

Botneti

Omrežja okuženih računalnikov

..KRIMINALNE ZDRUŽBE SO POTENCIAL INTERNETA ZA SVOJE FINANČNO MOTIVIRANE ZLORABE ODKRILE ŽE PRED ČASOM. MEDTEM SO OSVOJILE TUDI ZNANJE, KI JIM OMOGOČA GRADNJO LASTNIH OMREŽIJ Z OKUŽENIMI RAČUNALNIKI – BOTNETOV..



Trend povezovanja okuženih računalnikov v botnete je februarja 2000 začel takrat 15-letni Kanadčan Michael Calce, ki je bil kasneje obsojen na vsega osem mesecev hišnega pripora, brez dostopa do računalnikov. Calce, bolj znan pod vzdevkom MafiaBoy, je svoj botnet zgradil iz osemdesetih računalnikov, večina teh se je nahajala v učilnicah njegove srednje šole, uporabljal pa jih je za DDoS napade (porazdeljene ohromitvene napade na storitve). Na kolena je uspel spraviti spletne velikane kot so eBay, Yahoo, Amazon, CNN in nekateri drugi. Danes, deset let kasneje, so kompleksna in dinamična botnet omrežja primarno sredstvo organiziranih skupin kiberkriminalcev za svoje dejavnosti. Upravljalca takšnega omrežja ima skozi nadzorni center botneta na svojih strežnikih nad okuženimi računalniki ali tako

imenovanimi zombiji popoln nadzor, uporabljajo pa jih lahko za prej omenjene DDoS napade, okuževanje in vdore na spletne strani, vrivanje SQL stavkov (SQL injection), krajo osebnih podatkov, izsiljevanja, pošiljanje neželene in ribarskih sporočil ter vse ostale nevarne dejavnosti. Svoja botnet omrežja preko spletnih forumov ponujajo celo v najem.

Botneti v veliki večini vključujejo računalnike z operacijskimi sistemi Microsoft Windows, letos pa so odkrili tudi dve različici botneta OSX.I-service, ki ogroža tudi operacijske sisteme Mac OS X. Obstajajo tudi botneti z operacijskimi sistemi Linux ter celo takšni, ki vključujejo mobilne telefone Apple iPhone.

Dejstvo je, da botneti postajajo vse večja težava. Zaenkrat je boj proti upravljalcem takšnih omrežij mogoč le s sodelovanjem strokovnjakov s področja informacijske varnosti, ponudniki internetnih storitev in predstavniki zakona. S takšnim sodelovanjem so v preteklosti že uspeli zapreti tri podjetja - EstDomains, Atrivo in McColo. Na strežnikih slednjega so bili nameščeni nadzorni centri nekaterih največjih botnetov za pošiljanje neželene pošte. Ko so podjetje odrezali od interneta in ga zaprli je število poslanih neželene pošte po celem svetu čez noč padlo za več kot 50 odstotkov!

Svoj računalnik lahko pred tem, da postane

eset NOD32 TOP 10 <small>www.eset.si</small>	
Deset najbolj razširjenih groženj v zadnjem tednu	
	število okuženih e-sporočil
različica Win32/Injector.BZ trojan	12016
Win32/Zafi.B worm	11694
Win32/Netsky.Q worm	6922
Win32/Netsky.C worm	1406
Win32/Mydoom.Q worm	810
različica Win32/Kryptik.BEN trojan	602
Win32/Merond.AA worm	494
Win32/Netsky.Z worm	290
Win32/Bagle.HE worm	208
Win32/Netsky.D worm	161

zombie in del botneta zaščitite z rednim posodabljanjem svojega operacijskega sistema in druge programske opreme, predvsem spletnih brskalnikov. Najpomembnejši del obrambe pred vsemi vrstami groženj pa je brez dvoma protivirusna rešitev na vašem računalniku. ESET NOD32 Antivirus in ESET Smart Security s svojo proaktivno zaščito skrbita, da ste pred novimi grožnjami varni že takoj ob izbruhu. Pred nekaj dnevi je ESET v beta različici predstavil tudi svojo varnostno rešitev za operacijska sistema Mac OS X in Linux (Debian in Red-Hat distribucije kot so Ubuntu, OpenSuse, Fedora in ostali) ter tako omogočil najvišjo možno stopnjo varnosti tudi uporabnikom teh operacijskih sistemov. (P.R.)

NOVE GENE, PRILAGOJENE RECESIJI

Varujemo vašo zasebnost

ESET SMART SECURITY

Antivirus
Antispyware
Firewall
Antispam

ESET NOD32 ANTIVIRUS

Antivirus
Antispyware

www.eset.si

SI SPLET, d. o. o. | Dolenjska c. 138, Ljubljana
01 428 94 05 | info@sisplet.com

SI SPLET
INFORMACIJSKE TEHNOLOGIJE