Информациска безбедност

Предавање:
Злонамерен софтвер

Проф. д-р Весна Димитрова

Малициозен софтвер

- Овој софтвер е дизајниран за да ја пробие безбедноста на програмите. Бидејќи овој софтвер е злонамерен во неговата намера, му е доделено името malware (злонамерен, лош, пакостен).

- ***Вирус*** е малициозен софтвер кој се потпира на некој друг или на нешто друго за да се рашири од еден систем на друг. На пример, e-mail вирус се закачува самиот себеси на e-mail кој е пратен од еден корисник кон друг.

- ***Црв*** е слична форма на вирус кој се шири самиот себеси без потреба од надворешна асистенција.

Малициозен софтвер

- ***Тројански коњ*** или само ***тројанец***, е софтвер кој има некои неочекувани функционалности. На пример, навидум обична игра за деца може да направи штета додека корисник ја игра.

- ***Стапица*** или ***задна врата*** дозволува неавторизиран пристап до системот.

- ***Зајак*** е малициозна програма која ги истрошува системските ресурси. Зајакот може да биде имплементиран преку вирус, црв или други малициозни програми.

Малициозен софтвер

- Каде најчесто живеат вирусите во еден систем?
  - *Boot sector* вирусите живеат во *boot sector* -от, од каде што можат да превземат контрола во процесот на boot-ирање.
  - Друга класа на вируси се оние кои што живеат во меморија или memory resident вируси.
  - Вирусите исто така можат да живеат во апликации, макроа, податоци, библиотеки, компајлери, дебагери и дури и во анти-вирус програми.

Малициозен софтвер

- Првата форма на вируси била регистрирана од страна на Fred Cohen во 1980 година, кој демонстрирал како некој малициозен софтвер може да се искористи за да се разбие повеќе-нивовски безбедносен систем во тоа време.
- Првиот вирус кој се појавил и имал некое значење е *Brain* во 1986. Овој вирус не направил ништо штетно и затоа не ја пробудил љубопитноста кај луѓето.
- Голема узбуна настанала во 1988 година кога црвот *Morris* се појавил. Овој црв се уште останува интересен дел од малициозниот софтвер кој се разгледува.

Brain

- Вирусот ***Brain*** кој се појавил во 1986 е повеќе интересен за разгледување отколку штетен. Неговата важност е во тоа што тој е првиот вирус и како таков станува прототип за развој на многу вируси во иднина.
- И покрај јасното предупредување презентирано од страна на ***Brain*** вирусот, компјутерските системи остануваат екстремно подложни на вируси и малициозен софтвер.
- ***Brain*** вирусот се сместува во boot секторот и други места во системот. Потоа тој ги заштитува сите пристапи до дискот со цел да избегне детекција и да ја си ја одржи својата “инфекција”.
- Потоа откако ќе го прочита дискот, ***Brain*** ќе го провери boot секторот за да види дали тој е инфициран. Доколку не е, прво ќе се реинсталира самиот себеси во boot секторот, по што ќе стане тежок за отстранување.

Morris

- Безбедносната перспектива за компјутерскиот свет се менува засекогаш кога црвот ***Morris*** го нападнал Интернет во 1988 година. Важно е да се напомене дека Интернетот во 1988 година воопшто не наликувал на денешниот Интернет како што го знаеме.
  - Во тоа време, Интернет примарно е популаризан помеѓу академската заедница кои разменувале e-mail-ови и употребувале `telnet` за оддалечен пристап до супер – компјутерите.
- Црвот ***Morris*** бил паметно дизајниран и претставувал софистицирано решение во софтверска смисла, кој бил креиран и напишан од страна на студент од Cornell универзитетот.
- Црвот наводно требало да проверува дали некој систем е веќе инфициран пред да почне тој самиот да го инфицира. Но оваа проверка не била секогаш успешно направена, и така црвот се обидувал да ги ре-инфицира веќе инфицираните системи, што водело до исцрпување на ресурсите на системот.

Morris

- Малициозниот ефект кој што го постигнал ***Morris*** црвот бил всушност ефектот на таканаречен зајак (rabbit).
- Црвот ***Morris*** бил дизајниран да прави три работи:
  - да одреди каде може да ја шири својата инфекција
  - да ја рашири неговата инфекција кога е тоа можно
  - да остане неоткриен
- За да ја рашири својата инфекција, црвот Morris требало да добие оддалечен пристап до компјутерите на мрежата. За да го направи тоа црвот требало да ги погоди корисничките лозинки. Ако не успеел во тоа, тој почнувал да го преполнува баферот во `fingerd` (дел од Unix) и исто така да стави замка во `sendmail`.
- Откако ќе бил добиен пристап на некој компјутер од системот, црвот праќал “подигнувач со подигната рака” на жртвата. Овој подигнувач се состоел од 99 линии на C код, кој компјутерот на жртвата го компајлирал и извршувал. Овој подигнувач потоа го превземал остатокот од црвот. Во овој процес, компјутерот на жртвата можел дури и да го автентицира испраќачот.

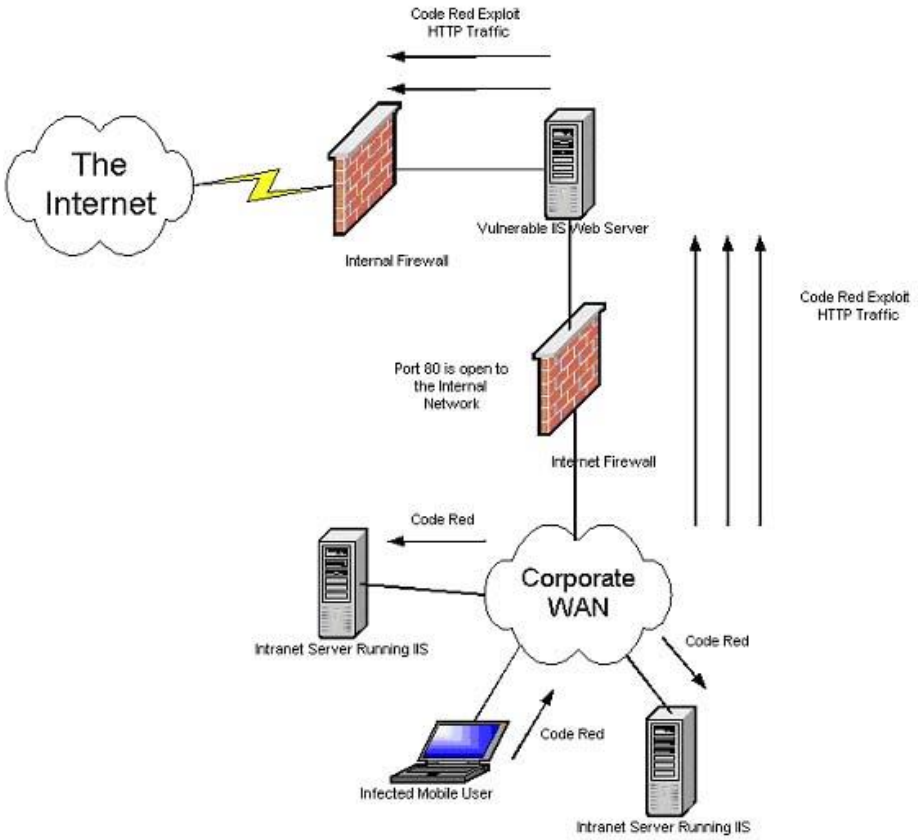
Morris

- Ако преносот на црвот се прекинел, целиот код од преносот ќе бил избришан. Кодот исто така се енкриптирал во време на превземање, и превземениот изворен код се бришел откако бил декриптиран и компајлиран.
- Кога црвот се извршувал на систем, тој периодично го менувал неговото име и неговиот идентификатор на процес (PID), за да систем администраторот не примети ништо сомнително.
- ***Morris*** црвот ја шокирал Интернет заедницата во 1988 година. Во тоа време за Интернет се претпоставувало дека може да преживее нуклеарен напад, но тој дошол до критичен застој предизвикан од студент и неколку стотици линии на C код.
- Многу малку експерти, ако не и ниеден, не ни сонувале дека Интернет може да подлежи на таков вид напади.
- Како директен резултат на нападот на Morris црвот, е формирана CERT (Computer Emergency Response Team), која е и до ден денеска прва “куќа за чистење” кога станува збор за информации поврзани со компјутерската безбедност.

Code red

- Кога се појавил Code red во Јули 2001 бил способен да инфицира повеќе од 250 000 компјутери во временски период од 10 до 15 часа. Пред да биде јавно откриен тој веќе имал инфицирано повеќе од 750 000 од вкупно 6 000 000 осетливи компјутерски системи низ светот.
- За да добие пристап до системот Code red црвот го искористувал преполнувањето на баферот. Тој го прател сообраќајот на порта 80, барајќи други осетливи сервери.
- Малициозните акции на Code red зависеле од денот. Од ден 1 до ден 19 во месецот тој се ширел во сите осетливи системи, а од 20 до 27 правел т.н. DDos напад (distributed denial of service).
- Се претпоставувало дека Code red е некаков бета тест за војна со инфомации меѓутоа тоа никогаш не било докажано.

Code red



Пример за Code Red

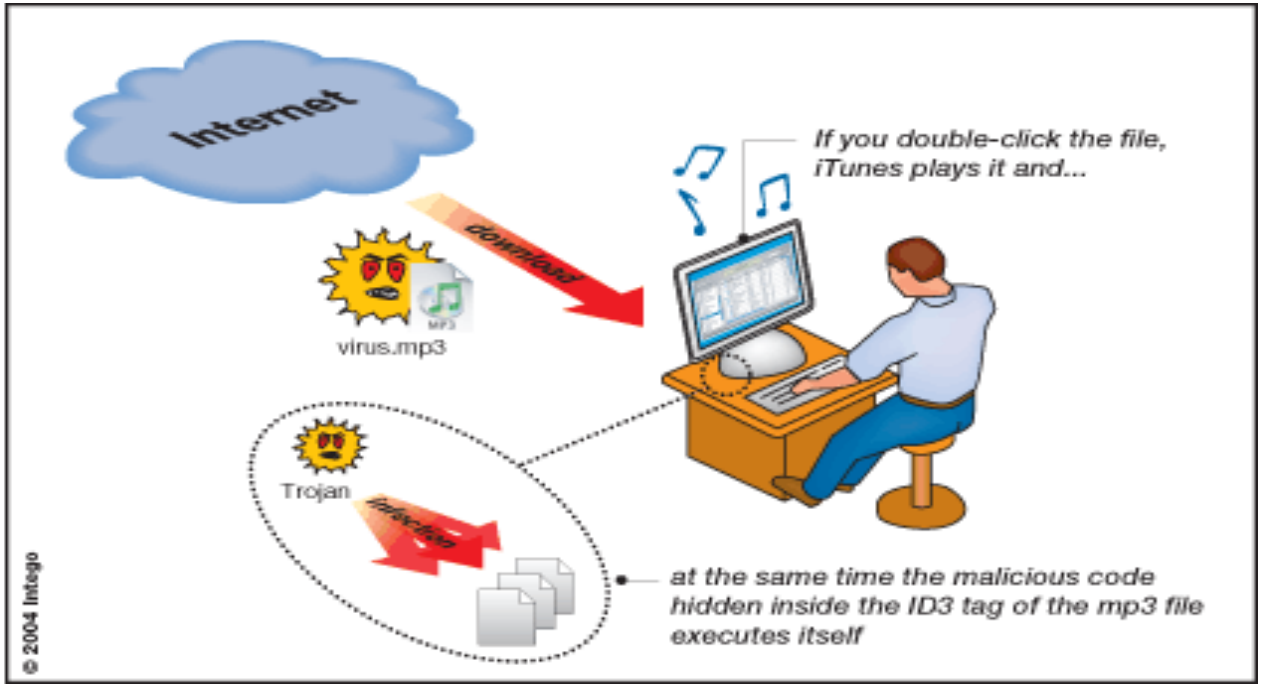
SQL Slammer

- SQL Slammer црвот се појавил летото 2004 кога успеал да инфицира 250000 компјутерски системи за само 10 минути.
- Кратка споредба: SQL Slammer црвот инфицирал за 10 минути онолку компјутери колку што инфицирал Code Red за 15 часа.
- Кај овој црв бројот на инфицирани компјутери се дуплирал на секои 8.5 секунди. Истражувањата покажуваат дека SQL Slammer се ширел многу брзо и ефективно го искористувал слободниот пропусен опсег (bandwidth) на Интернет.Тој всушност го зголемувал сообраќајот на Интернет. Овој црв всушност кога ќе инфицирал еден сајт барал нови ослабени сајтови по случајно избрани IP адреси.
- Зошто всушност бил овој црв толку успешен? Заради една едноставна работа, овој црв се ставал во еден 376- бајтен UDP пакет. Firewall –от е честопати конфигуриран да пропушта мали пакети претпоставувајќи дека еден таков пакет не може да му наштети на системот. После тоа Firewall-от ја надгледува конекцијата да види дали нешто необично ќе се случи. Бидејќи било очекувано дека многу повеќе од 376 бајти би биле потребни за напад овој црв успешно се пробивал низ заштитата на компјутерите.

Тројанец

- Тројанец - тоа е програм што се појавува како нешто што всушност не е. Тројанецот доаѓа од светот на Мекинтош. Неговиот креатор може многу лесно да го направи да биде малициозен.
- Обичниот тројанец најчесто се јавува во аудио форма и тоа MP3 и скоро сите корисници го симнуваат и извршуваат односно отвараат незнаејќи дека тоа всушност не е некоја песна туку дека се работи за некаква апликација. Откако ќе се отвори штетата што може да ја направи тројанецот зависи од неговиот креатор т.е. од тоа како е испрограмиран.

Пример за тројанец



Пример за Тројанец

Malware Detection

- Постојат 3 најчесто користени методи за препознавање malware.
- **Детекција со потпис**, се потпира на пронаоѓање потпис кој е присутен во одреден дел од malware
- **Детекција на промени,** наоѓа датотеки кои се промениле, датотеката која е неочекувано променета може да укажува на инфекција
- **Откривање аномалија,** целта е откривање на необични вирус датотеки

Malware Detection - детекција со потпис

- Потписот е генерално низа од битови кој се наоѓа во некоја датотека
- Пример: вирусот содржи низа од битови 0x23956a58bd910345 и тогаш можеме да земеме во обзир дека овој стринг ќе биде потпис за вирусот и оваа низа од битови ќе ја бараме во сите датотеки на системот
- Дали во сите датотеки во кои сме ја пронашле оваа низа од битови мора да има вирус?

Malware Detection - детекција со потпис

- Предности:

- минимален товар на корисниците и администраторите, бидејќи се што е потребно е повремено да се скенира од вируси

- Недостатоци:

- може датотеките да бидат големи, па скенирањето ќе биде многу бавно

- може да се користи само за откривање на познати вируси, така што варијанта на некој познат вирус може да биде пропуштена односно да не биде детектирана

Malware Detection - детекција на промени

- Ако се детектира некаде промена во системот, тогаш тоа може да укажува на инфекција
- Доколку се детектира дека датотеката се променила таа може да биде заразена со вирус
- Како можат да се детектираат промените?
  - Хаш функциите се корисни во овој поглед. Ако ги пресметаме сите хаш вредности на сите датотеки на системот за безбедно складирање, можеме да ги пребројиме хаш вредностите и да ги споредиме со новите вредности и ако датотеката се променила во една или повеке позиции ќе видиме дека новата хаш не се совпаѓа со предходната, па тогаш се работи за вирусна инфекција.

Malware Detection - детекција на промени

- Предности:

- можеме да откриеме непознат вирус

Недостатоци:

- датотеки често се менуваат, како резултат на тоа ќе има многу лажно-позитивни резултати кои оставаат работа на администраторите и корисниците

Malware Detection - откривање аномалија

- Откривање на аномалија е насочено кон наоѓање на необичен вирус или друга штетна активност
- Основниот предизвик со аномалија е одредувањето на она што е нормално и она што е невообичаено. Системот мора да се адаптира на промени или ризици со лажни аларми.

Malware Detection - откривање аномалија

- Предности:

- има шанси за откривање на предходно непознати инфекции

- Недостатоци:

- Аномалија како детекција не е доволно силна да се користи самостојно и затоа најчесто се комбинира со потпис

Доверлив Софтвер

- Како знаеме кој софтвер е доверлив?
- Што се случува ако во нашиот компајлер е вметнат вирус?
- Што се случува ако со ваков компајлер го рекомпалјираме оперативниот систем?
- Што ќе се случи ако се вметне вирус во софтверот што треба да го детектира?