# Povijest zlonamjernih programa

1

00:00:00,000 --> 00:00:08,000

Dobro došli. U ovom videu proći ćemo kroz

povijest nastanka virusa.

2

00:00:08,000 --> 00:00:18,666

Pod zlonamjernim (malicioznim) se programima

podrazumijevaju bilo koji programi koji mogu

narušiti jedan od ključnih elemenata sigurnosti:

3

00:00:18,666 --> 00:00:31,332

povjerljivost, integritet ili dostupnost. Iako je tek u

zadnjih nekoliko godina zabilježen velik rast broja

zlonamjernih programa, oni postoje već čitav niz

4

00:00:31,333 --> 00:00:38,399

godina, praktički od samih početaka izrade

programa.

5

00:00:38,400 --> 00:00:50,166

Ideja programa koji se sami reproduciraju, što je

jedno od glavnih obilježja virusa, potiče još od

Johna von Neumanna koji je 1940. razmatrao

6

00:00:50,166 --> 00:01:00,199

idejuo o samo reproduktivnim programima. Prvim

zlonamjernim programom koji je bio napravljen

pod kontroliranim uvjetima smatra se program koji

7

00:01:00,200 --> 00:01:12,533

je 1962. godine napisalo nekoliko zaposlenika

laboratorija Bell. Ovi su znanstvenici napisali

program pod nazivom „Darwin“ čiji je cilj bio

8

00:01:12,533 --> 00:01:21,099

automatski se reproducirati i pronalaziti druge

programe u memoriji te ih brisati.

9

00:01:21,100 --> 00:01:31,400

Zlonamjerni su programi bili ipak relativno rijetki

sve do pojave kućnih računala. Ipak, iz prethodnog

se razdoblja može izdvojiti virus pod imenom

10

00:01:31,400 --> 00:01:42,133

Creeper koji je inficirao računala spojena na

ARPANET, računalnu mrežu američke vojske

početkom sedamdesetih godina prošlog stoljeća.

11

00:01:42,133 --> 00:01:51,499

Ovaj je virus inficirao računala s operacijskim

sustavom Tenex koji je bio popularan u to vrijeme

te se automatski kopirao na druga računala preko

12

00:01:51,500 --> 00:02:00,900

modemske veze. Na inficiranim računalima virus

je ostavio poruku „I'M THE CREEPER: CATCH

ME IF YOU CAN“.

13

00:02:00,900 --> 00:02:14,433

Ovaj virus je zanimljiv i po tome što je za njega, po

prvi puta, napisan i "antivirusni program" također

sa svojstvima virusa, samoreprodukcijom. Ovaj je

14

00:02:14,433 --> 00:02:24,599

događaj prvi pokazao da izrada programa za

automatsko brisanje virusa, koji dijele svojstva

virusa, nema dobar učinak jer je i Reaper, kao

15

00:02:24,600 --> 00:02:30,433

antivirusni program, izazvao probleme na

računalnoj mreži ARPANET.

16

00:02:30,433 --> 00:02:41,799

Početkom osamdesetih godina prošlog stoljeća

kućna računala postajala su sve popularnija. Prvi

virus zabilježen za kućna računala jest Elk Cloner,

17

00:02:41,800 --> 00:02:52,966

virus za računala Apple II koji se širio preko

disketa. Virus je modificirao ključne sektore na

disketama kako bi se pokrenuo pri pokretanju

18

00:02:52,966 --> 00:03:04,666

računala jer su računala Apple II podizala i

operacijski sustav s disketa. Elk Cloner tako je bio

memorijski rezidentan virus, što znači da je bio

19

00:03:04,666 --> 00:03:14,366

aktivan tijekom rada računala te je inficirao sve

druge diskete umetnute u računalo tijekom

njegova rada.

20

00:03:14,366 --> 00:03:25,732

Prvi virus za IBM osobna računala računala

(Personal Computer) otkriven je 1986. godine.

Riječ je o virusu pod imenom Brain koji je poput

21

00:03:25,733 --> 00:03:31,433

virusa Elk Cloner inficirao diskete.

22

00:03:31,433 --> 00:03:34,899

Lekcija je završena.

# Štetni softver (malwer)

1

00:00:00,000 --> 00:00:08,166

Dobrodošli. U ovoj lekciji naučiti ćemo što čini štetni softver.

2

00:00:08,166 --> 00:00:23,366

Zajednički naziv svim vrstama zlonamjernoga računalnog koda engleski je izraz „malware“ (malicious software – maliciozni, zlonamjerni kod,

3

00:00:23,366 --> 00:00:26,666

program).

4

00:00:26,666 --> 00:00:38,732

U zlonamjerni, štetni softver spadaju aplikacije sa zlim namjerama ili zlonamjernim posljedicama. Tako možemo razaznati Trojance,

5

00:00:38,733 --> 00:00:44,699

rootkitove

6

00:00:44,700 --> 00:00:49,933

i zadnja vrata (back doors).

7

00:00:49,933 --> 00:00:59,366

Svima je zajedničko da se na računalo instaliraju bez korisničkog pristanka, a detaljnije će biti obrađeni u nastavku.

8

00:00:59,366 --> 00:01:05,566

Po tipovima ih možemo podijeliti na: viruse

9

00:01:05,566 --> 00:01:09,966

i crve.

10

00:01:09,966 --> 00:01:13,699

Lekcija je završena.

# Virusi

1

00:00:00,000 --> 00:00:07,500

Dobro došli. U ovom videu ćemo naučiti što su to

virusi.

2

00:00:07,500 --> 00:00:18,333

Virus je zlonamjeran kod koji se pri izvršavanju

pokušava umnožiti (replication), kopirati samog

sebe unutar drugog izvršnog koda

3

00:00:18,333 --> 00:00:28,866

odnosno programa. Ako je pokušaj uspješan, za

kod se kaže da je zaražen. Tako zaraženi kod pri

izvršavanju može na isti način proširiti zarazu

4

00:00:28,866 --> 00:00:32,032

dalje, na novi kod.

5

00:00:32,033 --> 00:00:42,099

To samorepliciranje u postojeći izvršni kod ključno

je obilježje u definiranju virusa. Iako nema

univerzalne definicije, često je korištena ona dr.

6

00:00:42,100 --> 00:00:53,566

Frederica Cohena koja računalni virus definira kao

„program koji može "zaraziti" druge programe

modificirajući ih tako da u njih uključuje kopije

7

00:00:53,566 --> 00:01:03,432

samog sebe“. Pod zarazom se podrazumijeva da

virus ubacuje samog sebe u slijed naredbi

programa, tako da pokušaj izvršavanja legitimnog

8

00:01:03,433 --> 00:01:10,499

programa dovodi do izvršavanja virusa zajedno s

tim programom (ili umjesto njega).

9

00:01:10,500 --> 00:01:19,300

Od samih početaka virusi se umnožavaju i šire

unutar jednog računala i zatim se prenose od

računala do računala

10

00:01:19,300 --> 00:01:28,900

prijenosnim medijima kao što su diskete, CD i

DVD mediji te USB memorijski uređaji.

11

00:01:28,900 --> 00:01:39,400

Jednako tako, mogu se širiti i preko dijeljenih

datoteka u lokalnoj mreži. Smatra se da je danas

Internet glavni medij za prijenos virusa. U velikom

12

00:01:39,400 --> 00:01:50,400

se broju slučajeva virusi prenose preko

elektroničke pošte, ali ne i isključivo. Mogu se

nalaziti kao izvršne i druge datoteke u privitku e-

13

00:01:50,400 --> 00:02:01,000

poruke ili je čak nekad dovoljno da korisnik samo

otvori poruku pa da se računalo inficira. Pristigla

poruka može biti i od neke poznate osobe jer

14

00:02:01,000 --> 00:02:11,166

virusi, zajedno s brojnim drugim vrstama štetnih

programa, imaju sposobnost da se sami pošalju

elektroničkom poštom sa zaraženog računala na

15

00:02:11,166 --> 00:02:14,632

sve adrese iz elektroničkog adresara.

16

00:02:14,633 --> 00:02:26,833

Računalni se virus sastoji od tri dijela, odnosno tri

mehanizma: mehanizam zaraze (infection) – način

na koji se virus širi;

17

00:02:26,833 --> 00:02:37,099

korisničkog sadržaj (payload) – čini ono što virus

zapravo radi i može se odnositi na štetu koju radi;

18

00:02:37,100 --> 00:02:44,500

okidač (trigger) – ono što će pokrenuti izvršavanje

virusa.

19

00:02:44,500 --> 00:02:58,500

Mehanizam zaraze za svaki je virus obvezan, kako

bi on uopće bio tako klasificiran, a druga su dva

mehanizma opcionalna.Virus ne mora nužno biti

20

00:02:58,500 --> 00:03:06,866

napravljen s namjerom da učini konkretnu štetu

(bez korisničkog sadržaja), no i u tim slučajevima

nerijetko nastaje nekakva usputna, slučajna šteta.

21

00:03:06,866 --> 00:03:16,266

Posljedice zaraze tako mogu biti samo

zauzimanje sistemskih resursa – prostora u

memoriji i na tvrdom disku, zbog čega može doći

22

00:03:16,266 --> 00:03:26,399

do usporavanja računala i veze na Internet (možda

čak i tolikog usporavanja da računalo postane

neupotrebljivo).

23

00:03:26,400 --> 00:03:35,566

Lekcija je završena.

# Crvi

1

00:00:00,000 --> 00:00:11,000

Dobro došli. U ovoj lekciji ćemo se upoznati sa crvima, kao slijedećom vrstom malicioznih programa.

2

00:00:11,000 --> 00:00:22,766

Crv (worm) jest naziv za štetni računalni kod koji se samostalno replicira i inficira računala, sposoban samostalno tražiti nove sustave

3

00:00:22,766 --> 00:00:34,166

domaćine i inficirati ih preko mreže. Mnogi često poistovjećuju crve s virusima, nazivajući ih samo posebnom podvrstom virusa.

4

00:00:34,166 --> 00:00:43,732

Jednako tako, mnogi bi poznati štetni programi koji su popularno prozvani virusima po pravilu trebali biti smatrani crvima ili hibridima tih dviju

5

00:00:43,733 --> 00:00:52,199

vrsta štetnih programa. Točno je da crvi imaju neka zajednička obilježja s virusima. Najvažnije obilježje koje dijele jest

6

00:00:52,200 --> 00:01:02,566

mogućnost samo repliciranja, samo umnažanja, no u načinu umnažanja se razlikuju. Prvo, crvi ne trebaju domaćina da bi se širili kao virusi za koje

7

00:01:02,566 --> 00:01:12,699

možemo reći da se takoreći ponašaju kao paraziti, crvi su samostalni, samostalno djeluju i šire se. Druga je razlika što je osnovni medij

8

00:01:12,700 --> 00:01:23,000

širenja crva mreža odnosno Internet. Dakle, virusi se šire inficirajući druge programe, drugi kod, a crvi imaju sposobnost samostalne

9

00:01:23,000 --> 00:01:38,000

migracije sa sustava na sustav preko mreže. Crv koji se nalazi na nekom računalu traži druga dostupna računala preko lokalne mreže (LAN) ili

10

00:01:38,000 --> 00:01:47,233

preko internetske veze. Kad pronađe drugo računalo, replicira se, kopira se na to novo računalo, odakle ta kopija, odnosno nova instanca

11

00:01:47,233 --> 00:01:57,599

crva dalje traži nova računala. Dvije najčešće metode širenja crva jesu: elektronička pošta (e-mail) i iskorištavanje sigurnosnih slabosti i

12

00:01:57,600 --> 00:02:03,300

propusta na računalima spojenima na mrežu ili na Internet.

13

00:02:03,300 --> 00:02:16,066

Crvi koji rabe e-poštu za širenje nazivaju se e-mail crvi odnosno crvi koji se masovno šalju (mass-mailing). Najčešće su napravljeni tako da su

14

00:02:16,066 --> 00:02:27,332

usmjereni na Microsoft. Crv obično provjerava korisnikov e-imenik i zatim šalje kopije samog sebe na svaku od adresa.

15

00:02:27,333 --> 00:02:39,733

Za razliku od njih, internetski se crvi šire pretraživanjem Interneta u potrazi za računalom na kojem se rabi specifični operacijski sustav ili web-

16

00:02:39,733 --> 00:02:50,299

poslužitelj s određenom poznatom manom ili sigurnosnom slabošću. Kad crv pronađe ranjivo računalo, kopira se na to računalo iskorištavanjem

17

00:02:50,300 --> 00:03:00,066

te ranjivosti i zatim se koristi tim novim računalom u potrazi za novim metama napada.

18

00:03:00,066 --> 00:03:10,899

S pomoću crva napadač zapravo može preuzeti kontrolu nad računalom i šteta koju može načiniti ovisi isključivo o mašti i ciljevima napadača.

19

00:03:10,900 --> 00:03:20,433

Uobičajene radnje jesu: otvaranje „stražnjih vrata“ (backdoor) – s pomoću kojih napadač zadobiva potpunu daljinsku kontrolu (remote control) nad

20

00:03:20,433 --> 00:03:24,799

inficiranim sustavom;

21

00:03:24,800 --> 00:03:36,600

postavljanje izvršitelja DDoS (distributed denial-of-service) što izaziva potrošnju goleme količine memorije, procesorske snage, čime se potpuno

22

00:03:36,600 --> 00:03:45,500

onemogućuje komunikacija napadnutog sustava s ostatkom mreže (na meti su obično web-poslužitelji i sl.);

23

00:03:45,500 --> 00:03:56,900

izvođenje kompleksnih matematičkih operacija – inficiranjem velikog broja računala na pravi način napadač dobiva mogućnost iskoristiti njihove

24

00:03:56,900 --> 00:04:08,600

resurse za obavljanje zahtjevnih matematičkih operacija (kao npr. razbijanje ključa za šifriranje ili šifrirane lozinke i slično).

25

00:04:08,600 --> 00:04:19,900

Stražnja vrata (Backdoor ili Back door) označuju štetni kod koji radi upravo ono na što upućuje njegovo ime, otvara vrata odnosno „stražnji ulaz“ u

26

00:04:19,900 --> 00:04:29,566

neku aplikaciju, operacijski sustav ili mrežu. Stražnja vrata (backdoor) izvorno su mehanizmi koje su stvorili programeri kako bi im omogućili

27

00:04:29,566 --> 00:04:40,099

poseban pristup njihovim programima, obično da bi mogli prepraviti kod u slučaju neke greške. Danas taj termin (u okviru hakera i hakiranja)

28

00:04:40,100 --> 00:04:49,766

označuje bilo kakav mehanizam koji napadaču potajno omogućuje ponovni pristup kompromitiranom operacijskom sustavu ili mreži

29

00:04:49,766 --> 00:04:58,499

bez ponavljanja prvotnog procesa napada.

30

00:04:58,500 --> 00:05:08,000

U svrhu definiranja pojma možemo reći da je stražnji ulaz (backdoor) dio koda (program ili modifikacija programa) koji zaobilazi normalne

31

00:05:08,000 --> 00:05:31,400

sigurnosne provjere i autoru omogućuje pristup nekoj aplikaciji, operacijskom sustavu ili mreži. Pristup koji napadač dobiva ovisi o napadačevim namjerama i vrsti stražnjih vrata. Osnovne vrste pristupa koje takav kod omogućuje jesu sljedeće.

32

00:05:31,400 --> 00:05:37,466

Povećanje privilegija – takva vrsta stražnjih vrata napadaču koji ima skriveni korisnički račun na sustavu omogućuje mijenjanje tog računa u

33

00:05:37,466 --> 00:05:45,666

administratorski. S privilegijama administratora napadač može izmijeniti postavke računala ili pristupiti bilo kojoj datoteci smještenoj na

34

00:05:45,666 --> 00:05:48,932

računalu.

35

00:05:48,933 --> 00:06:01,999

Udaljeni pristup naredbenom retku – poznat i kao „remote shell“. Takav tip stražnjih vrata omogućuje izravan pristup naredbenom retku (Command

36

00:06:02,000 --> 00:06:12,033

prompt). S druge strane mreže napadač može pisati u naredbenom retku ciljanog računala. Napadač može iskoristiti sve mogućnosti

37

00:06:12,033 --> 00:06:22,333

naredbenog retka poput izvršavanja naredbi, pisanja skripte, manipuliranja datotekama. Takva stražnja vrata simuliraju izravan pristup tipkovnici

38

00:06:22,333 --> 00:06:26,466

inficiranog računala.

39

00:06:26,466 --> 00:06:37,799

Udaljeni pristup grafičkom korisničkom sučelju (GUI) – takva stražnja vrata idu korak dalje od naredbenog retka i omogućuju da napadač vidi

40

00:06:37,800 --> 00:06:47,900

grafičko korisničko sučelje (GUI) računala žrtve, kontrolira pomake miša i udarce tipki na tipkovnici. S udaljenom kontrolom nad grafičkim

41

00:06:47,900 --> 00:06:54,933

korisničkim sučeljem napadač može vidjeti sve što žrtva radi na računalu.

42

00:06:54,933 --> 00:07:06,099

U nastavku će biti opisani programi koji napadačima omogućuju da kod neopreznih ili nedovoljno educiranih korisnika računala izazovu

43

00:07:06,100 --> 00:07:15,733

konkretne opasnosti. Ranije smo vidjeli da posljedica djelovanja virusa može npr. biti smanjena propusnost naše mreže odnosno „izlaza

44

00:07:15,733 --> 00:07:23,999

na Internet“. No ovi su programi daleko konkretnija opasnost.Osnovno obilježje trojanskih konja jest da su štetni

45

00:07:24,000 --> 00:07:34,933

programi koji se nisu u stanju sami širiti. Dakle, za razliku od virusa i crva, trojanski konji sami po sebi ne mogu inficirati nova računala, već se za njihovo

46

00:07:34,933 --> 00:07:45,366

širenje često rabe posrednici, i to u obliku virusa ili crva. Termin „trojanski konj“ potječe od opće poznate

47

00:07:45,366 --> 00:07:57,032

priče iz Homerove Ilijade. Naziv označuje zamku maskiranu u nešto naizgled bezopasno. Analogija vrijedi i u računalnom svijetu.

48

00:07:57,033 --> 00:08:07,399

Prije nego što trojanski konj može napasti, najprije mora pronaći način da namami korisnika da kopira program i pokrene ga. Dva su načina na

49

00:08:07,400 --> 00:08:16,500

koja se to postiže. Pokušava se „predstaviti“ kao neki bezopasan ili koristan program. Možemo reći da se preruši u

50

00:08:16,500 --> 00:08:26,433

neki drugi program za koji korisnik može pomisliti da je bezopasan – poput neke računalne igrice ili nekog uslužnog programa, poput programa za

51

00:08:26,433 --> 00:08:35,999

optimizaciju rada računala i sl. Katkad je čak dovoljno da se promijeni ime trojanskog konja u ime nekoga poznatog programa da bi ga korisnik

52

00:08:36,000 --> 00:08:44,466

pokrenuo. Nakon što smo ga skinuli sa Interneta ili pokrenuli, napravit će neku štetu na našem računalu.

53

00:08:44,466 --> 00:08:53,366

Druga je mogućnost da se sami „sakriju“ unutar nekoga legitimnoga poznatog programa poput Microsoftova Excela,te da se zapravo integriraju

54

00:08:53,366 --> 00:09:03,999

unutar nekog programa.Opasni su po tome što im je namjena krađa osobnih podataka.

55

00:09:04,000 --> 00:09:11,766

Lekcija je završena.

# Špijunski kod (spyware)

1

00:00:00,000 --> 00:00:08,300

Dobro došli. U ovom videu naučit ćemo koje su prijetnje od špijunskih programa.

2

00:00:08,300 --> 00:00:19,833

Špijunski kod odnosno špijunski programi (spyware) jest aplikacija odnosno programski kod koji sakuplja informacije o nekoj osobi ili

3

00:00:19,833 --> 00:00:27,833

organizaciji, i to tako da korisnici nisu ni svjesni da su sami to, zapravo, dopustili.

4

00:00:27,833 --> 00:00:35,599

Informacije se sakupljaju sa svrhom novčane zarade (prodajom informacija), a špijunski se program (spyware) također smatra štetnim

5

00:00:35,600 --> 00:00:43,500

programom (malware) zbog toga što se instalira na računalo bez znanja korisnika.

6

00:00:43,500 --> 00:00:54,300

Definicija špijunskog koda prilično je općenita zbog toga što postoje mnogi oblici s razlikama u načinu širenja, načinu funkcioniranja,

7

00:00:54,300 --> 00:01:04,866

mogućnostima i krajnjem cilju. Špijunski programi (spyware) računalne su zaraze koje su ilegalne, nemoralne, narušavaju privatnost i vrlo ih se teško

8

00:01:04,866 --> 00:01:17,132

riješiti. Jedan od razloga tome je što često čuvaju nevidljive kopije na tvrdom disku pa ako se ne uklone svi mogući tragovi i nakon brisanja se sami

9

00:01:17,133 --> 00:01:19,966

ponovo instaliraju.

10

00:01:19,966 --> 00:01:33,832

Za razliku od uobičajenih programa koji su vidljivi na listi aktivnih procesa koje prati operacijski sustav, špijunski se programi „zakopaju“ daleko od

11

00:01:33,833 --> 00:01:44,699

naših očiju tako da su mogućnosti vrlo male da će korisnik slučajno uočiti nekog od njih dok je aktivan. Nerijetko korisnik uopće ne može otkriti

12

00:01:44,700 --> 00:01:48,933

špijunski kod na svom računalu.

13

00:01:48,933 --> 00:01:59,099

Špijunski se kod infiltrira u računalo na razne načine. Neki su virusi, crvi i trojanski konji dizajnirani sa svrhom instaliranja špijunskih

14

00:01:59,100 --> 00:02:02,466

programa na ciljano računalo.

15

00:02:02,466 --> 00:02:13,799

Druga je mogućnost inficiranja iskorištavanjem ranjivosti web-preglednika, koji dopuštaju preuzimanje i pokretanje nekog štetnog sadržaja.

16

00:02:13,800 --> 00:02:19,200

To mogu biti neke ActiveX kontrole ili dodaci (plug-in) za preglednike.

17

00:02:19,200 --> 00:02:32,033

Primjer programa koji u sebi gotovo uvijek sadržava štetni kod jest tzv. generator ključeva (key generator). Generatore ključeva trebamo u

18

00:02:32,033 --> 00:02:41,766

situacijama kojima se nikako ne bismo smjeli ponositi, a to je kada instaliramo programe za koje nemamo važeću licencu. U takvim ga

19

00:02:41,766 --> 00:02:52,932

slučajevima uz pomoć generatora ključeva pokušavamo učiniti „kupljenim“. U konačnici i dalje imamo program kojim se nezakonito koristimo te

20

00:02:52,933 --> 00:02:57,899

računalo zaraženo nekom vrstom štetnog koda.

21

00:02:57,900 --> 00:03:09,066

Špijunski kod nakon inficiranja računala može: pratiti aktivnost korisnika, bilježiti svaki udarac tipke (key logger, keystroke logging), pratiti svaki

22

00:03:09,066 --> 00:03:18,632

aktivni program i bilježiti vrijeme korištenja svakim programom na računalu, mijenjati postavke i „oteti“ (hijack) web-preglednik tako da promijeni

23

00:03:18,633 --> 00:03:31,233

postavljenu početnu stranicu pri svakom pretraživanju te samostalno dodavati oznake (bookmark) i sl, može nametati neželjene reklame

24

00:03:31,233 --> 00:03:41,333

i oglase, sakupljati informacije o svim programima instaliranima na računalu te pratiti navike pretraživanja korisnika te sakupljati elektroničke

25

00:03:41,333 --> 00:03:47,499

adrese isključivo radi daljnjeg "spama".

26

00:03:47,500 --> 00:03:56,300

Lekcija je završena.

# Reklamni kod

1

00:00:00,000 --> 00:00:08,333

Dobro došli. U ovom videu naučit ćemo što je to

reklamni kod.

2

00:00:08,333 --> 00:00:20,266

Reklamni kod, odnosno reklamni programi

(adware) najčešće su različiti oblici besplatnih

(freeware) programa koji od korisnika, u zamjenu

3

00:00:20,266 --> 00:00:27,766

za besplatno korištenje, zahtijevaju izvođenje

sponzorskih oglasa tijekom rada programa.

4

00:00:27,766 --> 00:00:38,566

Iako se na prvi pogled čini da je takav način rada

korektan i pošten jer se zasniva na načelu „Vi se

koristite programom besplatno, a ja se na račun

5

00:00:38,566 --> 00:00:46,966

toga reklamiram“, problem je što takvi programi u

pozadini obavljaju i neke poslove kojih korisnik

nije svjestan.

6

00:00:46,966 --> 00:01:00,899

Tako, na primjer, mogu:sakupljati informacije o

korisniku, o njegovim navikama pretraživanja

Interneta i korištenja računalom; te na temelju tako

7

00:01:00,900 --> 00:01:13,500

formiranog profila korisniku prikazivati oglase koji

bi ga mogli zanimati; mogu korisniku prikazivati

oglasni privremeni (pop-up) prozori prema

8

00:01:13,500 --> 00:01:23,466

podacima o njegovim navikama ili čak oglasi

vezani za ono što u tom trenutku radi; mogu

također mijenjati postavke web-preglednika:

9

00:01:23,466 --> 00:01:33,566

preglednik se preusmjerava na određena web-

mjesta s ciljem potencijalne prodaje ili sl. I za kraj,

mogu modificirati određene postavke

10

00:01:33,566 --> 00:01:41,066

operacijskog sustava koje se odnose na rad na

mreži i znatno narušiti performanse računala.

11

00:01:41,066 --> 00:01:53,299

Problem je što je korisnik svjesno instalirao takav

program i time pristao na bilo koju radnju, a

nerijetko se složio i s tzv. licenčnim uvjetima prije

12

00:01:53,300 --> 00:01:55,700

instalacije programa.

13

00:01:55,700 --> 00:02:07,466

S obzirom na to da se korisnik složio s uvjetima

licence (EULA, End User License Agreement),

ispada da takav način rada nije nezakonit.

14

00:02:07,466 --> 00:02:15,499

Lekcija je završena.

# Birači (dialer)

1

00:00:00,000 --> 00:00:08,966

Dobro došli. U ovom videu obradit ćemo birače, kao još jednu vrstu malicioznih programa.

2

00:00:08,966 --> 00:00:22,566

Birač (dialer) je u osnovi program instaliran na računalo kao dio operacijskog sustava, a omogućuje spajanje na Internet preko analogne

3

00:00:22,566 --> 00:00:28,566

modemske veze te biranje telefonskih brojeva bez dozvole korisnika računala.

4

00:00:28,566 --> 00:00:38,632

Kada govorimo o ovim programima, djelomično možemo odahnuti jer se pojavom (A)DSL priključaka smanjila upotreba analognih modema

5

00:00:38,633 --> 00:00:44,666

s pomoću kojih smo se svojedobno spajali na Internet.

6

00:00:44,666 --> 00:00:54,232

Birači su uglavnom prekidali normalnu vezu s pružateljem ISP usluga i uspostavljaju skupe međunarodne veze prema odredištima čija je

7

00:00:54,233 --> 00:00:59,199

cijena poziva skupo naplaćivana.

8

00:00:59,200 --> 00:01:11,800

Kao što je već rečeno, korisnici koji za izlazak na Internet rabe (A)DSL ili širokopojasne veze obično nisu u opasnosti, no „pisci“ zlonamjernog koda

9

00:01:11,800 --> 00:01:22,066

zbog toga su se usmjerili na mobilne uređaje preko kojih šalju SMS poruke koje se skupo naplaćuju ili pozivaju razne govorne automate s

10

00:01:22,066 --> 00:01:26,032

visokom cijenom poziva.

11

00:01:26,033 --> 00:01:32,966

Lekcija je završena.

# Alati za dobivanje administratorskih ovlasti na sustavu

1

00:00:00,000 --> 00:00:10,566

Dobro došli. U ovoj lekciji upoznat ćemo se sa naj

sofisticiranijim i naj opasnijim štetnim programom.

2

00:00:10,566 --> 00:00:21,266

Rootkit tehnologija omogućuje integriranje

zlonamjernih programa s ključnim funkcijama i

strukturama jezgre operacijskog sustava. Ova

3

00:00:21,266 --> 00:00:32,699

napredna metoda skrivanja postala je vrlo

popularna 2007. godine nakon čega se sve češće

pronalaze štetni programi koji imaju rootkit

4

00:00:32,700 --> 00:00:34,866

komponentu.

5

00:00:34,866 --> 00:00:44,499

Zbog kompleksnosti otkrivanja zlonamjernih

programa koji rabe rootkit komponente, u svrhu

njihova uklanjanja danas se uvijek preporučuje

6

00:00:44,500 --> 00:00:47,933

potpuna reinstalacija računala.

7

00:00:47,933 --> 00:00:57,199

Alati za dobivanje administratorskih ovlasti potječu

iz svijeta Unixa i poslije su prešli i na Windowsove

platforme.

8

00:00:57,200 --> 00:01:09,400

Stvoreni su da bi zamijenili standardne Unix alate

verzijama koje su korisniku davale korijenske

(root) privilegije odnosno privilegije Super-

9

00:01:09,400 --> 00:01:20,033

korisnika (paralela kod računala Windows jest

korisnički račun Administratora), pritom

omogućavajući da njihova aktivnost ostane

10

00:01:20,033 --> 00:01:30,699

nevidljiva ostalim korisnicima. Ta jedinstvena

sposobnost skrivanja ubrzo je zapela za oko

hakerima loših namjera kao idealan način da

11

00:01:30,700 --> 00:01:33,466

prikriju svoje zlokobne aktivnosti.

12

00:01:33,466 --> 00:01:46,199

Izraz „rootkit“ zapravo je nastao spajanjem

engleskih izraza „root“ (Unix referenca koja

implicira korijenski pristup sustavu i

13

00:01:46,200 --> 00:01:57,733

administratorske privilegije) i riječi „kit“ – komplet

alata (odnosi se na komplet alata koji se rabe za

dobivanje takvoga skrivenoga i privilegiranog

14

00:01:57,733 --> 00:01:59,899

pristupa).

15

00:01:59,900 --> 00:02:10,566

Alati za dobivanje administratorskih ovlasti na

sustavu (rootkit) jesu programi osmišljeni ne samo

da skrivaju sebe nego i da skrivaju druge

16

00:02:10,566 --> 00:02:21,932

programe i sve njima pridružene resurse (procese,

datoteke, mape, priključne točke, pogonske

programe (driver), vrijednosti registara) i to je

17

00:02:21,933 --> 00:02:31,033

zapravo cijeli smisao njihova postojanja. Usko su

povezani s drugim štetnim kodom tako da

uglavnom trebaju neku vrstu zlonamjernog

18

00:02:31,033 --> 00:02:43,933

programa da bi došli do ciljanog računala. A zatim,

kad stignu na cilj, obično se rabe da bi prikrivali

neki drugi štetni kod. Isključiva im je namjera

19

00:02:43,933 --> 00:02:46,399

krađa korisničkih podataka.

20

00:02:46,400 --> 00:02:56,266

Klasificiraju se kao: dobronamjerni (white-hat), i

označuju sigurnosni rizik i

21

00:02:56,266 --> 00:03:08,899

zlonamjerni (black-hat), čiji je cilj napraviti štetu.

Oni svoj posao obavljaju skrivajući svoj zlonamjerni

kod (malware) koji instalira stražnja vrata koja će

22

00:03:08,900 --> 00:03:20,700

na kraju omogućiti napadaču nesmetan i

neograničen pristup inficiranom računalu. Jednako

tako, prikrivaju prisutnost napadača u sustavu tako

23

00:03:20,700 --> 00:03:29,433

da npr. omogućuju da se napadač prijavi u sustav

bez generiranja sistemskih zapisa (log).

24

00:03:29,433 --> 00:03:37,866

Lekcija je završena.

# Zaštita računala

1

00:00:00,000 --> 00:00:09,000

Dobrodošli. U ovom videu upoznat ćemo se sa načinima zaštite računala.

2

00:00:09,000 --> 00:00:20,533

Zaštita računala vrlo je slojevita i komplicirana, a najbolji način zaštite računala od napadača i zlonamjernog koda jest korištenje aplikacijama

3

00:00:20,533 --> 00:00:24,399

napravljenima upravo za te svrhe.

4

00:00:24,400 --> 00:00:34,266

Jedna od takvih aplikacija je i vatrozid (firewall) koja spada u nužne aplikacije za zaštitu računala jer je prva crta obrane od zlonamjernih

5

00:00:34,266 --> 00:00:43,432

aplikacija i pokušaja provaljivanja. Analogno tomu, uloga vatrozida sprječavanje je neovlaštene komunikacije između našeg računala i

6

00:00:43,433 --> 00:00:46,033

Interneta.

7

00:00:46,033 --> 00:00:53,099

Kao što se dade zaključiti, vatrozid nam može poboljšati zaštitu našeg računala od napada hakera

8

00:00:53,100 --> 00:01:02,066

ili zlonamjernih programa poput crva. Isto tako, jedna od bitnih mogućnosti vatrozida je i sprječavanje da, ukoliko je naše računalo

9

00:01:02,066 --> 00:01:08,032

inficirano, pošalje zlonamjerne programe drugim učesnicima na mreži.

10

00:01:08,033 --> 00:01:18,599

Nekada je bilo dovoljno samo imati instaliran vatrozid, kako bi korisnik bio zaštićen na Internetu, no danas su ta vremena daleko iza nas.

11

00:01:18,600 --> 00:01:27,200

S obzirom na činjenicu da svakodnevno nastaju nove vrste i oblici štetnih programa, potrebno je imati ispravno podešen vatrozid, ali i antivirusni

12

00:01:27,200 --> 00:01:29,900

program.

13

00:01:29,900 --> 00:01:37,666

U nastavku videa vidjet ćemo podešavanje antivirusnog programa i vatrozida.

14

00:01:37,666 --> 00:01:44,866

S desne strane u meniju potražite "Postavke". Kliknite.

15

00:01:44,866 --> 00:01:48,732

Nakon toga odaberite "Upravljačka ploča",

16

00:01:48,733 --> 00:01:51,833

"Sustav i sigurnost",

17

00:01:51,833 --> 00:01:55,833

"Vatrozid za Windows".

18

00:01:55,833 --> 00:02:02,699

Nakon što smo ga odabrali, otvara nam se slijedeći dijaloški okvir. Kroz njega možemo napraviti

19

00:02:02,700 --> 00:02:05,766

sve prilagodbe vatrozida.

20

00:02:05,766 --> 00:02:13,032

Ono što bi svi trebali imati napravljeno je opcija: "Uključi vatrozid za Windows".

21

00:02:13,033 --> 00:02:21,899

Da li je vatrozid uključen možemo provjeriti tako da kliknemo na „Uključivanje ili isključivanje vatrozida za Windows“.

22

00:02:21,900 --> 00:02:25,733

Provjerite da li imate postavke kao što je trenutno na ekranu.

23

00:02:25,733 --> 00:02:35,466

Postavka je odabrana po zadanoj postavci. Kada je vatrozid za Windows uključen, blokirano je primanje informacija za većinu aplikacija kroz

24

00:02:35,466 --> 00:02:37,466

vatrozid.

25

00:02:37,466 --> 00:02:47,132

Ako želite nekoj aplikaciji dopustiti primanje informacija, slijedite korake u nastavku, a da biste je dodali na popis dopuštenih aplikacija.

26

00:02:47,133 --> 00:02:57,799

Primjerice, ako želimo da nam je Windows Media Player na popisu dopuštenih aplikacija, odaberite „Propuštanje aplikacije ili značajke kroz Vatrozid

27

00:02:57,800 --> 00:03:04,833

za Windows“, te u slijedećem dijaloškom okviru kliknite na Windows Media

28

00:03:04,833 --> 00:03:08,899

Player.Potvrdite sa U redu.

29

00:03:08,900 --> 00:03:17,666

Slijedeća mogućnost koju imamo sa lijeve strane je „Promjena postavki obavijesti“, koju kada smo odabrali imamo mogućnost da nas Vatrozid za

30

00:03:17,666 --> 00:03:21,866

Windows obavijesti kad blokira aplikaciju te će nam

31

00:03:21,866 --> 00:03:33,132

dati mogućnost da ju odblokiramo.

32

00:03:33,133 --> 00:03:43,333

Slijedeća opcija koju imamo je „Vraćanje zadanih postavki“ koja nas vraća na predefinirane postavke vatrozida.

33

00:03:43,333 --> 00:03:52,666

Zatim, ono što imamo još slijeve strane je mogućnost „Dodatne postavke“.Ona nam daje slobodu, da ukoliko naše aplikacije,

34

00:03:52,666 --> 00:04:01,066

koju želimo dozvoliti, nema na popisu aplikacija koje možemo dopustiti, poput Windows Media Playera u prethodnim koracima.

35

00:04:01,066 --> 00:04:17,099

U tom slučaju, kliknemo na New rule (Novo pravilo), odaberemo vrstu priključka te da li se radi o TCP ili UDP priključku i upišemo broj njegovog

36

00:04:17,100 --> 00:04:43,000

priključka. Kliknemo Next, dozvolimo konekciju, potvrdimo sa Next, odaberemo profil mreže i damo joj ime.

37

00:04:43,000 --> 00:04:54,733

Primjerice, isto možemo napraviti da bi s prijateljima igrali mrežnu igru za više igrača, bilo bi dobro da otvorite priključak za tu igru da bi

38

00:04:54,733 --> 00:05:00,999

vatrozid dopustio prolaz informacija o igri do vašeg računala. Oprez! Priključak ostaje otvoren cijelo vrijeme, stoga uvijek zatvorite

39

00:05:01,000 --> 00:05:04,033

priključke koje više ne trebate.

40

00:05:04,033 --> 00:05:11,766

U nastavku ćemo vidjeti podešavanje aplikacije Windows Defender.Da li je PC zaražen virusom možete brzo provjeriti

41

00:05:11,766 --> 00:05:21,132

pomoću programa Windows Defender. Ta je aplikacija za zaštitu od zlonamjernog softvera dostupna u sklopu sustava Windows, a omogućuje

42

00:05:21,133 --> 00:05:27,433

otkrivanje i uklanjanje virusa, špijunskog softvera i drugog zlonamjernog softvera.

43

00:05:27,433 --> 00:05:41,033

Otvorite Windows Defender tako da prijeđete mišem do desnog ruba zaslona, odaberite Pretraživanje, u okvir za pretraživanje unesite

44

00:05:41,033 --> 00:05:48,933

Defender, a zatim kliknete. Windows Defender.

45

00:05:48,933 --> 00:06:03,433

U odjeljku Mogućnosti pregleda odaberite vrstu pregleda koju želimo pokrenuti: Brzi pregled provjerava samo područja na PC-ju koja

46

00:06:03,433 --> 00:06:06,433

zlonamjerni softver najčešće zarazi te trenutno

47

00:06:06,433 --> 00:06:07,366

pokrenute

48

00:06:07,366 --> 00:06:10,432

aplikacije.

49

00:06:10,433 --> 00:06:20,166

Potpuni pregled provjerava sve datoteke na PC-ju. Pregled može trajati jedan sat ili duže, a to ovisi o vašem PC-ju.

50

00:06:20,166 --> 00:06:32,332

Prilagođeni pregled provjerava samo datoteke i mjesta koja odaberete.

51

00:06:32,333 --> 00:06:38,999

Odaberite "Pregledaj sada". U slijedećem dijaloškom okviru odaberemo lokaciju za koju sumnjamo

52

00:06:39,000 --> 00:06:54,666

da se na njoj nalazi neki virus ili crv.Potvrdimo sa U redu nakon toga kreće skeniranje našeg računala.

53

00:06:54,666 --> 00:06:59,266

Windows Defender viruse najčešće uklanja automatski. No u nekim ćete slučajevima virus možda

54

00:06:59,266 --> 00:07:07,599

morati ukloniti ručno.To može biti tehnički zahtjevan postupak koji se preporučuje samo ako ste iscrpili sve druge

55

00:07:07,600 --> 00:07:16,833

mogućnosti, ako ste upoznati s registrom sustava Windows te znate kako uključiti prikaz sistemskih i programskih datoteka u sustavu

56

00:07:16,833 --> 00:07:25,633

Windows i kako ih izbrisati. Najprije pokrenite aplikaciju protiv zlonamjernog softvera da biste saznali o kojem se virusu radi.

57

00:07:25,633 --> 00:07:34,266

Ako nemate aplikaciju protiv zlonamjernog softvera ili ako vaša aplikacija ne otkrije virus, možda ćete ga ipak moći prepoznati

58

00:07:34,266 --> 00:07:43,332

promatranjem njegova ponašanja.Zapišite riječi u porukama koje prikazuje ili, ako ste virus primili u poruci e-pošte, zapišite

59

00:07:43,333 --> 00:07:52,966

predmet ili naziv datoteke priložene poruci. Potom na web-mjestu proizvođača antivirusnog programa ili u Microsoftovu centru za zaštitu od

60

00:07:52,966 --> 00:08:03,366

zlonamjernog softvera potražite reference o tome što ste zapisali i pokušajte pronaći naziv virusa i upute za njegovo uklanjanje.

61

00:08:03,366 --> 00:08:12,532

Za antivirusne programe općenito, a isto tako i za Windows Defender vrlo je bitno da je redovito ažuriran te da ima uvijek najnovije definicije

62

00:08:12,533 --> 00:08:18,366

malicioznih programa, kako bi ih mogao prepoznati.

63

00:08:18,366 --> 00:08:21,399

Lekcija je završena.