Рачунарство и друштво - Безбедност рачунара и мрежа

Данијела Симић

5. мај 2021.

Математички факултет
Универзитет у Београду

Садржај

Безбедност рачунара и мрежа

- Да ли користите мреже које су доступне у кафићима, ресторанима, хотелима?

Безбедност рачунара и мрежа

- Да ли користите мреже које су доступне у кафићима, ресторанима, хотелима?
- Да ли је могуће да терористичка организација хакује рачунаре и управља саобраћајним знаковима или напајањем струје (*"Умри мушки 3"*)?

Безбедност рачунара и мрежа

- Да ли користите мреже које су доступне у кафићима, ресторанима, хотелима?
- Да ли је могуће да терористичка организација хакује рачунаре и управља саобраћајним знаковима или напајањем струје (*"Умри мушки 3"*)?
- Да ли преузимате непроверен софтвер?

Хаковање

Хаковање – прошлост, 1950 - 1960

- **Хакер** – истраживач, особа која преузима ризик, неко ко чини да систем ради нешто ново.
- Направили су електронски систем који је контролисао кретање возова.
- Појавом рачунара, за хакере се сматрају експерти који одлично познају систем и мреже.

Хаковање – прошлост, 1983. година

- 1983. године приказан је филм “Ратне игре” (енг. *War Games*).

Хаковање – прошлост, 1983. година

- 1983. године приказан је филм "Ратне игре" (енг. *War Games*).
- У филму тинејџер успева да нападне војни рачунар и умало изазове нуклеарну катастрофу.

Хаковање – прошлост, 1983. година

- 1983. године приказан је филм "Ратне игре" (енг. *War Games*).
- У филму тинејџер успева да нападне војни рачунар и умало изазове нуклеарну катастрофу.
- Након филма, велики број тинејџера добија надахнуће и верује да са рачунаром и модемом може да нападне државне институције.

Хаковање – прошлост, 1983. година

- 1983. године приказан је филм "Ратне игре" (енг. *War Games*).
- У филму тинејџер успева да нападне војни рачунар и умало изазове нуклеарну катастрофу.
- Након филма, велики број тинејџера добија надахнуће и верује да са рачунаром и модемом може да нападне државне институције.
- Нколицини то и полази за руком

Хаковање – данас

Хакер

Особа која неовлашћено приступа рачунарима и рачунарским мрежама.

Хаковање

- Хакеру је потребно корисничко име и шифра да би упао у неки систем и веома су вешти у њиховом проналажењу.

Хаковање

- Хакеру је потребно корисничко име и шифра да би упао у неки систем и веома су вешти у њиховом проналажењу.

Хаковање

- Хакеру је потребно корисничко име и шифра да би упао у неки систем и веома су вешти у њиховом проналажењу.

2013. године *Ars Technica* је питала три хакера да покушају да нападну листу од 16.000 хешираних шифри.

Хаковање

- Хакеру је потребно корисничко име и шифра да би упао у неки систем и веома су вешти у њиховом проналажењу.

2013. године *Ars Technica* је питала три хакера да покушају да нападну листу од 16.000 хешираних шифри.

Најмање успешном од њих је требало сат времена да идентификује 62% свих шифри.

Хаковање

- Хакеру је потребно корисничко име и шифра да би упао у неки систем и веома су вешти у њиховом проналажењу.

2013. године *Ars Technica* је питала три хакера да покушају да нападну листу од 16.000 хешираних шифри.

Најмање успешном од њих је требало сат времена да идентификује 62% свих шифри.

Најуспешнијем је требало 20 сати да идентификује 90% свих шифри.

Хаковање – коришћене технике

Коришћена техника: помоћу рачунара направе листу шифри, хеширају је и онда ту листу пореде са листом хешираних шифри која им је дата.

Хаковање – коришћене технике

Коришћена техника: помоћу рачунара направе листу шифри, хеширају је и онда ту листу пореде са листом хешираних шифри која им је дата.

За кратке шифре: користи се метод грубе силе

- Генеришу скуп од 95 карактера (26 великих слова, 26 малих слова, 10 цифара и 33 симбола)

Хаковање – коришћене технике

Коришћена техника: помоћу рачунара направе листу шифри, хеширају је и онда ту листу пореде са листом хешираних шифри која им је дата.

За кратке шифре: користи се метод грубе силе

- Генеришу скуп од 95 карактера (26 великих слова, 26 малих слова, 10 цифара и 33 симбола)
- За шифру дужине 6 направе $95^6 \sim 744$ милијарде различитих шифри.

Хаковање – коришћене технике

Коришћена техника: помоћу рачунара направе листу шифри, хеширају је и онда ту листу пореде са листом хешираних шифри која им је дата.

За кратке шифре: користи се метод грубе силе

- Генеришу скуп од 95 карактера (26 великих слова, 26 малих слова, 10 цифара и 33 симбола)
- За шифру дужине 6 направе $95^6 \sim 744$ милијарде различитих шифри.
- Рачунару је потребно неколико минута да испроба све ове шифре.

Хаковање – коришћене технике

За дугачке шифре: користи се напад коришћењем методе *речника*. У речнику се налазе речи из (енгелског) језика, као и најчешће коришћене шифре.

Хаковање – коришћене технике

За дугачке шифре: користи се напад коришћењем методе *речника*. У речнику се налазе речи из (енгелског) језика, као и најчешће коришћене шифре.

У *Ars Technica* експерименту су коришћењем методе речника погодили шифре као што су: *“Apr!l221973”*, *“ilovemySister31”*, *“Philippians4:6-7”*.

Хаковање – правила за креирање шифри и добру заштиту i

Одговорни људи воде рачуна о избору шифре:

- Препорука је да шифра буде минималне дужине 11 карактера.
- Не користити речи из речника.
- Не користити властита имена и датуме, године рођења и слично.
- Не ослањати се на замену бројева и слова (нпр. *jabuke* – *j4buk3*).
- Не користити старе шифре.
- Дати неочекиване одговоре на сигуносна питања.

Хаковање – правила за креирање шифри и добру заштиту ii

- Омогућити двофакторску аутетификацију ако је подржана системом.
- Омогућити начин за повратак шифре (остављањем још једног сигурносног мејла или броја телефона).

Хаковање

Напад у оквиру бесплатане WiFi мреже

Хаковање – *http* vs *https*

- Већина информација која се преноси путем интернета се преноси коришћењем HTTP протокола (HyperText Transport Protocol).

Хаковање – *http* vs *https*

- Већина информација која се преноси путем интернета се преноси коришћењем HTTP протокола (HyperText Transport Protocol).
- Веома мали проценат пакета се енкриптује.

Хаковање – *http* vs *https*

- Већина информација која се преноси путем интернета се преноси коришћењем HTTP протокола (HyperText Transport Protocol).
- Веома мали проценат пакета се енкриптује.
- Енкриптовање свега би направило Интернет споријим и скупљим.

Хаковање – *http* vs *https*

- Већина информација која се преноси путем интернета се преноси коришћењем HTTP протокола (HyperText Transport Protocol).
- Веома мали проценат пакета се енкриптује.
- Енкриптовање свега би направило Интернет споријим и скупљим.
- Веб страна која енкриптује почиње са https:// (secure HyperText Transport Protocol).

Хаковање – *http* vs *https*

- Већина информација која се преноси путем интернета се преноси коришћењем HTTP протокола (HyperText Transport Protocol).
- Веома мали проценат пакета се енкриптује.
- Енкриптовање свега би направило Интернет споријим и скупљим.
- Веб страна која енкриптује почиње са https:// (secure HyperText Transport Protocol).
- На WiFi мрежи, пакети који нису енкриптовани су изложени нападу.

Хаковање – напад у оквиру бесплатане WiFi мреже

Напад у оквиру бесплатне WiFi мреже (енг. *Sidejacking*)

Напад у оквиру бесплатне WiFi мреже је врста напада када хакер "ухвати" колачић који веб страна шаље кориснику. На основу колачића, хакер добија приступ сајту и иста права и могућности као и регистровани корисник који је нападнут.

Хаковање – напад у оквиру бесплатане WiFi мреже

- Веб сајтови најчеће користе енкрипцију приликом слања корисничког имена и лозинке.

Хаковање – напад у оквиру бесплатане WiFi мреже

- Веб сајтови најчеће користе енкрипцију приликом слања корисничког имена и лозинке.
- Али, најчешће не користе енкрипцију када шаљу колачиће кориснику да би наставио рад у оквиру сесију.

Хаковање – напад у оквиру бесплатане WiFi мреже

- Веб сајтови најчеће користе енкрипцију приликом слања корисничког имена и лозинке.
- Али, најчешће не користе енкрипцију када шаљу колачиће кориснику да би наставио рад у оквиру сесију.
- Многи су знали за овај пропуст. Нападачи су га користили, корисници се бунили, а веб странице се нису мењале . . .

Хаковање – Firesheep

- Firesheep је екстензија за *Firefox* написана 2010. године.

Хаковање – Firesheep

- Firesheep је екстензија за *Firefox* написана 2010. године.
- Коришћењем *Firesheep* ектензије сваки корисник може да преузме колачиће неенкриптоване веб стране.

Хаковање – Firesheep

- Firesheep је екстензија за *Firefox* написана 2010. године.
- Коришћењем *Firesheep* ектензије сваки корисник може да преузме колачиће неенкриптоване веб стране.
- **Како функционише:**

Хаковање – Firesheep

- Firesheep је екстензија за *Firefox* написана 2010. године.
- Коришћењем *Firesheep* ектензије сваки корисник може да преузме колачиће неенкриптоване веб стране.
- **Како функционише:**
  - корисник се прикачи на мрежу и притисне дугме *Start Capturing*

Хаковање – Firesheep

- Firesheep је екстензија за *Firefox* написана 2010. године.
- Коришћењем *Firesheep* ектензије сваки корисник може да преузме колачиће неенкриптоване веб стране.
- **Како функционише:**
  - корисник се прикачи на мрежу и притисне дугме *Start Capturing*
  - *Firesheep* региструје колачиће који се размењују у оквиру незаштићене WiFi мреже

Хаковање – Firesheep

- Firesheep је екстензија за *Firefox* написана 2010. године.
- Коришћењем *Firesheep* ектензије сваки корисник може да преузме колачиће неенкриптоване веб стране.
- **Како функционише:**
  - корисник се прикачи на мрежу и притисне дугме *Start Capturing*
  - *Firesheep* региструје колачиће који се размењују у оквиру незаштићене WiFi мреже
  - када "ухвати" колачић, кориснику се прикаже слика жртве, корисничко име жртве, као и сајт који користи (Amazon, Facebook, Twitter)

Хаковање – Firesheep

- Firesheep је екстензија за *Firefox* написана 2010. године.
- Коришћењем *Firesheep* ектензије сваки корисник може да преузме колачиће неенкриптоване веб стране.
- **Како функционише:**
  - корисник се прикачи на мрежу и притисне дугме *Start Capturing*
  - *Firesheep* региструје колачиће који се размењују у оквиру незаштићене WiFi мреже
  - када "ухвати" колачић, кориснику се прикаже слика жртве, корисничко име жртве, као и сајт који користи (Amazon, Facebook, Twitter)
  - двоструким кликом на слику, корисник постаје улогован у сајт као жртва напада и има надаље иста права као и жртва.

Хаковање – Firesheep

- Већ прве недеље имао је преко 500.000 преузимања.

Хаковање – Firesheep

- Већ прве недеље имао је преко 500.000 преузимања.
- Аутор (Eric Butler) је сматрао да је ово начин да се скрене пажња великим компанијама на пропусте на њиховим странама и да се заштите корисници од нападача.

Хаковање – Firesheep

- Већ прве недеље имао је преко 500.000 преузимања.
- Аутор (Eric Butler) је сматрао да је ово начин да се скрене пажња великим компанијама на пропусте на њиховим странама и да се заштите корисници од нападача.
- Три месеца након појављивања ове екстензије, *Facebook* је понудио опцију да сва комуникација иде коришћењем *https* протокола.

Хаковање – Firesheep и етика

Да ли је креирање Firesheep екстензије етички оправдан поступак?

- утилитаризам поступака

Хаковање – Firesheep и етика

Да ли је креирање Firesheep екстензије етички оправдан поступак?

- утилитаризам поступака
- етика врлине

Хаковање – Firesheep и етика

Да ли је креирање Firesheep екстензије етички оправдан поступак?

- утилитаризам поступака
- етика врлине
- кантијанизам

Хаковање

Казне за хакере

Казне за хакере – Изводи из кривичног закона Републике Србије

Сваки неовлашћен приступ рачунарској мрежи од стране хакера подлеже под чланове 302,303 и 304 Кривичног закона Републике Србије.

Казне за хакере – Изводи из кривичног закона Републике Србије

Члан 302: Неовлашћени приступ заштићеном рачунару, рачунарској мрежи или електронској обради података

1. Ко се, кршећи мере заштите неовлашћено укључи у рачунар или рачунарску мрежу или неовлашћено приступи електронској обради података, казниће се новчаном казном или затвором до шест месеци.
2. Ко употреби податак добијен на начин предвиђен у ставу 1 овог члана, казниће се новчаном казном или затвором до две године.
3. Ако су услед дела из става 1. овог члана дошло до застоја или озбиљног поремећаја функционисања електронске обраде и преноса података или мреже или су наступиле друге тешке последице, учинилац ће се казнити затвором до три година.

Казне за хакере – Изводи из кривичног закона Републике Србије

Члан 303: Спречавање и ограничавање приступа јавној рачунарској мрежи

1. Ко неовлашћено спречава или омета приступ јавној рачунарској мрежи,казниће се новчаном казном или затвором до једне године.
2. Ако дело из става 1 овог члана учини службено лице у вршењу службе, казниће се затвором до три године.

Казне за хакере – Изводи из кривичног закона Републике Србије

Члан 304: Неовлашћено коришћење рачунара или рачунарске мреже

1. Ко неовлашћено користи рачунарске услуге или рачунарску мрежу у намери да себи или другом прибави противправну имовинску корист, казниће се новчаном казном или затвором до три месеца.
2. Гоњење за дело из става 1. овог члана предузима се по приватној тужби.

Казне за хакере – Сједињене Америчке Државе

- У случају кршења закона који се односи на рачунарску превару, новчана казна може бити до 250.000$, док затворска може бити и 20 година.

Злонамерни софтвер

Злонамерни софтвер

Злонамерни софтвер (енг. *malware*) је софтвер дизајниран да нанесе штету циљном кориснику.

Злонамерни софтвер

Злонамерни софтвер (енг. *malware*) је софтвер дизајниран да нанесе штету циљном кориснику.

Мање опасни програми могу заузети процесорско време или меморију и успорити рад рачунара.

Злонамерни софтвер

Злонамерни софтвер (енг. *malware*) је софтвер дизајниран да нанесе штету циљном кориснику.

Мање опасни програми могу заузети процесорско време или меморију и успорити рад рачунара.

Опаснији злонамерни софтвер може уништити податке на рачунару или омогућити нападачу да преузме контролу над рачунаром. Тако, могу доћи до података о кориснику (шифре и кредитне картице) или могу користити жртвин рачунар за нелегалне активности.

Злонамерни софтвер

Вируси

Вируси

Вирус је програмски код који се самореплицира (прави сопствене копије) и део је другог програма који се зове домаћин (енг. *host*).

Вируси

Вирус је програмски код који се самореплицира (прави сопствене копије) и део је другог програма који се зове домаћин (енг. *host*).

Неки вируси заузимају само меморију и процесорско време.

Неки могу направити велику штету.

Вируси – начин рада

Начин функционисања:

- Корисник покрене програм који је домаћин вирусу.

Вируси – начин рада

Начин функционисања:

- Корисник покрене програм који је домаћин вирусу.
- Прво се покреће извршавање вируса.

Вируси – начин рада

Начин функционисања:

- Корисник покрене програм који је домаћин вирусу.
- Прво се покреће извршавање вируса.
- Вирус проналази други извршиви програм и мења га са извршивим програмом који у себи садржи вирус.

Вируси – начин рада

Начин функционисања:

- Корисник покрене програм који је домаћин вирусу.
- Прво се покреће извршавање вируса.
- Вирус проналази други извршиви програм и мења га са извршивим програмом који у себи садржи вирус.
- Након тога се извршва програм који је домаћин.

Вируси – начин рада

Начин функционисања:

- Корисник покрене програм који је домаћин вирусу.
- Прво се покреће извршавање вируса.
- Вирус проналази други извршиви програм и мења га са извршивим програмом који у себи садржи вирус.
- Након тога се извршва програм који је домаћин.
- Ако се вирус брзо извршава, корисник неће ни приметити његов рад.

Вируси – начин преношења

- Вируси се могу наћи свуда где се налазе и програми домаћини: хард сискови, преносиви дискови, CD дискови ...

Вируси – начин преношења

- Вируси се могу наћи свуда где се налазе и програми домаћини: хард сискови, преносиви дискови, CD дискови ...
- Преносе се са машине на машину коришћењем: преносивих дискова, CD дискова или се могу преузети са Интернета, бити прикачени као извршиви програми у имејлу.

Вируси – начин преношења

- Вируси се могу наћи свуда где се налазе и програми домаћини: хард сискови, преносиви дискови, CD дискови ...
- Преносе се са машине на машину коришћењем: преносивих дискова, CD дискова или се могу преузети са Интернета, бити прикачени као извршиви програми у имејлу.
- Данас се најчешће преносе преко имејл порука. Чак и поруке које не садрже извршиви програм могу бити проблематичне. Рецимо, текстуални документ или табеле могу садржати макрое који се кликом на документ активирају и на тај начин се вирус покреће.

Вируси – антивирусни софтвер

Антивирусни софтвер проналази у уништава копије вируса и спречава нападе новим вирусом. Ипак, овај софтвер зависи од базе вируса на основу које се ослања.

- Према статистикама Европске Уније, 31% Интернет корисника је било заражено са вирусом у току 2016. године.
- Чак 84% од њих је имало инсталиран антивирусни софтвер.
- То говори да људи ретко воде рачуна о ажурирању базе антивирусног софтвера.

Злонамерни софтвер

Рачунарски црви

Интернет црв

Интернет црв је самостални програм који се шири рачунарима на мрежи искоришћавањем рупа у безбедности на рачунарима повезаним на мрежу.

Интернет црв и Роберт Морис

- Отац Роберта Мориса је радио у Беловим лабораторијама и Роберт Морис је имао приступ рачунарима и упознао се са *Unix* системом.

Интернет црв и Роберт Морис

- Отац Роберта Мориса је радио у Беловим лабораторијама и Роберт Морис је имао приступ рачунарима и упознао се са *Unix* системом.
- Већ 1982. године пронашао је безбедносне рупе у систему које је искористио да се улогује на систем и чита туђе мејлове.

Интернет црв и Роберт Морис

- Отац Роберта Мориса је радио у Беловим лабораторијама и Роберт Морис је имао приступ рачунарима и упознао се са *Unix* системом.
- Већ 1982. године пронашао је безбедносне рупе у систему које је искористио да се улогује на систем и чита туђе мејлове.
- Као студент радио је у Беловим лабораторијама и важио је за *Unix* експрерта. Ипак, често је користио пропусте у систему да се нашали са колегама (нпр. логовање и *Пророчиште*).

Интернет црв и Роберт Морис

- 1988. године је открио пропусте у три програма: `ftp`, `sendmail`, `fingerd`.

Интернет црв и Роберт Морис

- 1988. године је открио пропусте у три програма: `ftp`, `sendmail`, `fingerd`.
- Црв је откривао шифре и нападао све рачунаре на мрежи заузимајући процесорко време.

Интернет црв и Роберт Морис

- 1988. године је открио пропусте у три програма: `ftp`, `sendmail`, `fingerd`.
- Црв је откривао шифре и нападао све рачунаре на мрежи заузимајући процесорко време.
- Услед грешке у самом коду црва, црв се копирао на исте рачунаре по пар стотина пута. Рачунари су се нон стоп гасили и постали су неупотребљиви.

Интернет црв и Роберт Морис

- 1988. године је открио пропусте у три програма: `ftp`, `sendmail`, `fingerd`.
- Црв је откривао шифре и нападао све рачунаре на мрежи заузимајући процесорко време.
- Услед грешке у самом коду црва, црв се копирао на исте рачунаре по пар стотина пута. Рачунари су се нон стоп гасили и постали су неупотребљиви.
- Брзо се проширио на све рачунаре војске, болница и направио је вишемилионску штету. Током два дана велики број система је био неупотребљив.

Интернет црв и Роберт Морис

- 1988. године је открио пропусте у три програма: `ftp`, `sendmail`, `fingerd`.
- Црв је откривао шифре и нападао све рачунаре на мрежи заузимајући процесорко време.
- Услед грешке у самом коду црва, црв се копирао на исте рачунаре по пар стотина пута. Рачунари су се нон стоп гасили и постали су неупотребљиви.
- Брзо се проширио на све рачунаре војске, болница и направио је вишемилионску штету. Током два дана велики број система је био неупотребљив.
- Роберт Морис је избачен са Корнел универзитета, добије је 400 сати корисно–друштвеног рада и казну од 100.000$.

Сасер

Сасер је црв који се појавио 2004. године и искористио је безбедносни пропуст у рачунарима који су имали *Windows XP* или *Windows 2000* оперативни систем. Инфицирани рачунари би се искључили неко време након подизања система.

Сасер

- *Microsoft* је увидео пропуст и послао је исправку.

Сасер

- *Microsoft* је увидео пропуст и послао је исправку.
- Ипак, 18 милиона рачунара широм света се “заразило” овим црвом.

Сасер

- *Microsoft* је увидео пропуст и послао је исправку.
- Ипак, 18 милиона рачунара широм света се “заразило” овим црвом.
- Изазавао је проблеме у раду аустралијских железница, *Delta Airlines*, британске обалске страже, европске комисије итд.

Сасер

- *Microsoft* је понудио награду од 250.000$ за откривање починиоца.

Сасер

- *Microsoft* је понудио награду од 250.000$ за откривање починиоца.
- Након изјаве школског друга, откривено је да је немачки тинејџер Свен (нем. *Sven Jaschan*) творац вируса.

Сасер

- *Microsoft* је понудио награду од 250.000$ за откривање починиоца.
- Након изјаве школског друга, откривено је да је немачки тинејџер Свен (нем. *Sven Jaschan*) творац вируса.
- Како је био малолетник, осуђен је на 30 сати корисно–друштвеног рада.

Црви у апликацијама за инстант поруке

- 2001. године су се појавили први црви који су нападали апликације за слање инстант порука.

Црви у апликацијама за инстант поруке

- 2001. године су се појавили први црви који су нападали апликације за слање инстант порука.
- Ипак, тада је број корисника ових апликација био мали.

Црви у апликацијама за инстант поруке

- 2001. године су се појавили први црви који су нападали апликације за слање инстант порука.
- Ипак, тада је број корисника ових апликација био мали.
- 2005. године црв *Kelvir* је натерао *Microsoft* да избрише 60.000 својих корисника.

Conficker

- *Conficker* (или Downadup) црв је нападао *Windows* оперативни систем.
- Било га је веома тешко очистити и веома лако се ширио (преносива меморија и системи са слабом шифром).
- Заразио је око 15 милиона рачунара, укључујући француске, британске и немачке војне рачунаре.
- Иако су милиони црва циркулисали мрежом није нанео велику штету. Није јасно који циљ су имали његови творци.

Злонамерни софтвер

Укрштање веб локација (енг. *Cross-Site Scripting*)

Укрштање веб локација (енг. *Cross-Site Scripting*)

- Ова врста напада се дешава на оним веб странама где корисници могу оставити своје коментаре.

Укрштање веб локација (енг. *Cross-Site Scripting*)

- Ова врста напада се дешава на оним веб странама где корисници могу оставити своје коментаре.
- Злонамерни корисници могу направити скрипту.

Укрштање веб локација (енг. *Cross-Site Scripting*)

- Ова врста напада се дешава на оним веб странама где корисници могу оставити своје коментаре.
- Злонамерни корисници могу направити скрипту.
- Та скрипта може да послужи да другим корисницима прати колачиће, да презме податке других корисника и слично.

Злонамерни софтвер

Успутно преузимање података (енг. *Drive-By Downloads*)

Успутно преузимање података (енг. *Drive-By Downloads*)

Успутно преузимање података (енг. *Drive-By Downloads*) представља напад на рачунар посетиоца заражене веб странице, тако што се на његов рачунар копирају злонамерне датотеке.

Успутно преузимање података (енг. *Drive-By Downloads*)

Успутно преузимање података (енг. *Drive-By Downloads*) представља напад на рачунар посетиоца заражене веб странице, тако што се на његов рачунар копирају злонамерне датотеке.

Нападач може изменити лоше обезбеђену веб страницу, тако да се на рачунар сваког посетиоца те странице копира одређени злонамерни програм, без знања корисника.

Успутно преузимање података (енг. *Drive-By Downloads*)

Успутно преузимање података (енг. *Drive-By Downloads*) представља напад на рачунар посетиоца заражене веб странице, тако што се на његов рачунар копирају злонамерне датотеке.

Нападач може изменити лоше обезбеђену веб страницу, тако да се на рачунар сваког посетиоца те странице копира одређени злонамерни програм, без знања корисника.

Посетилац може постати жртва напада и свесним преузимањем софтвера са заражене веб странице, чија намена је различита од представљене.

Злонамерни софтвер

Тројански коњ

Тројански коњ

Тројански коњ, назван по чувеном Тројанском коњу из Хомеровог епа Одисеја, представља штетни програм. Маскиран је у програм који је користан, док у позадини извршава злонамерне акције без знања корисника.

Тројански коњ

- На пример, Тројански коњ може да чисти вирусе и црве на рачунару, а да истовремено у позадини инстаира софтвер за шпиунирање корисника.

Тројански коњ

- На пример, Тројански коњ може да чисти вирусе и црве на рачунару, а да истовремено у позадини инстаира софтвер за шпиунирање корисника.
- Пример је тројански коњ *Мостех*, распрострањен у Кини. Уместо искључивог учитавања слика овај софтвер је прикривено крао личне информације о корисницима, шифре и слично.

Злонамерни софтвер

Софтвер за шпиунирање

Софтвер за шпиунирање

Софтвер за шпијунирање (енг. *Spyware*) је нежељени софтвер који упада у систем и краде поверљиве информације. Овај софтвер сакупља личне податке корисника и шаље их злонамерним појединцима или компанијама, које се баве рекламама или обрадом података.

Софтвер за шпиунирање

Софтвер за шпијунирање (енг. *Spyware*) је нежељени софтвер који упада у систем и краде поверљиве информације. Овај софтвер сакупља личне податке корисника и шаље их злонамерним појединцима или компанијама, које се баве рекламама или обрадом података.

Софтвер за шпиунирање може да прати веб претрагу или унос карактера или да прави слике радне површине (енг. *screenshots*).

Софтвер за шпиунирање – Адвер

Адвер (енг. *Adware*) се користи у сврху маркетинга, тако што прати историју претраживања и преузете податке са Интернета, са намером да предвиди какви би производи заинтересовали корисника и те информације прослеђује маркетиншким агенцијама. Може знатно да успори рачунар.

Софтвер за шпиунирање – колачићи за праћање

Колачићи за праћање (енг. *tracking cookies*) прате све акције корисника на Интернету, као што су историја претраживања или размена података. Њихова подразумевана намена није злонамерна, али могу да се искористе од стране сајбер криминалаца.

Софтвер за шпиунирање – посматрачи система

Посматрачи система (енг. *system monitors*) прате све акције корисника на рачунару, региструју сваки притисак дугмета на тастатури, прочитану електронску пошту, разговор на интернету, посећене веб странице и коришћене програме.

Злонамерни софтвер

Мрежа ботова

Бот

Бот је посебна врста тројанског коња који реагује на наредбе које шаље програм за управљање који се налази на екстерном рачунару.

Бот

- Први ботови су били легални.
- На пример, интернет игре са много корисника су имале ботове.
- Данас се ботови углавном користе за нелегалне активности.

Мрежа ботова (енг. *Botnet*)

Мрежа ботова (енг. *Botnet*) је колекција међусобно повезаних заражених уређаја, који су под контролом истог типа злонамерног софтвера. Корисници заражених уређаја често нису свесни да је њихов систем део мреже ботова.

Мрежа ботова (енг. *Botnet*)

Мрежа ботова (енг. *Botnet*) је колекција међусобно повезаних заражених уређаја, који су под контролом истог типа злонамерног софтвера. Корисници заражених уређаја често нису свесни да је њихов систем део мреже ботова.

Мрежа ботова (енг. *Botnet*)

- Мрежа ботова може да буде на неколико хиљада рачунара до неколико милиона рачунара.

Мрежа ботова (енг. *Botnet*)

- Мрежа ботова може да буде на неколико хиљада рачунара до неколико милиона рачунара.
- Користе за слање нежељене електронске поште.

Мрежа ботова (енг. *Botnet*)

- Мрежа ботова може да буде на неколико хиљада рачунара до неколико милиона рачунара.
- Користе за слање нежељене електронске поште.
- Такође, могу се користити за преусмеравање корисника на злонамерне веб странице.

Мрежа ботова (енг. *Botnet*)

- Мрежа ботова може да буде на неколико хиљада рачунара до неколико милиона рачунара.
- Користе за слање нежељене електронске поште.
- Такође, могу се користити за преусмеравање корисника на злонамерне веб странице.
- Процена је да 90% све нежељене поште долази са мреже ботова.

Мрежа ботова (енг. *Botnet*)

- Мрежа ботова може да буде на неколико хиљада рачунара до неколико милиона рачунара.
- Користе за слање нежељене електронске поште.
- Такође, могу се користити за преусмеравање корисника на злонамерне веб странице.
- Процена је да 90% све нежељене поште долази са мреже ботова.
- Мрежа ботова се користе често и за *DDoS* нападе.

Мрежа ботова (енг. *Botnet*)

Постоји два начина функционисања.

Мрежа ботова (енг. *Botnet*)

Постоји два начина функционисања.

I начин

Традиционални клијент/сервер приступ укључује постављање контролног сервера (енг. *ommand and Control server*), који шаље аутоматске команде ботовима користећи комуникационе протоколе, као што је *IRC* протокол (енг. *nternet Relay Chat*). Ботови су у стању чекања, све док не стигне наредба са контролног сервера.

Мрежа ботова (енг. *Botnet*)

Постоји два начина функционисања.

I начин

Традиционални клијент/сервер приступ укључује постављање контролног сервера (енг. *ommand and Control server*), који шаље аутоматске команде ботовима користећи комуникационе протоколе, као што је *IRC* протокол (енг. *nternet Relay Chat*). Ботови су у стању чекања, све док не стигне наредба са контролног сервера.

II начин

Децентрализовани приступ укључује мрежу равноправних корисника (енг. *peer–to–peer*). Заражени уређаји комуницирају унутар мреже и тако деле нове наредбе најскорије верзије злонамерног софтвера, који њима управља.

Злонамерни софтвер

Мере заштите од злонамерног софтвера

Мере заштите од злонамерног софтвера

Безбедносне закрпе софтвера

Безбедносне закрпе софтвера (енг. *Security patches*) представљају ажуриране делове софтверског решења, које је у својим претходним верзијама садржало одређене пропусте, од којих су неки откривени након претрпљених последица.

Мере заштите од злонамерног софтвера

Алати за одбрану од злонамерног софтвера

Алати за одбрану од злонамерног софтвера (енг. antimalware tools) се користе у превентивне сврхе или за анализу и отклањање заражених датотека, уз претходну сагласност корисника. Морају се редовно ажурирати ове алате.

Мере заштите од злонамерног софтвера

Заштитни зидови

Заштитни зидови (енг. *firewalls*) представљају софтвер који се користи за регулисање мрежног саобраћаја на рачунару. Заштитни зидови омогућавају кориснику да одабере која ће апликација имати приступ интернету. Не пружају довољну заштиту уколико су рачунари већ заражени типом злонамерног софтвера који може онеспособити заштитни зид.

Неки познати напади

Опрација “пацов” (енг. *Operation Shady RAT*)

- Рачунарски програмер са седиштем у Народној Републици Кини претпоставља се да је одговоран за ове континуиране сајбер нападе који су први пут започели 2006.
- Назван по коришћењу алата за даљински приступ који омогућавају даљинско управљање рачунарима са било ког места у свету.
- Овај хакер је успео да украде интелектуалну својину од најмање 70 јавних и приватних организација из 14 земаља. Међу жртвама су Уједињене нације, светска предузећа, Светска антидопинг агенција и Међународни олимпијски комитет.

Хаковање министарства одбране

- Тинејџер са Флориде успео је да угрози војни рачунарски систем још 1999.
- Инсталирањем софтвера за позадину у рачунарски систем Агенције за смањење претњи одбране, Џонатан Џејмс је био способан да пресретне високо класификоване имејлове.
- Они су укључивали информације о коду за одржавање живота у оквиру Међународне свемирске станице и многим другим важним питањима.

Мелиса вирус

- Вирус из 1999. године који је оштетио велики број корисника.
- Вирус је био маскиран као једноставан *Microsoft Word* програм и послат на безброј прималаца.
- Вирус се брзо проширио, а велике компаније попут *Intel*–а и *Microsofta*–а биле су принуђене да искључе све програме одлазне поште док се проблем не реши.

Comodo напад

- Безбедносни сертификати служе као обавештење да смо стигли на безбедну локацију.
- Компанију *Comodo*, која пружа те сертификате, хакирао је 2011. године ирански програмер.
- Успео је да створи лажне безбедносне сертификате који су навели људе да верују да се заправо пријављују на *Yahoo* или *Google*. Ово је омогућило хакеру да прислушкује било који имејл који је послат од ових служби и прибавља личне податке.

Play Station Network напад

- 2011. године хакер је приступио систему *Play Station Network*.
- То је резултирало губитком личних података за око 77 милиона корисника.
- Компанија је морала да се угаси на 20 дана и изгубила је, према проценама, 171 милион долара.