Autors: **Labi** Raksta ID= **273**

DDoS uzbrukumi mobilajiem tīkliem

Pēdējā laikā *Datuve.lv* ir daudz rakstu par dažādiem hakeru grupējumiem (LulzSecurity, Anonymous, AntiSec u.c.), kas zog datus no ASV valdības un turīgiem uzņēmumiem. Savus kiberuzbrukumus hakeri skaidro kā sodu konkrētajām institūcijām par viņuprāt netaisnīgām darbībām, piemēram, uzbrukumi PayPal saistīti ar to, ka šī kompānija aizvēra *Wikileaks* ziedojumiem paredzēto kontu. Interesanti, ka lielajos uzņēmumos strādā augstas klases drošības speciālisti, tomēr tas nepasargā no liela apjoma datu zādzībām.

Uzbrukt mājaslapai, meklējot kaut kādas programmētāja kļūdas ir pārāk ilgs un sarežģīts process, pietam administrators var izsekot hakera darbībām, tāpēc visbiežāk tiek veikti *DDoS* uzbrukumi. DDos (Distributed Denial of Service) uzbrukums ir vienlaicīga pieprasījumu veikšana serverim no ļoti daudziem inficētajiem datoriem , kas noved pie servera pārslodzes līdz ar to parastajiem lietotājiem konkrētais pakalpojums nav pieejams, bet hakeriem ir brīvs savu noziedzīgo darbību veikšanai. Pietam inficēto datoru īpašnieki bieži vien pat nezina, ka no viņu īpašuma tiek veikti pieprasījumi kādam attālinātam serverim, tāpēc šos datorus mēdz saukt par "zombijiem". Latvijā ir daudz "zaļo" hakeru, kas tālāk par servera "uzkāršanu" netiek, tomēr arī tas var radīt nopietnus zaudējumus.

Sanāca diezgan garš ievads, tagad var var ķerties pie raksta virsraksta tēmas. Pagājušā gada beigās pasaulē bija apmēram 4.6 miljardi mobilo telefonu, no tiem apmēram 20% ir viedtalruņi, kuriem ir iespējams ielādēt ar vīrusiem inficētas aplikācijas. Telefoni uz kuriem var uzinstalēt tikai **.JAR* aplikācijas šajā ziņā ir daudz drošāki, jo Java aplikācijām, lai veiktu kaut kādas nelietīgas darbības (piemēram, sūtīt SMS, zvanīt vai izmantot internetu), vismaz reizi ir "jāpaprasa" saimnieka atļauja. Tātad vai ir iespējams DDoS uzbrukums mobilajiem tīkliem? - Jā, bet to izdarīt ir daudz sarežģītāk nekā DDoS uzbrukumu WEB serverim, jo vienlaicīgi ir jāizpildās vairākiem noscījumiem:

1] Ir nepieciešama aplikācija (vīurss), kas viedtalruņa īpašniekam nezinot radīs slodzi mobilajam tīklam. Radīt slodzi var vairākos veidos, piemēram, sūtot vairākas SMS pēc kārtas bez pārtraukuma vai nepārtraukti izdarot zvanus (lai zvanīšana neaprautos kredīta trūkuma dēļ, varētu tikt izmantoti bezmaksas telefona numuri), vai arī pārsūtot lielus datu apjomus mobilajā internetā. Tā kā šobrīd vietalruņos tiek izmantotas dažādas operētājsistēmas, tad vīrusam ir jāpielāgojas visām populārākajām OS: iOS, Android, Blackberry un Symbian

2] Katram operatoram ir savs sakaru tīkls (izņemot virtuālos operatorus), tāpēc visiem inficētajiem viedtalruņiem jāizmanto viena konkrēta operatora pakalpojumi + virtuālo operatoru pakalpojumi, kas izmanto šo pašu tīklu, piemēram, LMT + Okarte + Amigo.

3] Visiem inficētajiem viedtalruņiem jāatrodas vienas bāzes stacijas tuvumā, jo ja tiks veikts DDoS uzbrukums ar viedtalruņiem, kas atrodas dažādās Latvijas malās, tad tas neradīs tīklam tik lielu slodzi kā

daudzi viedtalruņi, kas atrodas nelielā attālumā no vienas bāzes stacijas. Saprotams, ka jo vairāk ir inficēto viedtalruņu, jo lielāku pārslodzi tie rada uz konkrēto tīklu.
4] Lai hakeris zinātu, kad vienā nelielā teritorijā atrodas pietiekami daudz telefonu, lai varētu veikt kibernoziegumu, aplikācijai jāizmanto tā saukto **Geo Location** servisu, kas nosaka lietotāja atrašanās vietu. *Geo Location* tiek izmantots GPS aplikācijās, kā arī lielajos sociālajos tīklos kā **Facebook** un **Google+**.
5] Jābūt izstrādātam mehānismam, kā izplatīt ļaunprātīgo vīrusu pēc iespējas lielākā skaitā telefonu. Piemēram, pirmais Android vīruss izplatījās SMS veidā, kur tika lūgts ielādēt pavisam nelielu aplikāciju. Nesen pavīdēja informācija, ka katra 12. aplikācija **Android Marketā** satur vīrusu, tāpēc esiet uzmanīgi!

No augstāk minētajiem faktoriem ir skaidrs, ka DDoS uzbrukums mobilajiem tīkliem ir iespējams, tomēr to ir tehniski sarežģīti noorganizēt. Un kam gan būtu nepieciešams bojāt mobilo tīklu? - konkurentiem? ...Tas pagaidām nav skaidrs, tomēr jāatceras nesenais Tele2 tīkla "negadījums" (http://db.lv/tirdznieciba/pakalpojumi/papildinats-nedarbojas-tele2-tikls-skarti-vairak-neka-miljons-klientu-ari-igaunija-un-lietuva-241780) ,kad tika vainoti elektrības padeves truacējumi. Varbūt īstais iemesls bija kaut kas cits? Lai arī kā tur būtu, sakaru operatoriem īpaši jāuzmanās lielo mūzikas festivālu laikā, jo tad vienkopus ir ļoti daudz cilvēku. Šogad ļoti draudīgs varēja izrādīties *Positivus* festivāls, jo tas atbilst lielai daļai iepriekš minēto kritēriju. Pirms pasākuma tika izveidota Positivus aplikācija, kas varētu būt ļoti labs veids kā hakerim inficēt daudzus no festivālā klātesošajiem viedtalruņiem. Atliek tikai gaidīt vai DDoS uzbrukumi mobilajiem tīkliem nākotnē būs tikpat populāri, kā šobrīd WEB serveriem.

Izmantotie avoti: (WEB) http://articlesbase.com/cell-phones-articles/geo-location-based-ddos-on-mobile-networks-is-it-possible-3248156.html un (WEB) http://techworld.com/news/security/3253629/

Uzrakstīts:12:20 10-08-11