Botneti za distribuciju zloćudnog softwarea

Današnji *cyber* kriminalci koriste složene tehnike za isporuku zloćudnog softvera koji im omogućava stvaranje mreža sastavljenih od tuđih računala, kojima se onda koriste sami ili ih iznajmljuju drugima, a služe za slanje spamova, prikupljanje lozinki, brojeva kreditnih kartica, aktivističke napade na određene siteove i slično.

Botnetima se nazivaju mreže računala čije su zaštite probijene, pa više ne služe samo svojim legitimnim vlasnicima, već nekoj skrivenoj "trećoj strani". Sastoje se od botova (skraćeno od robot), pojedinačnih računala na koja je instaliran zloćudni softver, i kontrolera, također provaljenih računala koja s pomoću poznatih protokola poput IRC-a i HTTP-a uspostavljaju komunikacijske kanale kojima povezuju botove u mreže i upravljaju njima. Dok su botovi najčešće Windows računala, za kontrolere se koristi Linux.

Kako se stvaraju botneti? Najprije treba namamiti korisnika da si instalira trojanca, koji onda omogući da se tim računalom upravlja izvana. Standardni način su takozvani *drive-by* napadi, gdje korisnik, misleći da radi nešto drugo, "usput" pokupi trojanca. Primjeri su mailovi s prilozima, s tekstom koji nastoji primatelje navesti da kliknu na privitak ili na link i tako aktiviraju neki oblik virusa. To su trojanci-downloaderi, koji su u stanju s mreže skinuti dodatni softver za obavljanje konkretnih poslova, već prema potrebi vlasnika botneta. Koriste se i ranjivosti web preglednika, pa se otvaranjem inficiranih web stranica, klikanjem na slike i sličnim akcijama izaziva instalacija softvera na korisnička računala. Socijalni inženjering se koristi kako bi se ljude navelo da posjećuju sumnjive siteove, gdje se kao mamac nudi zanimljiv sadržaj, na primjer "besplatan" komercijalni software i filmovi. Za distribuciju malwarea koriste se porno siteovi i stranice koje obećavaju škakljive fotografije slavnih osoba, takozvanih *celebrityja*. Popularne društvene mreže često posluže kako bi se naivci naveli da posjete inficirane web stranice ili da skinu dokumente s trojancima, bilo da su to PDF-ovi, slike ili filmići, koji sadrže i skriveni kod. Još jedna od lukrativnih metoda za usmjeravanje na zločeste siteove je korištenje popularnih tražilica, gdje se koriste metode "search engine poisoninga". Za širenje zaraze mogu se koristiti i crvi, virusi koji ne zahtijevaju nikakvu pomoć od strane korisnika i sami se propagiraju, zahvaljujući nekoj tek otkrivenoj ranjivosti softvera koja još nije zakrpana.

Takve su mreže za isporuku zlonamjernih sadržaja (*Malware delivery networks*) dinamične i izuzetno prilagodljive, pa se korisnike stalno usmjerava na nove adrese koje plasiraju zaražene sadržaje, čime se otežava njihovo otkrivanje i blokiranje.

Zaštita od takvih složenih napada nije jednostavna. Više nije dovoljan antivirusni i antispam softver, ni tradicionalni firewall koji blokira adrese i portove. Napadači se mogu provući kroz otvorene portove, ukoliko firewall ne radi dubinsku analizu prometa.

Organizacije koje si to mogu priuštiti nabavljaju složenije uređaje, takozvane IPS-ove (*Intrusion Preventio System*) ili UTM-ove (*Universal Threat Management*), koji su evoluirali iz tradicionalnih firewala. Zato ih nazivaju još i *Next Generation Firewalls*. To su računala koja se postavljaju kao *gateway* tako da kroz njih prolazi sav promet organizacije, kako bi ga mogli pregledavati i analizirati. Oni su u stanju prepoznati i zaustaviti različite vrste napada i nepodobnog ponašanja, od virusa, spama, curenja informacija iz organizacije, a kao standardne funkcije nudi se blokiranje neželjenih web siteova, čiji sadržaji u najmanju ruku ne spadaju u poslovne procese. UTM-ovi ne pregledavaju samo e-mailove, već i FTP promet, web stranice, IRC kanale itd.

Dodatni bonus nabave takavog uređaja je činjenica da tvrtke koje ih proizvode i prodaju stvaraju svoju mrežu senzora i analizatora prometa, pa su u stanju stvoriti globalnu sliku prijetnji. Na primjer, ako jedan od IPS-ova otkrije IP adresu inficiranog računala, ta se adresa brzo propagira i postaje dio

crne liste. Kada takav uređaj prepozna promet koji izgleda sumnjivo, šalje ga na analizu, pa se tako otkrivaju nove vrste napada. Neke od tvrtki koje isporučuju IPS-ove nude svojim kupcima uslugu administriranja tih uređaja, ili podršku lokalnim administratorima, pa ih tako stručnjak obavještava, educira i savjetuje svaki puta kad se u mreži organizacije otkrije zloćudan promet.

Informacijska sigurnost postaje dio posla svakog informatičara i briga svakog educiranog korisnika, ali je količina informacija koju treba savladavati prevelika i traži obučenog specijalista koji će se baviti isključivo informacijskom sigurnošću. Zato je "rentanje" sigurnjaka koji nadziru rad IPS-a/UTM-a dobrodošla mogućnost za organizacije koje shvaćaju vrijednost svojih podataka, a ne žele ili ne mogu zaposliti i obučavati dodatnog stručnjaka s tako uskom specijalizacijom.

Tvrtke specijalizirane za informacijsku sigurnost izdaju godišnje izvještaje, u kojima se mogu naći zanimljive statistike i pregled novih trendova. Tako po lanjskom izvješću tvrtke Blue Coat ispada da se za usmjeravanje posjetitelja na malware siteove najviše koriste tražilice (39,2%), zatim e-mail (6,9%), pornografija (6,7%) i socijalne mreže (5,2%).

Najveća mreža za isporuku zloćudnih sadržaja koju je tvrtka Blue Coat otkrila nazvana je Shnakule. U prvoj polovini 2011. taj bi botnet dnevno namamio između 20.000 i 50.000 posjetitelja. Servirao im je lažne antivirusne programe, lažne dogradnje za Flash ili Firefox, *codece*, lažne ponude za posao od kuće, kockarske siteove i sumnjive farmaceutike. Prosječan broj računala uključenih u to mrežu iznosio je 2000. Shnakule je uključivao i druge botnete, na primjer Ishabor, specijaliziran za prodaju lažnih antivirusnih programa.

Treća mreža botova, Cinbric, nudila je ekskluzivan pristup web kamerama s porno sadržajima svima koji instaliraju njihov softver. Prosječan broj članova njihova botneta iznosio je 505, s maksimumom od 1602 računala, koja pripadaju pojedincima i organizacijama čiji zaposlenici gaje voajerske sklonosti.

Zanimljiva je i mreža Vidzeban, na koju se pomoću pretraživača usmjeravni ljudi koji su tražil *wareze*, piratski distribuirane sadržaje koji su inače autorski zaštićeni. Oni imaju svoju stalnu publiku, koja uz traženo dobije i skrivenog trojanca.

Sistemci iz iskustva znaju da korisnici koji skidaju takozvane generatore ključeva, programe koji generiraju aktivacijske kodove za komercijalni software, ubrzo zatraže pomoć sistemca, jer im se na računalo naselio virus. Tako među poslove sistemca spada i zaštita korisnika od njih samih. No kako napadi postaju sve složeniji i perfidniji, sve je veća potreba i za specijaliziranim zaštitnim uređajima i za specijalistima iz područja informacijske sigurnosti.

Pogledajte grafički prikaz mreže Shnakule [1].

pon, 2012-07-30 14:52 - Aco Dmitrović**Vijesti:** Sigurnost [2]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/1071

Links
[1] http://dubib.com/includes/image.php?image=/news_images/2011%2F07%2F826310994.jpg&width=600&height=350
[2] https://sysportal.carnet.hr/taxonomy/term/13