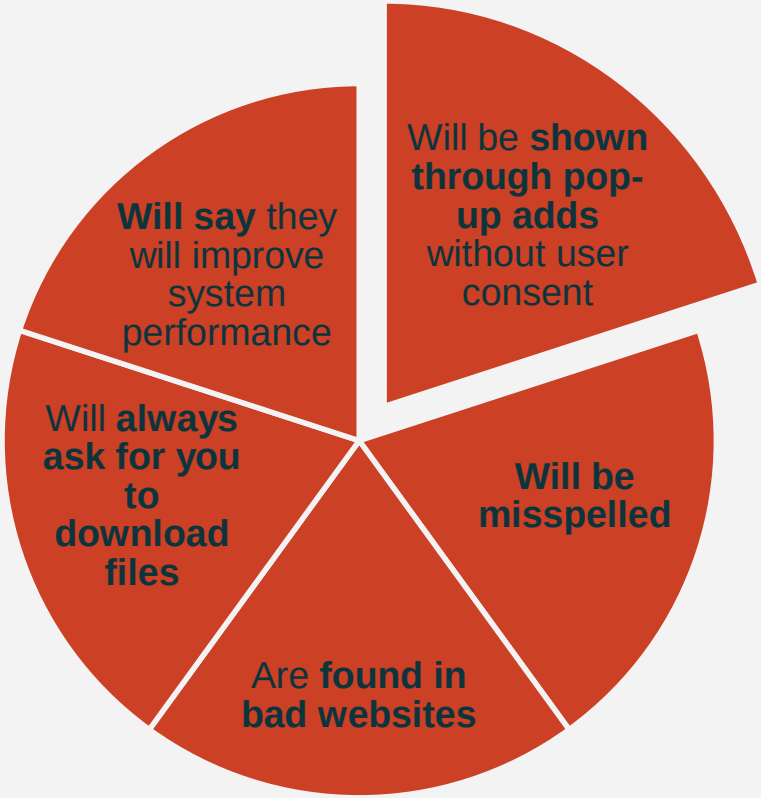
- It pretends to be a useful program and, when run, **it hides in the background** and gives **malicious people access** to your computer.
- For example, a **pirated software** on an unscrupulous website may actually contain a Trojan.

- وانمود می کند که یک برنامه مفید است و در هنگام اجرا، در پس زمینه پنهان می شود و به هکرها دسترسی به رایانه شما می دهد.

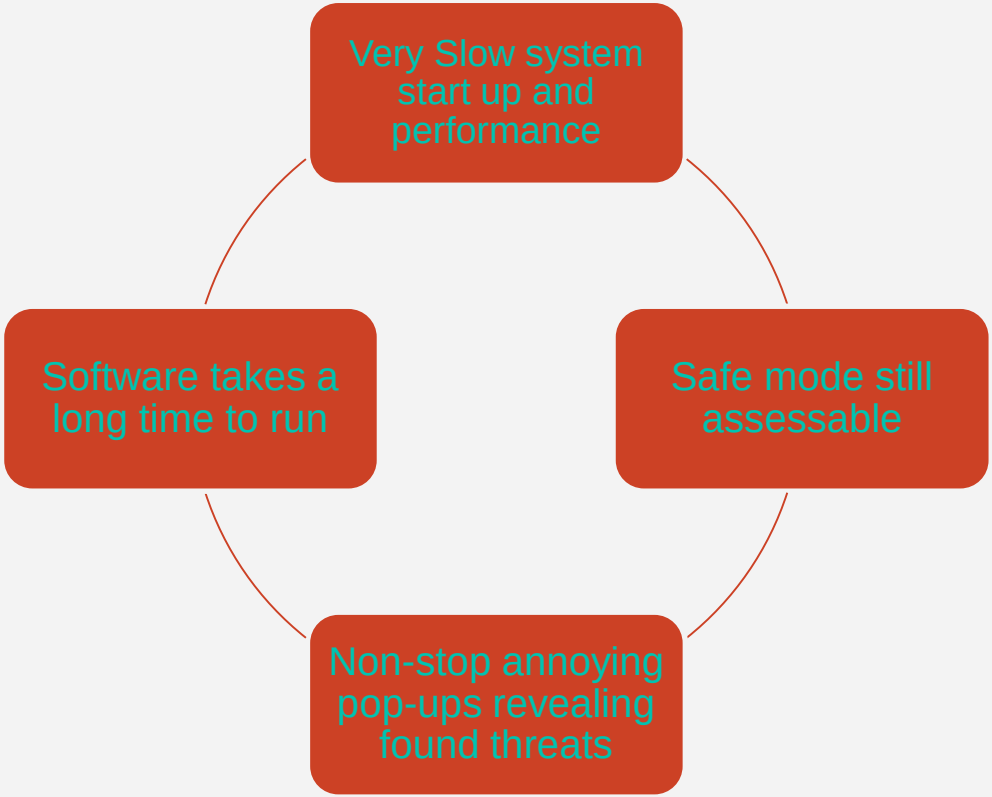
Trojan Examples

- Popular fake games
- Popular fake anti-virus programs
- Computer Maintenance software
- Pop-up ads advertising software

Characteristics of Trojan



Trojan Attack Symptoms



Spyware

04

Spyware

*Spyware can take **control, monitor** and **redirect** personal information, **surfing habits** and **redirect browsers to malicious sites.***

نرم افزارهای جاسوسی می توانند کنترل، نظارت و هدایت اطلاعات شخصی، عادات سرچ و مرورگرها به سایتهای مخرب را انجام دهند.

Spyware …

- It **collects a variety of different types of data**, depending on the piece of spyware.
- Different types of malware can function as spyware
    - There may be malicious spyware included in Trojans that spies on your keystrokes to steal financial data, for example.

- بسته به قطعه جاسوسی، انواع مختلفی از داده ها را جمع می کند.
- انواع مختلف بدافزارها می توانند به عنوان نرم افزارهای جاسوسی عمل کنند.
    - به عنوان مثال ممکن است یک جاسوس افزار مخرب در Trojans وجود داشته باشد که برای سرقت اطلاعات مالی، از کلیدهای کیبورد جاسوسی شما استفاده می کند.

Spyware …

- More “legitimate” spyware may be **bundled along with free software** and simply **monitor** your web **browsing habits**, **uploading this data** to advertising servers so the **software’s creator can make money from selling their knowledge of your activities**.

- ممکن است نرم افزارهای جاسوسی "قانونی" به همراه نرم افزار رایگان همراه شوند و به سادگی عادت‌های سرچ کاربر را کنترل کنند، این داده ها را روی سرورهای تبلیغاتی بارگذاری کنند تا سازنده نرم افزار بتواند از فروش دانش خود در مورد فعالیتهای شما درآمد کسب کند.

Protection from Spyware

Avoid **torrent, pornography,** and other **shady sites**.

Do not ever enter personal information if you are not on an known and secure site.

Secure sites will have an s after http://, https:// is a secure site.

Always clear your history and cookies after browsing.

Change security settings in browsers to meet your needs.

Adware

05

Adware

*It's **any type of software that displays advertising** on your computer.*

هر نوع نرم افزاری است که تبلیغات را در رایانه شما نمایش می دهد .

Adware …

- The kind of “adware” that’s particularly malicious is the kind that abuses its access to your system to display ads when it shouldn’t.

- نوع "تبلیغاتی" که مخرب است، و از دسترسی به سیستم شما برای نمایش تبلیغات در صورت لزوم سوء استفاده می‌کند.

Adware Example

- For example, a piece of **harmful adware** may cause **pop-up advertisements** to appear on your computer when you're not doing anything else.
- Or, adware may **inject additional advertising** into other web pages as you browse the web.

- به عنوان مثال، یک کار تبلیغاتی مزاحم مضر ممکن است باعث شود زمانیکه کار دیگری انجام نمی‌دهید، تبلیغات پاپ آپ روی رایانه شما نمایان شود.
- یا ممکن است adware هنگام مرور وب ، تبلیغات اضافی را به صفحات وب تزریق کند.

Adware …

- Adware is often combined with spyware
  - a piece of malware may monitor your browsing habits and use them to serve you more targeted ads.
  - Adware is more “socially acceptable” than other types of malware on Windows and you may see adware bundled with legitimate programs.

- نرم افزارهای تبلیغاتی مزاحم اغلب با نرم افزارهای جاسوسی ترکیب می‌شوند
  - یک تروجان ممکن است عادتهای سرچ ر شما را تحت نظر داشته باشد و از آنها برای ارائه تبلیغات هدفمند تر استفاده کند.
  - نرم افزارهای تبلیغاتی مزاحم نسبت به سایر انواع بدافزارهای ویندوز از نظر اجتماعی "قابل قبول" هستند و ممکن است مشاهده کنید که نرم افزارهای تبلیغاتی مزاحم با برنامه های قانونی همراه هستند.

Keylogger

06

Keylogger

A keylogger is a type of malware that ***runs in the background****,* ***recording every key stroke you make****.*

keylogger نوعی بدافزار است که در پس زمینه اجرا می شود و هر ضربه کلید کیبورد را ضبط می کند .

Keylogger

- These keystrokes can include usernames, passwords, credit card numbers, and other sensitive data.
- The keylogger then, most likely, uploads these keystrokes to a malicious server, where it can be analyzed and people can pick out the useful passwords and credit card numbers.
  - می تواند شامل نام های کاربری، گذرواژه‌ها ، شماره کارتهای اعتباری و سایر اطلاعات حساس باشند.
  - سپس، keylogger به احتمال زیاد، این اطلاعات را روی یک سرور مخرب بارگذاری می کند، جایی که می تواند آنالیز شوند و افراد بتوانند رمزهای مفید و شماره کارتهای اعتباری را انتخاب کنند.

Keylogger …

- Other types of malware can act as keyloggers. A virus, worm, or Trojan may function as a keylogger.
- Keyloggers may also be installed for monitoring purposes by businesses or even jealous spouses.

- انواع دیگر بدافزارها می توانند به عنوان keylogger عمل کنند. ویروس، کرم یا Trojan ممکن است به عنوان یک keylogger عمل کند.
- Keylogger ها همچنین ممکن است برای اهداف نظارت توسط مشاغل یا حتی همسران حسود نصب شوند.

Botnet

07

Botnet

*A botnet is a **large network** of computers that **are under the botnet creator's control**.*

بات نت شبکه بزرگی از رایانه ها است که تحت کنترل خالق بات نت قرار دارند.

Botnet, Bot

- Each computer functions as a “bot” because it’s infected with a specific piece of malware.
- Use command and control infrastructure which completely takes over a system remotely.

- هر رایانه به عنوان bot عمل می کند زیرا به یک بدافزار خاص آلوده است.
- از زیرساخت‌های فرمان و کنترل استفاده می‌کند تا کاملاً سیستم را از راه دور به دست گیرد.

Botnet …

- These are found online, are installed by worms and Trojans, hides malicious programs, exploits system, and can send sensitive information back to the controlling server.
- بصورت آنلاین یافت می شوند ، توسط کرم ها و تروجان ها نصب می شوند ، برنامه های مخرب را مخفی می کنند ، از سیستم سوء استفاده می کنند و می توانند اطلاعات حساس را به سرور کنترل کننده ارسال کنند.

Rootkit

08

Rootkit

A rootkit is a type of malware ***designed to burrow deep*** *into your computer,* ***avoiding detection by security programs and users****.*

rootkit نوعی بدافزار است که برای ریشه کردن عمیق در رایانه شما طراحی شده است و از شناسایی برنامه های امنیتی و کاربران جلوگیری می کند.

Rootkit …

- For example, a rootkit might **load before most of Windows**, burying itself deep into the system and **modifying system functions** so that **security programs can't detect it**.

- به عنوان مثال، ممکن است یک rootkit قبل از ویندوز بارگیری شود، خود را به عمق سیستم وارد کند و عملکردهای سیستم را تغییر دهد تا برنامه های امنیتی نتوانند آن را تشخیص دهند.

Rootkits …

- Goal is to **take over the operating system**.
- Will **hide system information** from the Operating system **making it vulnerable**.
- Are **hard to detect** and many **can not be shown on task manager.**
- Can be **Trojan**s and can install themselves to **drivers**.

- هدف این است که سیستم عامل را به دست بگیرید.
- اطلاعات سیستم را از سیستم عامل مخفی می کند و باعث آسیب پذیری می‌شود.
- تشخیص آن سخت است و بسیاری از آنها در مدیر وظیفه نمایش داده نمی شوند.
- می توانند Trojansباشند و می توانند خود را درایورها نصب کنند.

Ransomware

09

Ransomware

*It **holds your computer or files hostage** and **demands** a ransom **payment**.*

رایانه یا فایل‌های شما را گروگان نگه می دارد وشما را مجبور به پرداخت باج می‌نماید .

Ransomware …

- Some ransomware may simply **pop up a box** asking for money before you can continue using your computer.
- Such prompts are easily defeated with antivirus software.

- برخی از باج افزارها به سادگی می توانند قبل از ادامه استفاده از رایانه، از شما درخواست پول نمایند.
- چنین مدلی به راحتی با نرم افزار آنتی ویروس از بین می‌روند.

Ransomware …

- More harmful malware like **CryptoLocker** literally **encrypts your files** and **demands a payment** before you can access them.
- Such types of malware are dangerous, especially if you don’t have backups.

- بدافزارهای مضر دیگری مانند CryptoLocker به معنای واقعی کلمه فایل‌های شما را رمزگذاری می کنند و قبل از دسترسی به آنها نیاز به پرداخت دارید.
- چنین نوع بدافزارها خطرناک هستند، به خصوص اگر نسخه پشتیبان تهیه نکنید.

Ransomware …

- Most malware these days is produced for profit, and ransomware is a good example of that.
- Ransomware doesn't want to crash your computer and delete your files just to cause you trouble. It wants to take something hostage and get a quick payment from you.

- این بدافزارها این روزها برای سودآوری تولید می شوند.
- Ransomware نمی‌خواهد کامپیوتر شما را خراب کند و فایل‌ها را حذف کند، فقط مشکل ایجاد کند. می خواهد چیزی را گروگان بگیرد و سریع از شما درخواست پرداخت دارد.

Antivirus Software

- So why is it called “antivirus software” anyway?
- Well, most people continue to consider the word “virus” synonymous with malware as a whole.

- Antivirus software **doesn’t just protect against viruses**, but **against many types of malware** — except, sometimes **“potentially unwanted programs”,** which are not always harmful, but are almost always a nuiscance.
- Usually these require separate software to combat.

Thanks for your Attention.