

Интернет заплахи

Видове заплахи в интернет пространството



How Secure is Your PC?

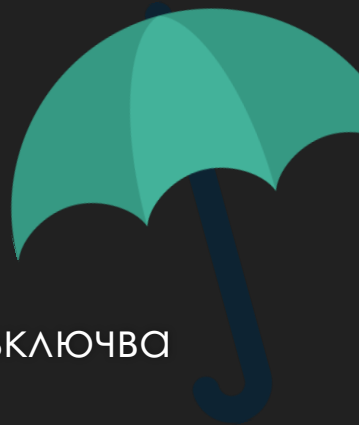
Лектор: Стефан Тафков

- Интернет заплахи
- Защо да се предпазваме
- Компрометиране сигурността на системата
- Инциденти по време на сърфиране
- Индустриален шпионаж
- Кражба на конфиденциална информация.
- Пробиви в системата с цел саботаж .
- Вътрешни заплахи
- Корпоративен шпионаж
- Корпоративно индивидуален шпионаж
- Недоволни служители

- Подкупни на служители
- Случайни пробиви
- Вируси (Malware)
- Привнесен саботаж.
- Външни заплахи интернет заплахи
- Какви заплахи ни дебнат в интернет
- Трябва да сме мнителни
- Защо сме прицел по време на сърфиране?
- Симолиране на заплаха
- Човешкия Фактор и неговото значение

Интернет заплахи

- Злонамерен софтуер (Malware):
- това е основен термин за софтуер, който е създаден със злонамерени цели. Той включва вирусни атаки, червеи, рекламен софтуер, троянски коне и шпионски софтуер.
- Атаки от тип „отказ от услуга“ (DoS): вид атака, която причинява загуба на услуга или невъзможност на мрежата да функционира.
- Уеб атаки: XSS (cross-site scripting), SQL injection (SQLi)
- “Отвличане” на HTTP сесии (Session hijacking): тези атаки представляват отвличане на идентификатора на потребителската сесия



Защо да се предпазваме



- Кражба на лични данни
- Шантаж
- Съботаж
- Загуба на клиенти!
- Губене на доверие между вас и клиентите ви !



Компрометиране сигурността на системата

- Какво е Хакер
- Хакерът и неговата роля.
- На какво е способен Хакера



Инциденти по време на сърфиране

- Инжектиране на зловреден код в системата ви
- Проследяване на дейността ви
- Подслушване

Индустриален шпионаж

- Кой би ни го причинил
- Защо се случва точно на нас
- Колко е сериозно
- Застрашава ли ни



Кражба на конфиденциална информация.

- Загуба на информация
- Каква е целта – кражба на клиенти
- Как ще се отрази на нашия бизнес

Пробиви в системата с цел саботаж .

- Заложени уязвимости в системата
- Заложени уязвимости в софтуера който използваме
- Привнесени пробиви – Чрез инсталиране на софтуер
- Поражения – загуба на информация

Вътрешни заплахи

- Корпоративен шпионаж
- Корпоративно индивидуален шпионаж
- Вътрешни политики
- Недоволни служители
- Подкупи на служители
- Случайни пробиви
- Вируси (Malware)
- Привнесен саботаж.

Корпоративен шпионаж

- Принципи на шпионажа
- С какво ни вреди
- Полезно ли е
- Корпоративният шпионаж е най-висшата вътрешна заплаха за сигурността. Важна задача, която стои пред всяка фирма е опазването на търговските тайни свързани с бизнеса.

Човешкият Фактор и неговото значение



Подкупни на служители

- Хора с ниски заплати .
- Хора недоволни от политиките на фирмата.
- Хора с прекалено много изисквания .
- Хора с проблеми.

Корпоративно индивидуален шпионаж

- Какво представлява
- Корпоративно индивидуален шпионаж е метод с който външни фирми или хора искат да се доберат до конкретна информация по точно определен проекти или случай.Този тип шпионаж е индивидуална насоченост.(Точно определена личност)Която незнае че е под чуждо влияние!

Външни атаки

- Denial-of-Service (DoS) Attacks
(Атака за отказ на услуга) “Man in the Middle” (MITM)
- Drive-By Downloads
- Malvertising
- Rogue Software
- Data Modification
- Application layer DDoS attack

Denial-of-Service (DoS) Attacks

(Атака за отказ на услуга)

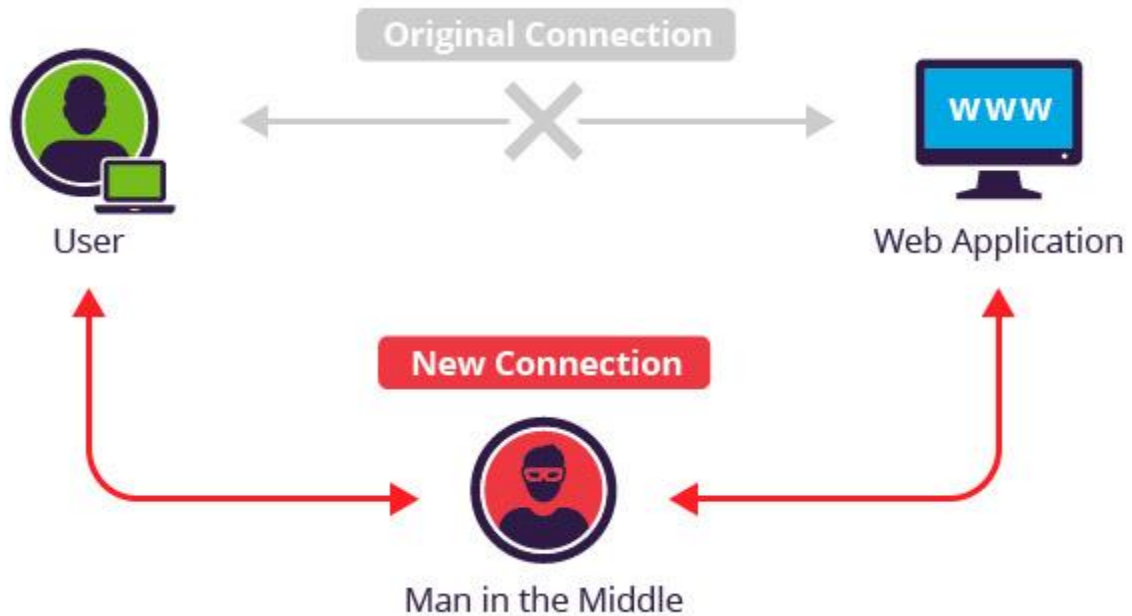
- Атака за отказ на услуга (denial-of-service attack, съкратено DoS attack — DoS атака) е опит дадена Фигура (Хакер), предоставян от чужд компютър (наричан жертва), да бъде направен недостъпен за интернет общността (Потребители). Принципите на атаката са да изпращат празни заявки до дадената система с цел изтопяване на нейните ресурси което ще доведе в определени случаи отказ за работа или срив в системата.

“Man in the Middle” (MITM)



- MITM атака е вид кибер атака, където хакер се внедрява в комуникационната сесия м/у две страни (потребители или сървъри), където подлъгва и се представя за 2те страни без те да знаят това.
- MITM е вид подслушване на разговор, в която хакера се внедрява в комуникацията като Proxy м/у 2 потребителя или сървъри
- MITM атаката действа в реално време следи финансови транзакции, разговори или трансфер на друга информация.
- MITM атака позволява на хакера да получава/изпраща информация насочена към някой друг без 2те страни да знаят това докато не е станало късно.

Man In The Middle Attack



Drive-By Downloads

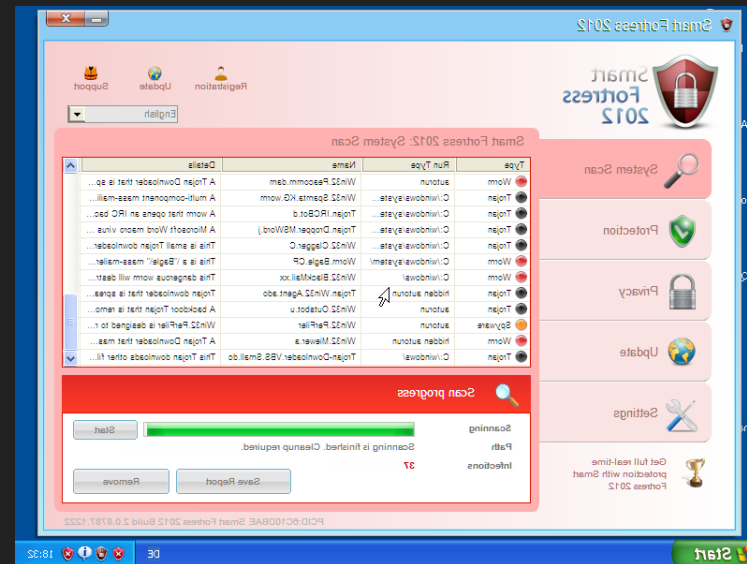
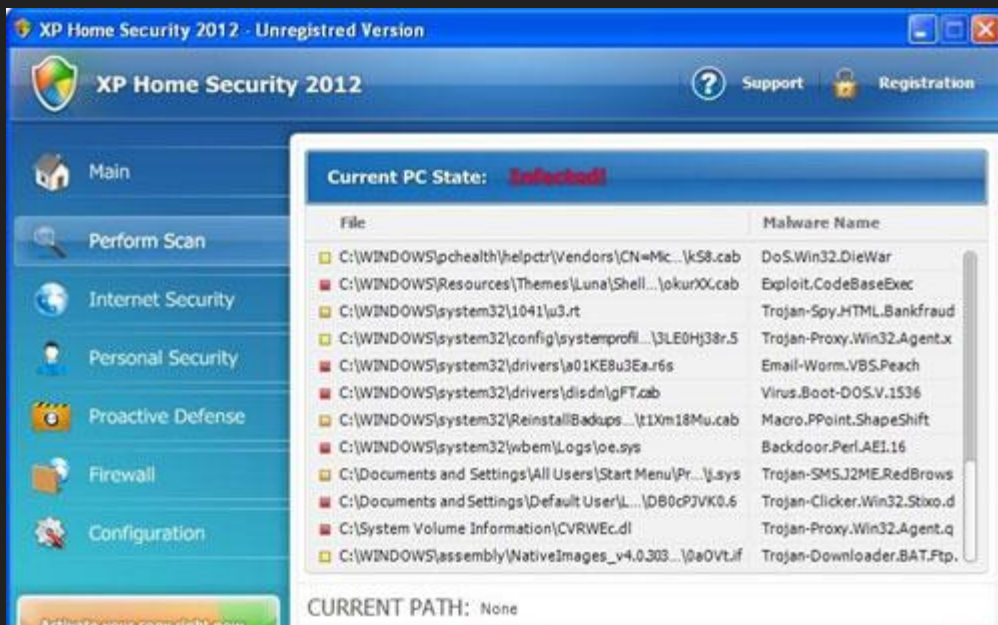
- Това е програма която автоматично се сваля на потребителския компютър без той да знае това. За тази атака са нужни две страни тази на Хакера и тази на потребителя. Като потребителя отвори линк към сайт или прекачен линк към email той отваря за достъп на хакера който може да нареди на програмата както да Краде информация така и да я унищожава. В повечето случаи това става през torrent тракери.

Malvertising

- Malvertising е начин хакера да придобие достъп и контрол над дадена система чрез.
- Приципа на атаката е потребителя да навигира курсора на мишката и да отвори заразен banner (реклама) която директно сваля и инсталира вредоносна програма на машината.

Rogue Software

- Rogue Software това е софтуер който се представя за друг легитимен софтуер с цел кражба на лична информация и най вече банкови сметки .

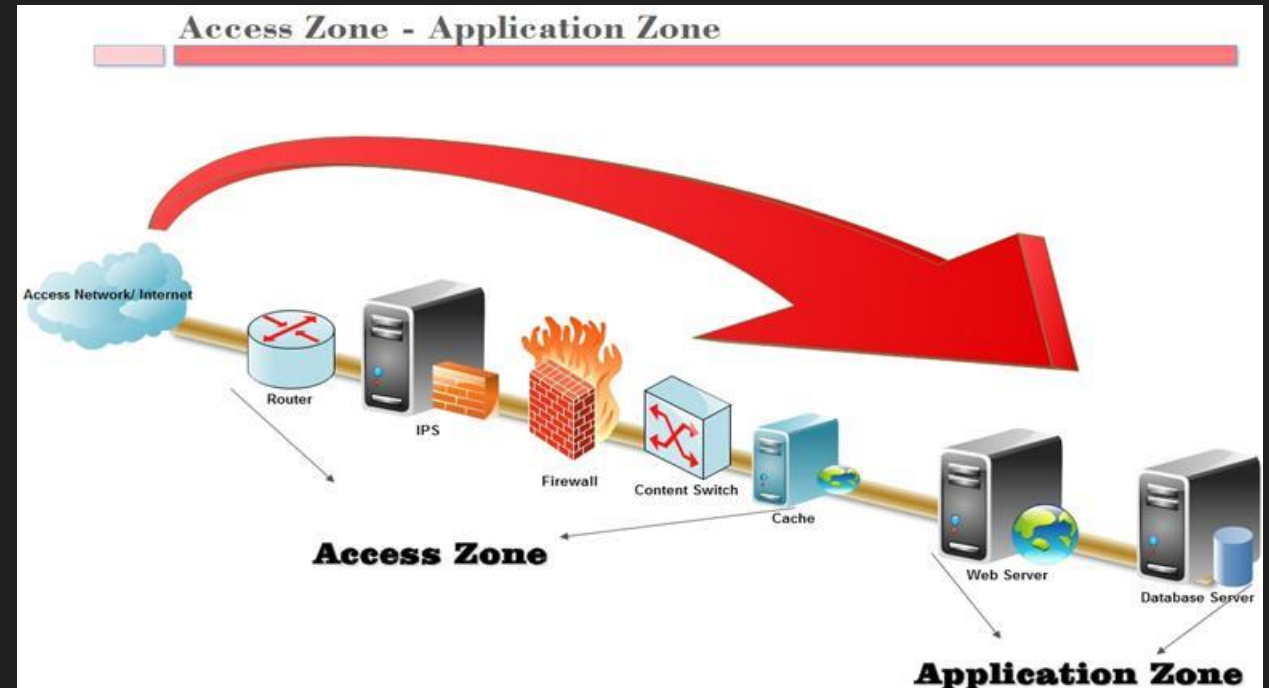


Data Modification

- Какво е Data Modification
- Това е похват на Хакера да се намесва в активна интернет сесия и да променя обстоятелства с цел кражба на информация .
- С тази атака Хакера може да наблюдава всичките ви кореспонденции и включително да се намесва в тях с цел изгода в повечето от случаите Финансова.

Application layer DDoS attack

- Този тип Интернет атака е с цел парализирането на системите който седят зад входящия интернет.



Недоволни служители

- Това са хора които или не харесват работната обстановка, или работодателя и неговата политика.
- С какво могат да ни навредят?
- Можем ли да променим мнението им?
- Колко би ни струвал такъв човек.

Случайни пробиви

- Това са най често атаки към комуникационните системи
- Не това не са омишлени нападения
- Понякога пробива помага за отриването на по сериозни заплахи
- Може ли да ни навреди

Вируси (Malware)



- Това са тези малки файлове които скапват работата!



Привнесен саботаж.

- Какво представлява
- Към кого е насочен
- - Секретарка
- -Чистачка
- - Всеки който ползва смарт устройство

Външни заплахи интернет заплахи

- Неоторизиран достъп чрез пароли и ключове
- Софтуер за мрежово следене
- ARP Positioning
- IP Spoofing
- DNS Spoofing
- DoS (Denial of Service) атаки
- TCP kill
- TCP nice
- SYN flood
- UDP flood attack
- ICMP flood

Какви заплахи ни дебнат в интернет

- Phishing(Риболов)
- banking Trojan(Банков Торянски кон)
- Key loggers(клавиатура плен)
- Network Sniff(анализация на интернет трафик)



Трябва да сме мнителни



- Защо ни е да сме мнителни
- Вичко което виждате на монитора може да е лъжа!



Защо сме прицел по време на сърфване?

- Какво значи това
- Има ли начини за разбиране дали сме прицел
- Колко време трае – Всичко зависи от поръчителя на атаката

Bye Bye

