Lekcija\_2\_1\_1

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.

Lekcija\_2\_1\_2

1

00:00:01,866 --> 00:00:07,966

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

2

00:00:07,966 --> 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 --> 00:00:25,966

program).

4

00:00:25,966 --> 00:00:38,432

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

5

00:00:38,433 --> 00:00:44,499

Rootkitove

6

00:00:44,500 --> 00:00:48,966

i Zadnja vrata (Back doors).

7

00:00:48,966 --> 00:00:59,499

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

8

00:00:59,500 --> 00:01:06,900

Po tipovima ih možemo podijeliti na: Viruse

9

00:01:06,900 --> 00:01:09,766

i Crve.

10

00:01:09,766 --> 00:01:13,699

Lekcija je završena.

Lekcija\_2\_1\_3

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.

Lekcija\_2\_1\_4

1

00:00:00,000 --> 00:00:10,933

Dobrodošli. U ovoj lekciji ćemo se upoznati s crvima, kao sljedećom vrstom malicioznih programa.

2

00:00:10,933 --> 00:00:23,233

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

3

00:00:23,233 --> 00:00:28,266

domaćine i inficirati ih preko mreže.

4

00:00:28,266 --> 00:00:37,566

Mnogi često poistovjećuju crve s virusima, nazivajući ih samo posebnom podvrstom virusa. Jednako tako, mnogi bi poznati štetni programi

5

00:00:37,566 --> 00:00:46,632

koji su popularno prozvani virusima po pravilu trebali biti smatrani crvima ili hibridima tih dviju vrsta štetnih programa.

6

00:00:46,633 --> 00:00:55,733

Točno je da crvi imaju neka zajednička obilježja s virusima. Najvažnije obilježje koje dijele jest mogućnost samo repliciranja, samo umnažanja,

7

00:00:55,733 --> 00:01:05,233

no u načinu umnažanja se razlikuju. Prvo, crvi ne trebaju domaćina da bi se širili kao virusi za koje možemo reći da se takoreći ponašaju kao

8

00:01:05,233 --> 00:01:15,899

paraziti, crvi su samostalni, samostalno djeluju i šire se. Druga je razlika što je osnovni medij širenja crva mreža odnosno Internet.

9

00:01:15,900 --> 00:01:28,466

Dakle, virusi se šire inficirajući druge programe, drugi kod, a crvi imaju sposobnost samostalne migracije sa sustava na sustav preko mreže.

10

00:01:28,466 --> 00:01:41,032

Crv koji se nalazi na nekom računalu traži druga dostupna računala preko lokalne mreže (LAN) ili preko internetske veze. Kad pronađe drugo

11

00:01:41,033 --> 00:01:51,599

računalo, replicira se, kopira se na to novo računalo, odakle ta kopija, odnosno nova instanca crva dalje traži nova računala. Dvije najčešće

12

00:01:51,600 --> 00:02:01,000

metode širenja crva jesu: elektronička pošta (e-mail) i iskorištavanje sigurnosnih slabosti i propusta na računalima spojenima na mrežu ili na

13

00:02:01,000 --> 00:02:03,033

Internet.

14

00:02:03,033 --> 00:02:16,533

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

15

00:02:16,533 --> 00:02:27,266

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

16

00:02:27,266 --> 00:02:40,266

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

17

00:02:40,266 --> 00:02:50,399

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

18

00:02:50,400 --> 00:02:59,000

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

19

00:02:59,000 --> 00:03:11,133

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

20

00:03:11,133 --> 00:03:20,333

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

21

00:03:20,333 --> 00:03:25,033

inficiranim sustavom;

22

00:03:25,033 --> 00:03:36,533

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

23

00:03:36,533 --> 00:03:46,899

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

24

00:03:46,900 --> 00:03:56,633

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

25

00:03:56,633 --> 00:04:08,333

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

26

00:04:08,333 --> 00:04:20,133

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

27

00:04:20,133 --> 00:04:30,499

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

28

00:04:30,500 --> 00:04:40,366

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

29

00:04:40,366 --> 00:04:49,632

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

30

00:04:49,633 --> 00:04:57,933

bez ponavljanja prvotnog procesa napada.

31

00:04:57,933 --> 00:05:07,666

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

32

00:05:07,666 --> 00:05:17,666

sigurnosne provjere i autoru omogućuje pristup nekoj aplikaciji, operacijskom sustavu ili mreži. Pristup koji napadač dobiva ovisi o napadačevim

33

00:05:17,666 --> 00:05:29,632

namjerama i vrsti stražnjih vrata. Osnovne vrste pristupa koje takav kod omogućuje jesu sljedeće. Povećanje privilegija – takva vrsta stražnjih vrata

34

00:05:29,633 --> 00:05:39,166

napadaču koji ima skriveni korisnički račun na sustavu omogućuje mijenjanje tog računa u administratorski. S privilegijama administratora

35

00:05:39,166 --> 00:05:47,666

napadač može izmijeniti postavke računala ili pristupiti bilo kojoj datoteci smještenoj na računalu.

36

00:05:47,666 --> 00:06:02,366

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

37

00:06:02,366 --> 00:06:12,032

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

38

00:06:12,033 --> 00:06:23,599

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

39

00:06:23,600 --> 00:06:26,300

inficiranog računala.

40

00:06:26,300 --> 00:06:37,800

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

41

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

42

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

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

43

00:06:54,933 --> 00:07:06,166

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

44

00:07:06,166 --> 00:07:16,366

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

45

00:07:16,366 --> 00:07:24,032

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

46

00:07:24,033 --> 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

47

00:07:34,933 --> 00:07:45,533

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

48

00:07:45,533 --> 00:07:56,899

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

49

00:07:56,900 --> 00:08:07,133

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

50

00:08:07,133 --> 00:08:16,933

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

51

00:08:16,933 --> 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

52

00:08:26,433 --> 00:08:35,799

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

53

00:08:35,800 --> 00:08:44,700

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

54

00:08:44,700 --> 00:08:53,200

Druga je mogućnost da se sami „sakriju“ unutar nekog legitimnog poznatog programa poput Microsoftova Excela te da se zapravo integriraju

55

00:08:53,200 --> 00:09:03,300

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

56

00:09:03,300 --> 00:09:11,766

Lekcija je završena.

Lekcija\_2\_1\_5

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.

Lekcija\_2\_1\_6

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) prozor prema

8

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

podacima o njegovim navikama ili čak oglase vezane 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.

Lekcija\_2\_1\_6

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) prozor prema

8

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

podacima o njegovim navikama ili čak oglase vezane 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.

Lekcija\_2\_1\_7

1

00:00:00,000 --> 00:00:10,200

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

2

00:00:10,200 --> 00:00:19,766

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

3

00:00:19,766 --> 00:00:26,232

modemske veze te biranje telefonskih brojeva bez dozvole korisnika računala.

4

00:00:26,233 --> 00:00:35,699

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

5

00:00:35,700 --> 00:00:40,733

s pomoću kojih smo se svojedobno spajali na Internet.

6

00:00:40,733 --> 00:00:49,633

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

7

00:00:49,633 --> 00:00:53,599

cijena poziva skupo naplaćivana.

8

00:00:53,600 --> 00:01:04,500

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

00:01:04,500 --> 00:01:13,933

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

10

00:01:13,933 --> 00:01:16,833

visokom cijenom poziva.

11

00:01:16,833 --> 00:01:32,966

Lekcija je završena.

Lekcija\_2\_1\_8

1

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

Dobrodošli. U ovoj lekciji upoznat ćemo se s najsofisticiranijim 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 Windows 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.

Lekcija\_2\_1\_9

1

00:00:00,000 --> 00:00:07,566

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

2

00:00:07,566 --> 00:00:17,799

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

3

00:00:17,800 --> 00:00:21,033

napravljenima upravo za te svrhe.

4

00:00:21,033 --> 00:00:31,399

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

5

00:00:31,400 --> 00:00:40,066

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

6

00:00:40,066 --> 00:00:43,432

Interneta.

7

00:00:43,433 --> 00:00:52,499

Kao što se dade zaključiti, vatrozid nam može poboljšati zaštitu našeg računala od napada hakera ili zlonamjernih programa poput crva.

8

00:00:52,500 --> 00:01:02,433

Isto tako, jedna od bitnih mogućnosti vatrozida je i sprječavanje da, ukoliko je naše računalo inficirano, pošalje zlonamjerne programe drugim

9

00:01:02,433 --> 00:01:05,033

učesnicima na mreži.

10

00:01:05,033 --> 00:01:17,233

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

11

00:01:17,233 --> 00:01:27,266

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

12

00:01:27,266 --> 00:01:35,166

U nastavku videa vidjet ćemo podešavanje antivirusnog programa i vatrozida.

13

00:01:35,166 --> 00:01:41,232

S desne strane u meniju potražite "Postavke".

14

00:01:41,233 --> 00:01:46,233

Kliknite. Nakon toga odaberite "Upravljačka ploča",

15

00:01:46,233 --> 00:01:50,299

"Sustav i sigurnost",

16

00:01:50,300 --> 00:01:54,000

"Vatrozid za Windows".

17

00:01:54,000 --> 00:02:02,500

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

18

00:02:02,500 --> 00:02:14,800

Ono što bi svi trebali imati napravljeno je opcija: "Uključi vatrozid za Windows". Da li je vatrozid uključen možemo provjeriti tako da kliknemo na

19

00:02:14,800 --> 00:02:18,633

„Uključivanje ili isključivanje vatrozida za Windows“.

20

00:02:18,633 --> 00:02:30,399

Nakon što ste kliknuli, provjerite da li imate postavke kao što je trenutno prikazano na ekranu. Postavka je odabrana po zadanoj vrijednosti.

21

00:02:30,400 --> 00:02:38,200

Kada je vatrozid za Windows uključen, blokirano je primanje informacija za većinu aplikacija kroz vatrozid.

22

00:02:38,200 --> 00:02:49,300

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

23

00:02:49,300 --> 00:03:00,166

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

24

00:03:00,166 --> 00:03:02,299

za Windows“,

25

00:03:02,300 --> 00:03:10,000

te u sljedećem dijaloškom okviru kliknite na Windows Media Player. I potvrdite sa "U redu".

26

00:03:10,000 --> 00:03:18,200

Sljedeća mogućnost koju imamo sa lijeve strane je „Promjena postavki obavijesti“, koju kada smo

27

00:03:18,200 --> 00:03:29,000

odabrali imamo mogućnost da nas Vatrozid zaWindows obavijesti kada blokira aplikaciju te će nam dati mogućnost da ju odblokiramo.

28

00:03:29,000 --> 00:03:39,966

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

29

00:03:39,966 --> 00:03:49,899

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

30

00:03:49,900 --> 00:04:00,233

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

31

00:04:00,233 --> 00:04:06,399

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

32

00:04:06,400 --> 00:04:17,600

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

33

00:04:17,600 --> 00:04:23,100

Defender, a zatim kliknete na "Windows Defender."

34

00:04:23,100 --> 00:04:34,900

U odjeljku "Mogućnosti pregleda" odaberite vrstu pregleda koju želite pokrenuti: Brzi pregled provjerava samo područja na računalu koja

35

00:04:34,900 --> 00:04:40,400

zlonamjerni softver najčešće zarazi te trenutnopokrenute aplikacije.

36

00:04:40,400 --> 00:04:55,866

Potpuni pregled provjerava sve datoteke na računalu. Pregled može trajati jedan sat ili duže, a to ovisi o brzini Vašeg računala.

37

00:04:55,866 --> 00:05:07,799

Prilagođeni pregled provjerava samo datoteke i mjesta koja odaberete. Odaberite "Prilagođeno" i "Odmah pregledaj".

38

00:05:07,800 --> 00:05:20,100

U slijedećem dijaloškom okviru odaberemo lokaciju za koju sumnjamo da se na njoj nalazi neki virus ili crv. Potvrdimo sa "U redu" i nakon toga

39

00:05:20,100 --> 00:05:28,200

kreće skeniranje našeg računala.

40

00:05:28,200 --> 00:05:35,066

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

41

00:05:35,066 --> 00:05:43,132

To može biti tehnički zahtjevan postupak koji se preporučuje samo ako ste iscrpili sve drugemogućnosti.

42

00:05:43,133 --> 00:05:52,666

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

43

00:05:52,666 --> 00:05:56,566

malicioznih programa, kako bi ih mogao prepoznati.

44

00:05:56,566 --> 00:06:05,666

Ako je program Windows Defender ključen, obavijestit će vas ako se špijunski ili drugi potencijalno neželjeni program pokuša pokrenuti ili

45

00:06:05,666 --> 00:06:08,866

instalirati na računalo.

46

00:06:08,866 --> 00:06:09,966

Ako koristite

47

00:06:09,966 --> 00:06:18,766

zadane postavke, program Windows Defender također provjerava ima li novih definicija (datoteke koje se koriste za određivanje je li neki softver

48

00:06:18,766 --> 00:06:29,832

špijunski) te automatski uklanja sve otkrivene stavke za koje ima preporučenu akciju uklanjanja.Windows Defender nudi dva načina zaštite

49

00:06:29,833 --> 00:06:40,066

računala od zaraze špijunskim softverom: Prvi je "Zaštita u stvarnom vremenu".‍‍ Windows Defender upozorava kada se špijunski softver pokuša

50

00:06:40,066 --> 00:06:49,032

instalirati ili pokrenuti na računalu. I drugi je: "Mogućnosti pregledavanja". Windows Defender može se koristiti za pregled računala radi

51

00:06:49,033 --> 00:06:58,366

otkrivanja špijunskog softvera koji je možda instaliran na računalu, za zakazivanje redovitih pregleda, te za automatsko uklanjanje bilo čega

52

00:06:58,366 --> 00:07:00,766

otkrivenog tijekom pregleda.

53

00:07:00,766 --> 00:07:08,932

Prilikom korištenja programa Windows Defender važno je imati ažurne definicije. Definicije su datoteke koje djeluju kao stalno dopunjavane

54

00:07:08,933 --> 00:07:13,799

enciklopedije potencijalnih softverskih prijetnji.

55

00:07:13,800 --> 00:07:23,033

Windows Defender definicije koristi za upozorenje o potencijalnim rizicima ako utvrdi da je otkriveni softver zapravo špijunski ili neki drugi potencijalno

56

00:07:23,033 --> 00:07:25,099

neželjeni softver.

57

00:07:25,100 --> 00:07:36,433

Da bi definicije bile ažurne, Windows Defender u kombinaciji sa servisom Windows Update automatski instalira nove definicije čim se objave.

58

00:07:36,433 --> 00:07:46,099

Kad Windows Defender program stavi u karantenu, premješta ga na drugo mjesto na računalu te sprječava njegovo pokretanje sve dok

59

00:07:46,100 --> 00:07:51,600

ne odaberete njegovo vraćanje ili uklanjanje s računala.

60

00:07:51,600 --> 00:08:21,400

Lekcija je završena.