Какво е вирус?

(Много) Кратка екзе (.exe) програма която се размножава прикрито (без знанието и разрешението на потребителя), като се вмъква в друг код (програма) или документ. Наричаме го така, заради сходствата с биологичния вирус, който се вмъква в живи клетки.

Вирусите се създават от хора с умения в областта на програмирането. Някои от тях правят опити (примерно колко бързо може да се разпространи по света) като начин да станат известни. Други ги създават с цел отмъщение (примерно на работодател) или с цел кражба на информация.



Какво е червей?

Самовъзпроизвеждаща се компютърна програма. Използва мрежата за да разпраща свои копия до крайните устройства (нашите компютри). Не се нуждае от прикачване към съществуваща програма. Почти винаги причиняват вреда- консумират пропускателната способност на мрежата.

Най-честите методи за разпространение са: чрез електронна поща, чрез уязвимости в операционната ни система, инсталирания софтуер или мрежовите протоколи и чрез съобщения.



<https://youtu.be/n8mbzU0X2nQ> - разлика между компютърни вируси; червеи и троянски коне

Мауер и бот атака; Фишинг

Мalware атака- предназначен да повреди, наруши функционирането, открадне, разруши или да извърши негативни и нелегитимни действия в рамките на компютърни системи. Съществуват различни видове зловреден софтуер, които се различават по начинът, по който проникват в компютърните системи и се разпространяват в тях. Това може да стане чрез програми или файлове, в които е включен зловреден код или скрипт. Други се инсталират, като използват уязвимости в използваната операционна система, мрежовите устройства, антивирусните програми или други програми като уеб браузърите, при което е необходимо потребителят само да посети определена уеб страница. По-голямата част от случаите на инсталиране на зловреден софтуер в компютърните системи се дължи на действия на потребителите, които посещават уеб страници с нелегитимно съдържание, отварят приложения към имейли от непознати податели или свалят файлове от Интернет. Малуерът не може да нанесе физически щети на компютри или мрежово оборудване, но може да повреди информацията или програмите до степен те да не могат да функционират.

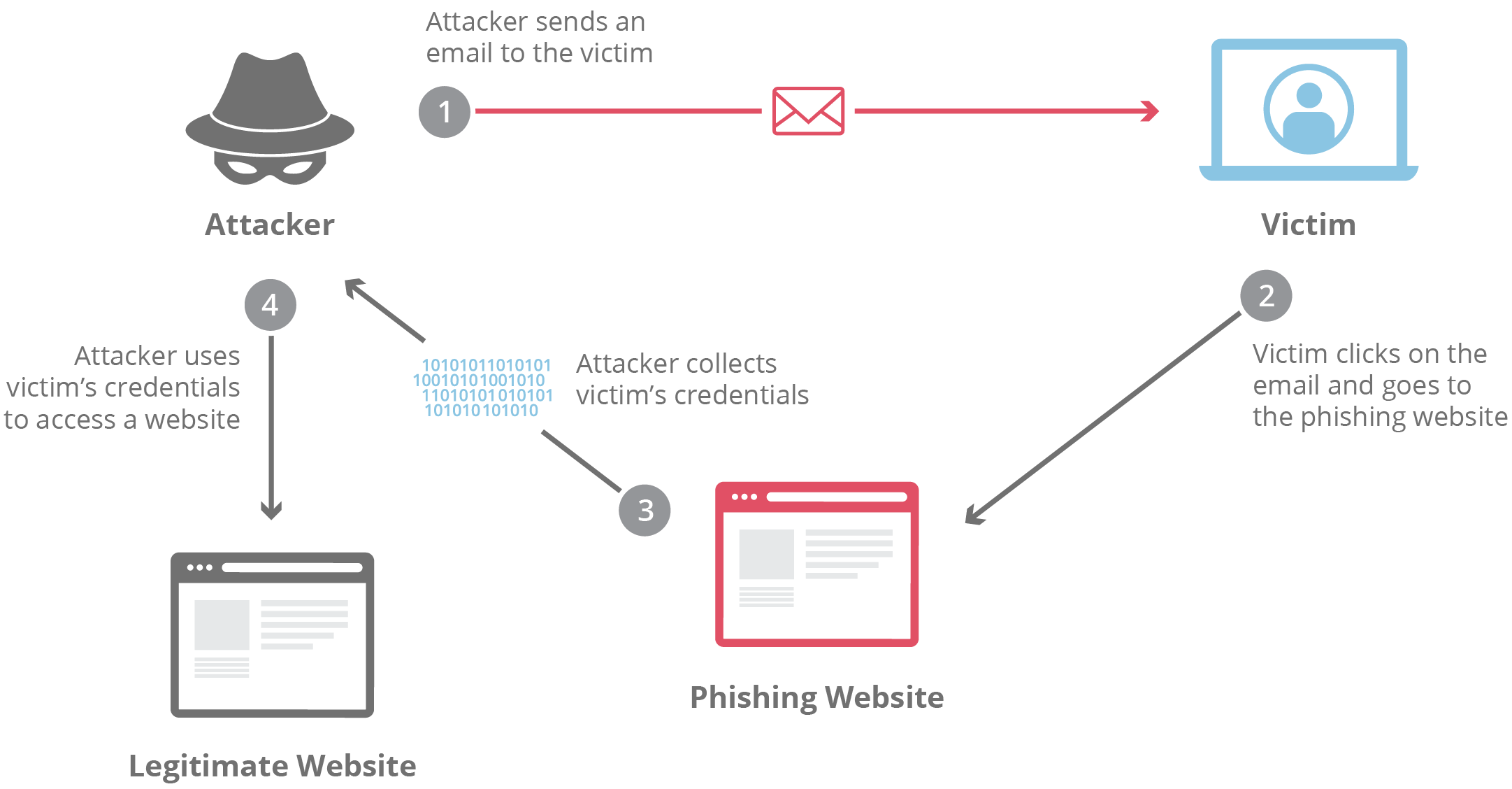
Бот атаките стават все по-чести. Целта на киберпрестъпника е да натрупа възможно най-много ботове- заразени устройства. Ботовете се използват за атаки с конкретна цел- преодоляване на киберсигурността на една или няколко системи. Последици от такива атаки са- прекъсване на мрежата; мрежови инфекции; кражба на информация; кражба на ресурси. За да се избегнат бот атаки, фирмите предприемат мерки- политики за сигурно сърфиране; процеси за мониторинг; повишено внимание при ползване на електронна поща



Фишинг атаки- **използва прикрити имейли, директни съобщения и уебсайтове, които приличат на реални и имат за цел да извлекат чувствителна информация** и достъп до важни акаунти на своите жертви. Често това става, през маскирани страници или съобщения, наподобяващи известни платформи, институции и компании, които жертвите използват в действителност. Измамниците ги подтикват да актуализират данните на кредитната си карта през изпратен от тях линк, в опит да откраднат тази ценна информация и по-късно да я използват, за да правят неоторизирани плащания.

Фишинга е един от най-старите видове киберпрестъпления. Започва да се прилага още през 90-те години на миналия век. Този вид атаки все още са широко разпространени и имат висока ефективност.





Какво представлява дифендър?

Windows Defender е софтуерно приложение, което защитава системата от зловреден софтуер. Aнтишпионска програма, създадена да се бори с неоторизирания достъп и да защитава компютрите с Windows от нежелан софтуер. Въведена с инсталационния пакет на Windows Vista, в момента тя е достъпна за безплатно изтегляне като част от Microsoft Security Essentials.

Преди това Windows Defender е бил известен като Microsoft AntiSpyware.

Как да проверим Аваст колко битов е?

<https://forum.avast.com/index.php?topic=202068.0>

Как да проверим разрядността на нашата ОС

1. Click on the Start button then choose Settings.
2. Click on System.
3. Under System, choose About. You will be able to see the bit-version on the System type field.

Text

Description automatically generated

Avast

-Сигурност

-Ефективност

-Следи за нередности в мрежата

-Пази пароли

-Защита на данни

-Избягва фалшиви сайтове

-Тества всяка подозрителна програма

-Firewall

-Блокира спам

-Спира шпиониране през уеб камера

-Поддръжка на VPN

-Сканира подозрителни програми

Предимства на Avast:

-Споделени папки: споделянето на файлове, съдържащи се в споделени папки, е в основата на сървърната технология и е достъпно веднага след инсталирането на Windows Server Essentials.;

-Потребители и групи: при споделяне на папки и файлове трябва да се настроят разрешения. Потребителите и групите правят настройката лесна и управляема;

-Интеграция с хоствани услуги и приложения: лесно интегриране и внедряване на външни хоствани версии на Exchange, SharePoint, SQL Server и Windows Server Update Services чрез таблото за управление. Опциите за интеграция включват също Office 365 и Windows Azure.; Storage Spaces:

-Функция, позволяваща управление на съхранението на сървъра колективно, а не диск по диск. Това позволява лесно управление на съхранението.;

-Споделяне на медии: споделяне на видеоклипове, снимки и музика чрез интернет или мрежа.;

-Отдалечен достъп: позволява на служителите да работят от разстояние. Windows Server Essentials опростява процеса на формулиране на отдалечен достъп и дава възможност за достъп до мобилни устройства., Архивиране:

Сървърът на Windows Essentials лесно се конфигурира за архивиране на клиентски и сървърни файлове, (т.е. компютри с Windows 8, свързани към мрежата)., Здравни отчети: наблюдавайте и/или обработвайте сигнали и отчети за служителите., BranchCache: интегрирана функция, която ви позволява да сведете до минимум използването на интернет, като същевременно увеличите достъпа до данни чрез кеширане на входящи данни, постъпващи от външни източници., Икономичност: Цената на Windows Server Essentials е приблизително 500,00 USD и е по-евтина от другите версии на сървърите на Microsoft Windows и е по-евтина от закупуването на опции.

Недостатъци:

-Виртуализация: Тази програма не може да бъде реализирана като Hyper-V хост, освен това лицензът за сървър не включва права за виртуализация. Тя обаче може да се изпълнява чрез виртуална машина.

-Сървърно ядро: Windows Server Essentials не поддържа сървърно ядро, но целевият бизнес, който се нуждае от това решение, не би трябвало да изисква тази конкретна функция.

Active Directory Federation Services (ADFS): Windows Server Essentials не изисква Active Directory Federation Services (ADFS) за еднократна регистрация.

Exchange, SharePoint, SQL Server и Windows Server Update Services: могат да бъдат инсталирани отделно, обаче Windows Essentials Server има метод за това, предназначен да поддържа целевия пазар.