CARNet

HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Osnovno korištenje portala antibot.hr

NCERT-PUBDOC-2014-08-343

Nacionalni CERT

ACDC

Nacionalni CERT

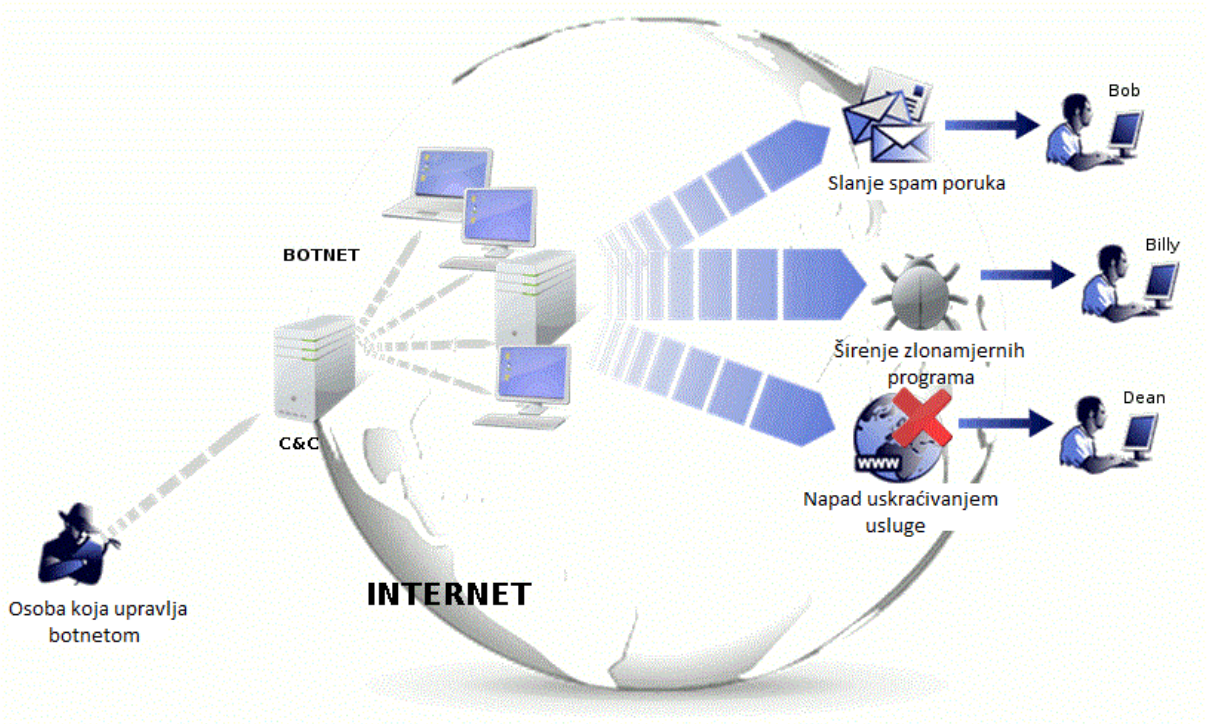
Sadržaj

Ovaj dokument pripremljen je uz financijsku podršku Europske unije. Sadržaj rada izražava mišljenje autora i ni na koji način ne izražava mišljenje i stavove Europske unije.

1 Botneti i botovi

Čitanjem ovog dokumenta dobit će te uvid u najveću sigurnosnu prijetnju na Internetu – **botnete**, način njihovog funkcioniranja, odnosno širenja zaraze na druga računala te kako obraniti svoje računalo.

Bot (zaraženo računalo ili tzv. „zombie“) je sastavni dio velike mreže računala s kojima upravlja računalni kriminalac. Naredbe koje šalje računalni kriminalac s udaljenog računala, izvršit će se bez da ih vlasnik zaraženog računala opazi. Te naredbe služe za distribuciju neželjenog i zlonamjernog sadržaja na druga računala, krađu financijskih sredstava (podataka o karticama), napade uskraćivanjem usluge te distribuciju spam poruka. Prema tome, botneti služe kao osnovna infrastruktura Internetskom kriminalu i jedni su od najvećih ilegalnih izvora prihoda na Internetu.



Alati koji su dostupni na portalu antibot.hr služe kako bi korisnici mogli provjeriti da li im je računalo zaraženo te ga u tom slučaju očistiti. Postoji također alat koji nudi zaštitu od pokretanja zlonamjernog koda unutar web preglednika i tako štiti računalo od toga da postane bot. Tu su i online skeneri koji pregledavaju računalo u potrazi za ranjivostima u softveru koji bi neki zlonamjerni program mogao iskoristiti. Initiative-S servis služi za periodičko pregledavanje registrirane web stranice u potrazi za zlonamjernim kodom koji bi mogao zaraziti posjetitelje te web stranice. Svi navedeni alati i servisi prvenstveno ciljaju na zaštitu krajnjih korisnika. Kako alati i online skeneri rade, detaljnije je objašnjeno u nastavku dokumenta.

2 Initiative-S sigurnosni servis za web sjedišta

Prema Symantecovon izvještaju o sigurnosti Interneta, više od pola računalnih napada u svijetu usmjereno je na mala i srednja poduzeća. Web stranice poduzeća koje su zaražene zlonamjernim kodom predstavljaju opasnost na Internetu, ne samo za vlasnike poduzeća, već i za njihove korisnike i partnere. U slučaju da je web stranica zaražena, a pristupa joj korisnik koji nema adekvatnu zaštitu, zaraza se širi i na njegovo računalu te na taj način ono može postati dio botnet mreže. Napadači obično ubacuju skriveni (zlonamjerni) kod na web stranicu s ciljem da zaraze što veći broj posjetitelja web stranice, a da pritom taj kod bude što duže neotkriven. Time napadači (operatori botneta) žele povećati broj zaraženih računala u svojoj botnet mreži.

Initiative-S je sigurnosni servis pružen od strane eco-a (udruženje njemačke Internet industrije) koji na dnevnoj bazi provjerava je li Vaša web stranica zaražena. Pokušavaju se pronaći maliciozne php/Java skripte, softverska preuzimanja, maskirane skripte i poveznice prema zlonamjernim stranicama. Vlasnik web stranice dobiva obavijest ukoliko se pronađe zlonamjeran sadržaj. Ukoliko je stranica "čista", vlasnik stranice ne dobiva nikakvu obavijest. Kako bi prijavili svoju web stranicu za periodičko skeniranje, potrebno je posjetiti web stranicu Initiative-S i obaviti potrebne korake. Detaljnije upute možete pronaći na web stranici http://antibot.hr/initiatives

3 Programi za otklanjanje malicioznih sadržaja i otklanjanje prijetnji na računalima krajnjih korisnika

EU-Cleaner je program koji služi za uklanjanje zlonamjernog sadržaja s Vašeg računala zbog kojih je računalo dio botnet mreže. Detaljne upute za korištenje programa, kao i poveznicu za njegovo preuzimanje možete pronaći na web stranici http://www.antibot.hr/blog/eu-cleaner/

HitmanPro.Alert je besplatan dodatak Internet pregledniku i alat za detekciju uljeza koji upozorava korisnika prilikom izvođenja nesigurnog online bankarstva i financijskih transakcija. U zadnjoj inačici HitmanPro.Alerta nalazi se dodatak zvan CryptoGuard, koji prati i obavještava o sumnjivim operacijama nad korisnikovim datotečnim sustavom. Ukoliko HitmanPro.Alert primjeti sumnjivo ponašanje, zlonamjerni kôd se neutralizira, a datoteke ostaju zaštićene.
Detaljne informacije o načinu rada dodatka, kao i poveznicu za njegovo preuzimanje možete pronaći na web stranici http://www.antibot.hr/blog/hitmanpro-alert/

Na portalu je moguće naći poveznice i na niz drugih antivirusnih alata, kako za privatne korisnike, tako i za pravne osobe. Popisu alata i poveznicama za njihovo preuzimanje za privatne korisnike možete pristupiti na stranici http://antibot.hr/popisalata, te na stranici http://antibot.hr/pravneosobe za pravne osobe.

4 Održavanje operacijskog sustava i instaliranih programa ažurnim

Proizvođači operacijskih sustava i aplikacija redovito izdaju nove, osvježene inačice i ažuriranja koji poboljšavaju sigurnost njihovih proizvoda. Praćenje svakog pojedinog programa može biti zahtjevan posao, stoga Vam preporučamo instaliranje jednog od dva poznatija alata namijenjena za to, **Secunia PSI** ili **CSIS Heimdal**. Pomoću njih na jednom mjestu dobivate uvid u stanje i verziju Vašeg operacijskog sustava i programa instaliranih na njemu. Navedene alate možete preuzeti na web stranici https://www.check-and-secure.com/completion/_hr/

5 Provjera otvorenih portova

Važan korak u očuvanju sigurnosti Vašeg računala je provjera otvorenih portova. **Portovi** su krajnje točke komunikacije koji računalu omogućuju istovremenu komunikaciju s više drugih računala, poslužitelja i mrežnih uređaja. Skeniranjem portova utvrđuje se njihova potencijalna ranjivost, „otvorenost" za ubacivanje zlonamjernog koda. Zatvaranjem nepotrebnih portova smanjuje se mogućnost zaraze Vašeg računala. Čest slučaj je da računala/poslužitelji koji su već zaraženi zlonamjernim programima koriste tehniku skeniranja otvorenih portova na drugim računalima u mreži s ciljem širenja zaraze. Na stranici https://www.check-and-secure.com/portcheck/_hr/ moguće je obaviti provjeru otvorenih portova na Vašem računalu i ovisno o rezultatu zatvoriti nepotrebne/kritične.

6 Provjera ranjivosti web preglednika

Web preglednik s kojim pristupate sadržajima na Internetu je kompleksan program koji u sebi sadrži velik broj programskih dodataka s kojima se olakšava rad. Zastarjele verzije tih dodataka u sebi sadrže ranjivosti koje se otklanjaju u novim verzijama. Veliki broj zaraza zlonamjernim programima može se izbjeći ukoliko su dodatci web preglednika redovno ažurirani. Provjeru dodataka Vašeg web preglednika moguće je obaviti na web stranici https://www.check-and-secure.com/browsercheck/_hr/