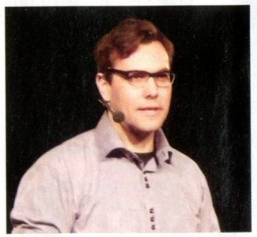
НЕВИДЉИВИ ИНТЕРНЕТ

КАО ГЛАВИЦА ЦРНОГ ЛУКА

У недавним догађајима у свету сви помињу улогу „Фејсбука”. Али, кумовали су им и противречни хакер и програм направљен за америчку војску

„Арапско пролеће”

Када је Џејкоб Епелбаум говорио на скупу арапских блогера у Бејруту 2009. године, знао је да ће привући посебну пажњу слушалаца. Протеклу годину овај двадесетшестогодишњи амерички програмер провео је у Египту, Јордану, Сирији, Тунису и Хонгконгу – обучавајући тамошње активисте и припаднике покрета како да употребљавају један, однедавно све омиљенији про-



Џејкоб Епелбаум на скупу арапских блогера

грам. Име му је „тор”, а корисници штити од покушаја било кога, па и власти, да прати њихово кретање по Интернету.

„Захваљујући овом програму, људи могу да раде шта год пожеле на мрежи, а да за собом не оставе траг”, поручио је тада Епелбаум. И то за програм који може да поткопа снагу неке државе, а настао је под државним скутом – наручила га је америчка влада.

Скривање у шуми Интернета

Све је почело 1995. године када су програмери у Морнаричкој истраживачкој лабораторији у Вашингтону добили задатак да нађу начин који би омогућио да амерички војници и шпијуни безбедно користе цивилни Интернет. Да се из света јављају бази, а да нико не може да открије одакле и о коме се ради. Три године касније настала је техника коју су осмислили Мајкл Рид, Пол Сајверсон и Дејвид Голдшлаг, а патентирала Америчка морнарица (US Patent No. 6266704).

Она порекло и одредиште појединачних пакета података крије тако што их насумично усмерава помоћу три рачунара – у посебној врсти мреже. Подаци су шифровани а ови рачунари, названи чворови или рутери, уклањају по један слој заштитних шифара да би сазнали адресу следећег рутера у мрежи. Пошто су шифре поређане у слојевима око поруке, слично као љуске црног лука око његовог језгра, техника је добила чудно име – The Onion Routing, скраћено tor (енг. onion – црни лук, routing – усмеравање).

Морнарички стручњаци убрзо су увидели да ће оваква, посебна војна мрежа, лако упасти у очи. Ако „тор” буде искључиво војно средство, то другим речима значи да је свако ко га користи – војно лице. За-

„Торов” лого садржи главицу лука

кључено је да је много сигурније да се мрежа прошири на што већу групу корисника (у гушћој шуми лакше се крије зец). Онда ће бити тешко да се пакетима с подацима уђе у траг, а још теже да се следи њихов траг уназад до пошиљаоца. Тако је 2006. године одлучено да се „Тор пројекат” прогласи непрофитним и да се „тор” програм понуди јавности – да може бесплатно да се скида са Интернета и слободно користи.

Годину дана касније „Тор пројекат” запошљава Епелбаума да ради као иноватор на програму, односно да га усавршава јер се већ „истакао” успешним хакерисањем „Епловог” шифрованог програма.

ФБИ користи „тор”, али и „Викиликс”

На први поглед, чудан поступак за организацију насталу под окриљем Министарства одбране. Али, и „тор” је необичан хибрид. Већи део новца и даље му пристиже од федералних власти, а остатак добија од корисника „Гугла” и од „Хјуман рајтс воча”. Циљ војних програмера се остварио – „торова” мрежа многоструко се повећала. Тако је само током прошле године, у петој години откако је постао јаван, програм скинут 36 милиона пута са сајта „Тор пројекта”.

Овакав нагли успон програма донео је Епелбауму и неугодности – а неке су стигле и од властите владе, исте оне која га је наручила и платила. Пошто је и група активиста под именом „Викиликс” користила „тор” да би тајне документе америчке војске послала на своје сервере у Шведској – Министарство за унутрашњу безбедност САД прогласило је Епелбаума „за особу од интереса”. Средином јуна ове године он је ухапшен и испитиван о својим везама с „Викиликсом”.

„Нисам пристао да променим своје погледе, ни животни пут који сам изабрао”, написао је на „Твитеру” чим је ослобођен.

Епелбаум се недавно вратио у Египат, да из прве руке види плодове својих путовања из 2009. године.

Савршенство – с маном

„За време арапских пролећних протеста уочили смо велико повећање коришћења тора”, казао је. Скидање овог програма с мреже порасло је пет пута у данима који су претходили 27. јануару – тренутку када су египатске власти одлучиле да искључе свој Интернет.

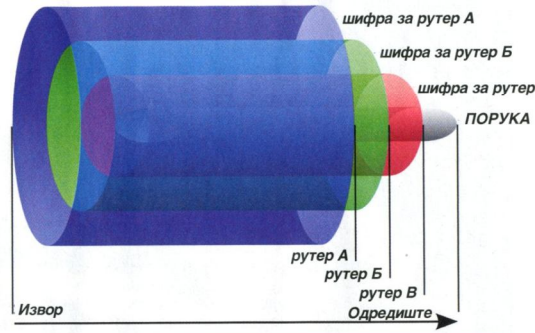
„Онјон рутирање” је техника која се састоји у обмотавању текстуалне поруке с неколико слојева заштитних шифара. Сваки слој крије адресу чвора у мрежи и мора да се дешифрује да би порука могла да се проследи следећем чвору. Тамо се поступак понавља. Тако на чворовима могу да се сазнају само две ствари: који је претходни чвор и који је следећи. На овим рутерима није могуће открити порекло, полазну адресу поруке, нити њено крајње одредиште. То могу да знају само пошиљалац, последњи посредник у мрежи, такозвани излазни рутер и прималац.

Ако су „торови” корисници добро обучени, односно упућени шта тачно треба да раде са својим рачунаром (што често није случај), путању овако шифроване поруке тешко је пресрести и одгонетнути. Али, није и сасвим немогуће, јер „тор” није савршена техника. Има неколико недостатака које вешти хакери могу да искористе. Две његове основне мане су: испадање рутера из „торове” мреже и чињеница

„ОНЈОН РУТИРАЊЕ”

Кад корисник (горе, лево), пошаље пакет с подацима (М), он путује заобилазном путањом кроз чворове – друге рачунаре у „торовој” мрежи. Док пакет путује, слојеви шифара се уклањају (3, 2, 1), а он на циљ стиже дешифрован.

да на излазном рутеру подаци више нису заштићени. Пре него што поруку проследи на крајње одредиште, овај чвор уклања последњи слој заштите и порука, пошто је насумично пропутовала кроз „торову” мрежу и друге чворове – одједном постаје читљива! А у овој добровољној врсти мреже сваки упућени учесник може да постави „торов” чвор.

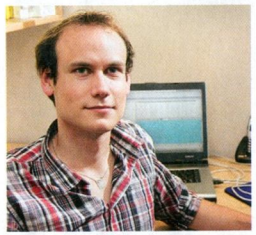


„ТОРОВА” ПОРУКА ОБМОТАНА ЈЕ С ТРИ СЛОЈА ШИФАРА

Ове слабости први је обзнанио шведски хакер Дан Егерстед 2007. године. Да ли их је и први уочио, друго је питање. Направивши излазни рутер, Егерстед је пажљивим посматрањем саобраћаја на њему сазнао лозинке и садржај преко 1000 и-мејлова. Од тога њих око 100 потицало је од службеника неких страних амбасада у Шведској (Ирана, Индије, Јапана, Русије и још неких). Припадале су и запосленима у неким великим предузећима, па и једном које има годишњи приход од око десет милијарди долара.

Лов у мутном?

У први мах Егерстед није знао шта да ради са овим подацима. Схватио је да су многи корисници „тора” у ствари у заблуди. Мисле да су њихове поруке сасвим безбедне – ако их само провукуу кроз овај програм – што није тачно. То је могло да се закључи и из упутства самог програма. Онда се запитао: А шта ако се ова заблуда намерно пређуткује да би се злоупотребила? Овакву Егерстедову сумњу поткрепило је сазнање да на мрежи постоје и врло јаки и скупи рутери – а мало је вероватно да такви припадају обичном добровољцу. Могло би да се ради о хакерима било које врсте. Уосталом, „тор” је – осим за војску, дипломате, невладине организације и противнике режима – постао савршена алатка и за хакере. Вероватно и највише. Тако је Егерстед почео да сумња да наводне жртве уопште нису користиле „тор”, већ непознати хакери да дођу до поверљивих података. У општој збрци ко кога шпијунира, одлучио је да све објави на Интернету. Испоставило се да су лозинке биле праве.



Дан Егерстед први је обзнанио „торове” слабости

Ипак, ово његово својеврсно упозорење као да је заборављено. Јер, на исти начин је и „Викиликс” дошао до поверљивих података. У ствари, поново се испоставило да је једини потпуно безбедан начин саобраћања на Интернету тај да поруке остану шифроване од почетка до краја свога пута – од првог до последњег корисника ■

Г. Војиновић