Sue Halpern

Da li su hakeri heroji

The New York Times

New York,septembar 2012.

Beograd, mart 2013.

Poslednjeg dana juna 2012. godine, tek sajt zvani *Redmond Pie* postavio je na svoju naslovnicu jedan za drugim dva nepovezana članka.

Prvi je , sa naslovom *"Root Nexus 7 na Android 4.1 Jelli Bean, Unlock Bootloader i Flash ClockvorkMod Recoveri"*,bio tutorial o tome kako da promenite softver, uglavnom s ciljem kako da se preuzme kontrola nad operativnim sistemom u Googleovom ganc novom brend tablet računaru Nexus 7, koji je bio toliko nov da još nije bio ni isporučen kupcima.

Drugi naslov običnom čitaocu je bio malo teži za razumevanje: *"Novi OS X Tibet Malvare na Apperance, Šalje lične podatake korisnika na udaljeni server."* Ta priča, koja se odnosila na otkrivanje tzv. "Trojanskog konja" računarskog virusa na pojedinim kompjuterima u Tibetu, pokazala je da Apple računari nisu više tako otporni na zlonamerne viruse i crve, kao što su to bili u prošlosti, i da ovaj napad, kojim je ciljano na tibetanske aktiviste, protivnike kineskog režima, nije bio slučajan već politički. Kada su tibetanski aktivisti preuzeli zaraženu datoteku, njihove računare virus bi povezivao sa serverom u Kini koji je pratio njihove aktivnosti i snimao sadržaj u njihovim kompjuterima. (Pisac Redmond Pie sumnjao je da su Apple računari bili meta napada iz razloga što su omiljeni brend Dalaj Lame.)

U stvari priče *Nexus 7* i *Tibetanski trojanski konj* imale su istu temu: hakerisanja i hakere, iako je hakovanje hakera Nexusa 7 – posredstvom online sajta s imenom Rootzwiki - bilo veoma različito od hakovanja koje je obavio tim koji se ugnjezdio u računare tibetanskih aktivista.

Hakovanje i hakeri postali su sveobuhvatniji pa se značenje osnovnog pojma sada skoro uvek mora izvoditi iz konteksta. Ipak, u poslednjih nekoliko godina, nakon britanskog telefonsko-hakerskog skandala, nakon Anonymousa i LulzSeca, nakon Stuxneta, u kome su Amerikanci i Izraelci

HAKERI KAO PODSTREKAČI NAPRETKA

koristili kompjuterski virus da bi probili centrifugu i odložili iranski nuklearni projekat, posle brojnih kradja identiteta, kontekst tendinra ka naglašavanju destruktivne strane hakovanja.

U februaru, kada je Facebook CEO Mark Zuckerberg u svom pismu potencijalnim akcionarima, pre nego što će preduzeće izvesti na bezansko tržište, konstatovao da je Facebook prihvatio filozofiju pod nazivom "Hakerski put ", on nije bio toliko provokativan već je više pokušavao da pomeri težište u drugom pravcu. (Zuckerberg je takođe podsetio na reči veterana tehnološkog novinarstva Steven Levz-a, čija je knjiga Hakeri: Heroji računarske revolucije objavljena 1984. godine bila prvi ozbiljan pokušaj da se razume subkultura koju su nam dali Steve Jobs, Steve Woyniak i Bill Gates.) Prema Cukerbergu:

''U stvarnosti, hakovanje samo znači nešto bržu gradnju ili testiranje granica šta može da se uradi. I kao većina stvari, može koristiti dobru ili zlu, ali ogromna većina hakera koje sam sreo u osnovi su idealisti, ljudi koji žele da imaju pozitivan uticaj na svet .... Hakeri veruju da nešto uvek može biti bolje, i da ništa nikada nije završeno. Oni bi baš da poprave to, i u prkos, za šta ljudi kažu da je to nemoguće ili da su zadovoljni sa statusom quo .''

Iako bi mogla da izgleda kao neutralna, ispostavlja se da je reč "popraviti" otvorena za interpretaciju.
Da li je novi Google Nexus 7 tablet bio provaljen i pre nego što je spakovan i isporučen?
''Ne'' - za Googl ili ogromnu većinu ljudi koji su

ga naručili, ali "da" za one koji su videli njegove specifikacije i primetili, na primer, da je imao relativno malu količinu ugrađene memorije, a želeo je da omogući prihvatanje eksternog uređaja kojim bi se omogućio veliko proširenje njegove memorije.
Slično tome, nije bilo pogreške ni sa originalnim iPhone-om, radio je odlično. Ali, za korisnike koji su se nadali učitavanju softvera, koji Apple nije odobrio ili proverio, one koji nisu želli da budu ograničeni određenom uslugom provajdera (AT & T) i one koji vole da prtljaju jer smatraju da je to njihovo pravo, jer su vlasnici, razne hakerske "provale" su bile način zaobilaženja takvih ograničenja, a prema Zuckerbergovom rečniku to bi bilo njihovo "popravljanje" problema.! [(1)]
Apple, s druge strane, to nije tako video već je u tužbi u američkom Zavodu za autorska prava tvrdio da izmena operativnog sistema iPhone-a predstavlja kršenje autorskih prava i da je zato ilegalana. U presudi 2010., Kancelarija za Copyright nije se s' tim složila, navodeći da "nije bilo zakonske osnove koja bi Apple-u omogućila restriktivnu zaštitu njegovog poslovnog modela". Ipak, zakoni o autorstvu se razlikuju od zemlje do zemlje i 2012. godine troje ljudi u Japanu uhapšeno je u skladu sa tamošnjim nedavno ažuriranim Zakonom zbog nelojalnt konkurencije i modifikovanje - tj hakovanje – Nintenda, igračke konzole. Što se tiče hakera Nexusa 7, oni ne moraju da se brinu: Softver Google-vog Androida je "otvorenog koda", što podrauzmeva da je, budući da je namenjen za javnu upotrebu, javnost slobodna i da s' njim petlja i da ga proširuje.

Vrh hvalospeva Marka Zuckerberga o hakerima i razlog zašto je iskoristio priliku da o njima govori potencijalnim akcionarima je u tome što hakerisanje može, a često to i čini, da poboljša proizvode. Ono otkriva slabosti, podstiče inovacije, pokazuje kako je i šta je moguće i šta potrošači žele. Ipak, Zuckerberg je takođe nagovestio, i to sa dobrim razlozima, da hakovanje ima i mračnu stranu, onu koja baca senku na nje-

1.Pojedine vlasničke aplikacije koje Google distribuira sa Androidom, kao što je Gmail, nisu otvorene za manipulacije.

KO SU SVE ZAPRAVO HAKERI

govu razigranu, sportsku i kreativnu stranu, posebno u narodskom tumačenju. Hakovanje je postao omiljeni alat određenih vrsta lopova, onih od kojih jedni elektronskim putem podižu novac sa bankovnih računa, dok drugi prodaju lične informacije, što se posebno se odnosi na kreditne kartice i lozinke, u međunarodnom internetskom podzemlju, koje je u procvatu. Hakerisanje je takođe postalo metod koji se koristi za ucene, javno nasilje, poslovno ometanje, krađe intelektualne svojine, špijunažu, i eventualno, ratovanje.

Dve nedavne racije koje je izveo o FBI su zajedničkja ilustracija kako hakerisanje, u suštini, izvode loši momci.

Prva operacija, *Ghost Click*, u novembru 2011. godine, rezultirala je hapšenjem šestorice državljana Estonije, koji su zarazili više od četiri miliona računara u više od sto zemalja, sa virusom koji je omogućio da se nelegalno zaradi 14 miliona dolara ubiranjem procenata od reklamiranja na internetu. Virus je prosleđen tako što je maskiran u softver potreban za gledanje online videa. Jednom instaliran, on je hakerima omogućio da neprimetno preusmere i preuzmu kontrolu web pretraživača na zaraženom računaru. Kao neželjena kolateralna šteta, nakon što je FBI ugasio hakerske servere, "desetine hiljada računara koje njihovi bezazleni vlasnici koji nisu bili dezinfikovati" više nisu mogle da pristupe Internetu.

Druga FBI žaoka desila se juna 2012. Nazvana Operacija *Card Shop*, ona je "ulovila" dvadesetčetvoro ljudi u osam zemalja, na četiri kontinenta, koji su krali i prodavali podatke kreditnih kartica. A uhvaćeni su tako što je FBI

tajno postavio i nadgledao, internet "Carding" forum, koji je radio na principu "invitation only". Korisnici su mogli da kupe ili prodaju ukradene brojeve kreditnih kartica i druge lične podatke i da se medjusobno savetuju oko krađe i korišćenja tih informacija. FBI je procenio da je njihovim hapšenjem, spasao 400.000 potencijalnih žrtava i potencijalnih 205 miliona američkih dolkra. (Ukradene podatke FBI je vratio bankama, tako da su gubici, navodno, izbegnuti.)

Profili jedanaest Amerikanaca uhapšenih u operaciji Card Shop mogu se čitati kao kod za "Crno tržište", knjigu Miše Glenija (Misha Glenny), uznemirujući portret hakerskih kriminalaca – preciznije zvanih krekeri- uključenih u ranije šeme sa karticama, slične Card Shop operaciji i centrirane oko Internet foruma na kojem se trgovalo sa ličnim podacima.

Kao i u Glenijevoj knjizi, i u operaciji Card Shop, hakeri su bili mladi - niko nije bio stariji od dvadeset pet godina i svi su bili muškarci. Na primer, Majkl Hogue, 21.-godišnjak iz Tusona u Arizoni, prodavao je "malver" koji je dopuštao da njegov korisnik, kroz razne metode, uključujući veze-zamke, e-mail, kao i programe - preuzme i daljinski kontroliše poslovanje "zarobljenog" računara. Ne samo što je njegov "crv" bio zgodna opcija za krađu lozinki i pristup bankovnim računima, nego je mogao da 'zarobi' i web kameru zaraženog računara i špijunira bezazlene žrtve.

Neka bude pomenut i 19-godišnji Kristijan Cangeopol iz Lavrenceville-a u Džordžiji. On je razvio praksu zvanu "instoring" – online kupovinu skupe elektronske opreme putem ukradenih kreditnih kartica i njeno preprodavanje u stvarnim prodavnicama, za gotovinu.
Ako se ovi mladići čine kao sitna riba u krivičnom miljeu podzemlja, to se može učiniti zbog načina na koji ih je FBI uhvatio: bacio je mrežu da vidi ko će se upecati.
Ali, kako Gleni ističe, tipičnije je da je glavni internet kriminal udruženi rad koji dela iz nedodjije, medju kojima mnogi iz bivšeg Sovjetskog Saveza.

Otprilike u isto vreme kada je FBI obznanio Operaciju Card Shop, *McAfee*, kompanija za bezbednost ralunarskih sistema i *Guardian Analitika* objavili su belu knjigu obelodanujući sofisticirane hakerske sheme čiji su cilj bili bankovni računi preduzeća i pojedinaca sa velikim iznosima.
Hakeri su uspeli da provale lozinke i bankarske informacije, koje su potom koristili za prenos tih sredstava na svoj račun. Navedena Operacija High Roller (Bogataš) počela je s krađom u Italiji, prostrujala kroz Evropu, skočila do Latinske Amerike, a odatle u SAD, poput talasanja navijača na fudbalskim stadionima.

Impresivno je i što je sve ovo bilo daljinski orkestrirano iz Rusije sa šezdeset vrlo jakih računara. Jednom postavljena zamka je radila sama. " Nije joj bilo potrebno ljudsko učešće, a svaki napad je bio munjevit i precizan " naveli su autori bele knjige. "Ova operacija kombinovala je insajderski nivo razumevanja sistema bankarskih transakcija sa običnim i vanserijskim malver kodovima i dostojna je termina >visoko organizovani criminal<". Autori procenjuju da je u kradju bilo udruženo najmanje desetak kriminalnih grupa, koje su udruživanjem izazvale gubitak od oko78 miliona dolara. Takođe, da je cela operacija uspela do kraja, gubici bi dostgli blizu 2 milijarde evra.

Dve milijarde evra ili 2,5 milijarde američkih dolara predstavljaju mnogo novca, mada ni 78 miliona nije zanemarljivio. Obnarodovanje tih suma u javnosti, McAfee-a i Guardian Analitika, i procena FBI da su kriminalci kroz Card Shop mogli pričiniti štetu od 205 miliona dolara, imalo je za cilj da javnost bude upozorena na veličinu pretnje koju predstavljaju sajber kriminalaci. Ipak, brojke dobijene od McAfee-a, Guardian analitike i FBI su spekulacije koje se zasnivaju se na šta bi bilo da je bilo, a nije.

Slično tome, kada je softverska kompanija *Norton*, proizvodjač antivirusnih programa, izdala svoj izveštaj za 2011. "O visokotehnološkom kriminalu", pregled internetskog kriminala širom sveta, u kojem je procenjeno da su potrošači izgubili oko

114 milijardi američkih dolara, štampa se na ovo primila postavivši ekvivalent: u novcu, globalni sajber kriminal sada je takmac globalnoj trgovini drogom.

Ova šokantno nova činjenica našeg življenja u eri interneta, bez sumnje je doprinela da bezbroj ljudi pojača svoje kompjuterske lozinke i preuzme antivirusne softvere. Ali tu ne može biti tačka, jer u ovoj igri učestvuju i proizvodjači antivirusnih softvera i firme za bezbednost interneta. Kako raste sajberlopovluk, tako rastu i izdaci za sajberbezbednost. Prema jednoj proceni ti izdaci od 2006. godine rasli su 10 odsto na godišnjem nivou, dosegnuvši 80 milijardi dolara u 2011. godini.

Drugo objašnjenje o visokoj ceni sajber kriminala može biti da i nije istinito. Brojke u izveštaju Nortona, na primer, proističu iz anketiranja 12,704 odrasle osobe, 4.553 deteta i 2.379 nastavnika u februaru i martu 2011. Ekstrapolacijom iz njihovih odgovora, Norton je ne samo došao do broja od 114 milijardi dolara već takođe tvrdnje da je te godine 431 milion ljudi bio žrtva internet-kriminala. Međutim, prema Dinei Florencio i Cormac Herlei, istraživačima kompanije Microsoft, da dođu do tih brojeva u Nortonu su se oslonili na onu vrstu statističkih analiza koje se koriste kod izlaznosti i glasanja, u kome se uzorak uvek pomnoži da da celinu, ali je to metod koji nije prihvatljiv jer se preferencije birača i novčani gubici ne mogu izračunavati na isti način.

"Pretpostavimo da smo pitali 5.000 ljudi da prijave svoje gubitke zbog visokotehnološkog kriminala i da onda to ekstrapoliramo na stanovništvo od 200 miliona", napisali su Florencio i Herlei za The New York Times prošlog proleća. "Svaki navedeni dolar je pomnožen sa 40.000. a svaki pojedinac koji je slagao da ima 25.000 dolara gubitaka doprineo bi nastanku jedne lažne milijarde. A pošto niko ne može da dokaže takve negativne gubitke, onda se ni greška ne može poreći.

Ipak, ako gornje procene kvare brojke, to čine i procene koje su izostale.

Dosad je već je jasno dokazano da korporacije i druge institucije nerado priznaju gubitke ili narušavanje bezbednosti iz straha da će izgubiti kupce, da može doći do pada vrednosti njihovih akcija ili da bi to moglo podstaći oštećene da ih tuže.

Iako su u poslednje četiri godine hakeri tri puta provalili u računarski sistem lanca *Wyndham* hotela, sa stotinama hiljada brojeva kreditnih kartica, kompanija je odlučila da u svom godišnjem izveštaju akcionarima ovu kradju ne prizna.

Tako je postupio i *Amazon*, koji je proustio da prijavi veliku krađu korisničkih podataka iz svojih odeljenja 'Zappos' i '6 PM' oglušavajući se o zahteve Securities and Exchange Commission, koji su tražili veću transparentnost oko takvih informacija. (Ta komisija, medjutim, ne može da učini ništa više nego da apeluje, budući da njeni zaključci nisu obavezujući jer nemaju zakonsku snagu.).

Uprkos korporativnog oklevanja, a možda i zbog toga, sudovi su uveliko angažovani.

Pošto je *''Ruski sindikat''* s proleća 2011. ukrao oko 6,5 miliona lozinki sa društvene mreže sajta *LinkedIn* jedna od žrtava je pokrenula akciju tužbi tvrdeći ne samo da LinkedIn nije pravilno čuvao lične podatke, nego i da je svima onima čiji su podaci kompromitovani namerno uskratio obaveštenje o tom napadu. Lozinke su se mogle iskoristiti za pristup privatnim informacijama o korisniku, uključujući brojeve telefona, adrese i podatke o njegovoj profesinalnoj karijeri, često i za pristup drugim nalozima na mreži, kao što su e-mail poruke ili bankovni račun, budući da mnogi ljudi koriste jednu lozinku za većinu onoga što rade na mreži.

U međuvremenu, Savezna trgovinska komisija ponovo je podnela tužbu protiv Wyndhama Worldwide, navodeći da ta

kompanija nije uspela da zaštiti svoje goste zahtevajući od američkog Okružnog suda naredbu "da Wyndham prestane sa obmanjivanjem kupaca u pogledu svojih praksi informacione bezbednsti i da mu se naredi da im nadoknadi izgubljeni novac".

Kao što je kompanijama postalo zajedničko da informacije o sajber napadima čuvaju pod velom tajne, takođe je tačno i da su sada ti napadi toliko brojni i sofisticirani da preduzeća i druge organizacije često nisu ni svesni da su njihovi sistemi kompromitovani.

Prema studiji kompanije za internet tehnologiju *Juniper Networks*, kako je navedeno u njihovoj publikaciji pod nazivom *''Homeland Security News Wire''* ", u 2011. godini 90 odsto preduzeća je pretrpelo je najmanje jedan bezbednosni proboj."

Kada je Richard Bejtlich, glavni oficir za bezbednost u američkoj kompaniji za bezbednost računara Mandiant, uradio bezbednosnu analizu klijenata, on i njegove kolege otkrili su da njih 94 odsto nije ni shvatilo da su njihove njihove kompanije napadnute - u ovom slučaju od kineskih hakera u potrazi za trgovačkim tajnama i drugim informacijama koje bi im, možda, mogle doneti prednost u poslovanju. "U mnogim slučajevima, veštine protivnika su toliko sofisticirane da mogu da preskoče zaštitni zid, bez da se njegov alarm i oglasio i da , potom, isto i odu, rekao je za Wall Street Journal Shawn Henry iz FBI.

KOJI HAKERI NOSE CRNE A KOJI BELE ŠEŠIRE

Richard Bejtlich i njegova firma su ti koji su u hakerskom svetu poznati kao "beli šeširi" ili ‘’etički hakeri’’, oni koji koriste alate hakovanja da prodru u kompjuterske sisteme svojih klijenata, pronađu rupe u njihovoj bezbednosti i zakrpe ih, u idealnom slučaju. Dobrim momcima u belim šeširima veoma je stalo da ih ne mešaju sa lošim momcima u crnim šeširima, a već postoje i studije i konsultani Međunarodnog saveta za e-poslovanje koji potvrđuju njihove etičke *bona fides*. To se možda delimično dogadja i zbog toga što su mnogi beli šeširi nekada bili crni .

Sledeći put Cavin Mitnicka, čoveka koji nekoliko godina bio najozloglašeniji haker na svetu, crni šešir, noćna mora za FBI, koji je odslužio pet godina zatvora zbog upadanja u telekom kompanije, vladine agencije (uključujući, možda i Agenciju za nacionalnu bezbjednost NSA), i akademske institucije stižemo do Mitnicka sa belim šeširom koji sada vodi svoju kompaniju za kompjutersku bezbednost firmi i koji je odlično plaćen da čini ono što je nekad činio iz zezanja ili za obećanu čašu soka od pomorandže.

Od početka Mitnickovih najnovijih memoara *‘’Duh u žici’’* zastaje dah. U stilu ‘’Nemoguće misije’’ provaluje u korporacijsku kompjutersku mrežu, koristeći lažnu kartu za identifikaciju, a ondase uspinje do administratora korporacijske mreže smeštajući se, neprimećen, u računar administratora. Ovo pumpanje adrenalina za čitaoca prilično traje. A ostaje i zebnja da su svi hakeri od istog štofa.

Jedan od razloga što je, recimo, teško razlikovati hakera Anonymusa od hakera iz kineske vojske, i njih dvojicu od devetnaestogodišnjaka u Gruziji,je što hakeri tako hoće. Željni uspeha pod devizom "ne ostavljaj trag" oni rade iza proxy servera - posredničkih računara između hakera i njihovih meta - skrivajući jedinstvene identifikatore svojih računara, pa je skoro nemoguće tačno odrediti mesto u svetu gde su. Oni se opredeljuju da budu i onlajn ličnosti koje su, po pravilu, češće izišljene nego stvarne i koriste pseudonime koji u smišljeni da zavaravaju.. (Jedan od aktivnijih članova hakerske grupe Anonymous koji je sebe nazivao Kayla i tvrdio da je američka tinejdžerka, zapravo je bio britanski momak u dvadesetim godinama, s četiri godine vojne službe.) Kako to ističe Parmi Olson u njenoj izuzetnoj, mračnoj i zabavnoj priči "Mi smo Anonymus", "pojedinačne ličnosti se mogu pojavljivati, ali ljudi i dalje nemaju stvarne identitete".

U svom istraživanju, Miša Gleni utvrdio je da je "nemoguće u potpunosti ustanoviti šta se zaista dešava između igrača, kao i sa kim su naposletku povezani." Ovo nije samo problem za one izvan, autsajdere poput njega. Prema Olsonovoj čak i "javni" "Anonymusi nemaju pojma s' kim su saradjivali. Poverenje je nepouzdano i prolazno. Kad je haker koji se pojavio kao Sabu počeo da deli lične podatke, otkrivajući svoje stvarno ime i rodni grad, njegov kolega u Anonymus grupi, s imenom Topiari, prestao je da mu veruje. Bila je to obrnuta logika, ali se ispostavilo da je bila logična . Kada je FBI objavio da je u martu 2012. Sabu uhvaćen, takođe je otkrio da je prethodnih osam meseci Sabu bio i doušnik FBI "prodajući" svoju ekipu.

Parmi Olson kazuje nam priču da je Sabu, čije je pravo ime bilo Hector Monsegur, a prava adresa na šestom spratu u stanu stambene zgrade Jacob Riis na donjem njujorškom Ist Sajdu, svoju novu dvostruku ulogu prigrlio u tolikoj meri da se i policijskom službeniku predstavio kao kao federalni agent, što mu je na kraju donelo dužu zatvorsku kaznu.

Dok je FBI punio sa informacijama, Monsegur je nastavio da opšti i sa drugim "javnima" plotujući tako mapu koja je federalninim agentima omogućila da prikupljaju dokaze koji su na kraju umešali i njihove "prijatelje". Pod budnim okom FBI, Anonymusu je dozvoljeno da slobodno hakeriše, kako navodi Olsonova, i notorno napada i "globalne obaveštajce", kompaniju za strateško prognoziranje - *Stratfor* - obaveštajnu službu smeštenu u Austin-u koja zaradjuje novac prodajom biltena klijentima , medju kojima je i Odeljenje za unutrašnju bezbednost (SAD). FBI je posmatrao kako su im hakeri Anonymusa skrajnuli 60.000 kreditnih kartica s lozinkama, koje su potom koristili "donirajući" Crveni krst, Save the Children i druge dobrotvorne organizacije sa skoro million dolara. Takodje, preko pet miliona Stratforovih e-mailova "donirali"su WikiLeaksu.Između ostalog, e-mailovi s' izjavama Stratforovih zaposlenika otkrili su i da vlada špijunira američke građane i korporacije koje su špijunirale predstavnike sindikata i druge aktiviste. Oni su takođe najavili da Sjedinjene države pripremaju tajnu optužnicu protiv osnivača WikiLeaksa Juliana Assange-a. Stoga se može postaviti i pitanje: Kakve su boje bili šeširi koje su nosili ovi hakeri, beli ili crni?

Različite akcije Anonymusa i njegovih ogranaka uključuju obaranje (dva puta) SONY website-a (jednom da se osveti zbog Sony-eve tužbe protiv mladog hakera koji je "odblokirao" svoju konzolu PlayStation, a drugi put zbog podrške akciji Stop Online Piracy pred Kongresom SAD)[2], kratko obaranje web poslovanja *MasterCard*-a i *PayPal*-a, nakon što su te kompanije blokirale donacije za WikiLeaks i Julian-a Assange-a[3] i obaranje site-a Sajentološke crkve u naporu da se ona "protera sa interneta".

2. Treba istaći da je mladi haker Geroge Hotz, pod čijim imenom se taj napad dogodio, to porekao. U intervjuu za New Yorker, reporteru Davidu Kushneru (7. maja 2012) on je rekao: "Ja sam potpunoa suprotnost Anonymousu. Ja sam George Hotz. Sve što radim je javno i legalno. 3. Grupa koja je tvitovala: "Sloboda izražavanja je neprocenjiva. Za sve ostalo tu je MasterCard ", parafrazirala je oglasnu kampanju MasterCarda.

Ako u ovim akcijama postoji rukovodeći princip onda on glasi da "informacije zaslužuju da budu slobodne." Pritom se ne radi toliko o slobodi informisanja već principu koji uključuje i slobodu same informacije u odnosu na njene autore i organizaciju koja ih kontrolišu.

Pripsivati koherentnu političku filozofiju gomili pojedinaca koji uporno odbijaju koherentnost saveza i organizaciju koja ne postoji, u koju se ne može stupiti i koja nema članstvo, ne samo da bi bilo besmisleno, već bi dovelo do previda aktuelnog nihilizma koji struji Anonymusom u kome se, bar u početku, primarna svrhovitost svodila na "lulz"- to jest, zabavu i igu, kao i ismevanje, bez obzira o čijem trošku. (Tu je i rodno mesto, u imenu LulzSec, jednog od glavnih izdanaka Anonymusa, za jedan od glavnih internetskih akronima LOL, Laugh Out Loud.)

Zašto jedni druge nazivaju "pederčinama" i "crnčugama"? Zašto navedu ljude na seksualni čin i performans ispred kamera, a onda posredstvom Facebooka prete da će informacije o njima ili njihovom pronađenom pravom identitetu obnarodovati ili poslati i pretiti i ćlanovima njihove porodice'? Zašto - zato jer misle da je to zabavno - šokirati i poniziti.

Ipak, baš neki od ljudi koji su radili takve stvari "oslobodili" su i e-mailove Stratfor-a, baš kao što su hakovali i finansijske transakcije vlade po osnovu njenog ugovora sa firmom HBGary i još nekim kompanijama, preko Bank of America, a objavili ih zajedno sa planovima kako da se napadne i diskredituje WikiLeaks.(Prema onlajn izveštaju Forbsa, predlagani su "korišćenje falsifikovanih dokumenata, pritisak na donatore, pa čak i ucenjivanje onih koji navijaju za WikiLeaks.").

Pripadnik Anonymusa takođe je napravio program koji je Tunižanima omogućio da pristupe internetskoj mreži bez da na njih može da utiče vlada, sa malim bit kodom za skrivanje

KO SU,

ČIME SE RUKOVODE,

ŠTA HOĆE

pošiljalaca i primalaca e-mailova, koji je katalizovao Arapsko proleće.

Otprilike u isto vreme, a što je takođe bilo u lulz maniru, Anonymus je ukrao lične podatke nevinih ljudi koji su se nadali audiciji Fox televizije za Šou X Factor i preuzeo kontrolu sajta PBS-a (Javnog RTV sistema) jer im se nije dopao dokumentarni film o Assangeu. (Toliko o zalaganju za slobodan protok informacija.) U tom napadu, hakeri su takođe na zvanični sajt vesti PBSa ubacili izmišljenu vest o smrti rep zvezde Tupak Šakura koji je zapravo bio živ i živi na Novom Zelandu i promenili naslovnu stranu kompanije ubacujući crtani lik debelog čoveka koji jede ogroman hamburger s natpisom "LOL, HI, ja jedem decu."

Ako ovo izgleda neozbiljno i detinjasto to je možda zato što se ispostavilo kako su mnogi od članova Anonymusa ne mnogo stariji od same dece. Jake Davise je kada su ga hapsili bio osamneaestgodišnjak, T-flow, koji je napisao program za Tunižane, bio je šesnaestogodišnjak. Sa dvadeset osam, Hector Monsegur bio je skoro doajen. Kada je njegovo učešće razotkriveno, u novinama su ga žurno porglasili za lidera grupe, što je bila tvrdnja verovatno toliko istinita koliko je mogla biti i lažna.

Iako Anonymus namerno radi bez strukture ili hijerarhije i tvrdi da se rukovodi diktatom iz košnice saborne inteligencije pojedinaca, treba napomenuti da prave košnice - one iz kojih se dobija med- zapravo zuje pod rukovodstvom jednog prosvećenog monarha, matice. Liderstvo u Anonymusu je više fluidno, gde jedan (ili

više) Javnih, sugeriše neku akciju i da li da se drugi uključe ili ne, mada se kod uključenja Monsegura , pre činilo da je on za druge blokada u političkom pravcu.

Prednost što nema ni lidera, ni formalne strukture, ni planske agende, kada FBI i druge agencije za sprovođenje zakona širom sveta uhapse Monsegura i dvadeset četiri Javna i skinu ih sa mreže, postaje vidljiva tako što sa njima ne nestaje i Anonymus. Umesto toga, Anonymus nastavlja da funkcioniše, ponekad pod svojim imenom, a ponekad, izmedju ostalih, pod imenima LulzSecReborn, MalSec i SpekSec.Imena su zamenljiva, baš kao što je zamenljiv i Anonymous: svako ma gde bio može slobodno da radi iza njegove maske. Kako je neimenovani član LulzSecReborn navodno izjavio u intervjuu neimenovaom intervjueru koji je objavljen na rumunskom sajtu Softpedia, LulzSecReborn "nastavlja tamo gde stari LulzSec stao, da hakuje vojne i sajtove vlada oslobodjajući za javnost njihove datoteke, baze podataka, pune osetljivih informacija. Oni i njihovi sadrugovi u stanju su da očuvanju obećanje: "Mi smo Anonymous. Mi smo Legija. Mi ne zaboravljamo. Mi ne opraštamo. Očekujte nas. "

Čitanje o Anonymusu, LulzSec-u, AntiSec.u, MalSec-u, DarkMarket-u, operaciji Card Shop, operaciji High Roller, kineskim hakerima koji su nedavno provalilil u bazu podataka indijske mornarice, islamskom Javnom koji je nedavno ukrao i objavio podatke iz ličnih karti izraelskih građana, indijskim hakerima koji su (takođe nedavno) oštetili dva zvanična site-a pakistanske vlade u znak sećanja na smrt svojih sunarodnika stradilih 2011. u Mumbajiu u bombaškim napadima, novom izdanju WikiLeaksa, upadu Anonymusa u Stratfor, miliona dokumenata iz Sirije, itd., podseća na *Stuxnet* virus. Stuxnetovu genezu - od tajne ideje do tajne zajedničke tvorevine izraelskih i američkih programera, programa smešetnog medju vrhunske tajne podatke u iranskoj nuklearnoj elektrani i potom izazivanja javnog bekstva svih podataka po računarima širom sveta je upravo razotkrito Dejvid Sanger, kako u svom izveštavanju za The New York

Times tako i u svojoj majstorskoj novoj knjizi "Napadni i sakrij se".

Stuxnet je oružje u neobjavljenom ratu koji se vodi krišom, toliko tajnovito da prema Sangeru, naciljane mete dugo nemaju pojma šta, i ako ih je, udarilo. Sada kada vise nije tajna, i kada su njegova arhitektura i kodiranje dostupni da ih vide svi, Stuxnet je potencijal da se hakeriše,mutira, na novi nivo. Ako je u svojim ranim oblicima hakovanje bilo petljajnje sa hardverom i sa softverom koji kontroliše hardver - današnje hakovanje koje se odvija, u suštini, u zatvorenom univerzumu, kada se preselilo na internet, postalo je artefakt naših života, ili, barem, dela naših života koji se dešavaju na mreži - našeg rada, naše private prepiske, našeg plaćanja i kupovanja, i još mnogo čega. Ma koliki mogao biti stvrni broj ljudi pogođenih kompjuterskim kriminalom, svi smo ranjivi, bez obzira koliko specijalnih karaktera i brojeva i besmislenih fraza dodali u naše lozinke.

Ali nismo u opasnosti samo kao pojedinci. 2011. godine izvršeno je oko dve stotine pokušaja ili uspešnih napada na osnovne društvene infrastrukture, uključujući i postrojenja za preradu vode, električne mreže, naftovode i gasovode, rafinerije, elektraname, kao i transportne sisteme.No, sve ovo bledi u svetlu eksponencijalno razorne moći Stuxneta i drugih virusa koje generiše i inspiriše.[4] Kao što je nemački ekspert za bezbednost Ralf Langner, koji je prvi provalio Stuxnet-ov kod, napisao za The Nev York Times, realna je pretnja Stuxneta da će se pretvoriti u jeftino oružje dostupno organizovanom kriminalu, rigidnim nacošima, teroristima, hakerskoj deci, dangubama sa neograničenim vremenom i svakome ko želi da se "popravi" svet.

"Bilo koja elektrana u SAD, uključujući i nuklearnu, mnogo je lakša meta za sajber napad nego veoma čuvani objekti u Ira-

4 Moskovska sigurnosna kompanija Kaspersky Lab identifikovala je tri druga virusa razmešteni na Bliskom istoku, za koja veruje su " državno sponzorisani".

nu", napisao je Langner. "Napadač, koji ne mora biti zainteresovan za dugoročnu kampanju i angažovanje sofisticiranog prerušavanjana (a koje takvo nije) treba da uloži samo mali delić napora u odnosu na Stuxnet".

Uprkos tom saznanju, i uprkos upozorenjima generala Aleksandra Keitha, glavnokomandujućeg US Cyber Commande, da je "samo pitanje vremena", pre nego što će neki sajbernapad prouzrokovati veću fizičku štetu životnim sistemima, američki Senat, u avgustu 2012., pod pritiskom Američke privredne komore i drugih poslovnih interesa, stopirao je sredsta namenjena za sajber bezbednost predvidjena za podršku u odbrani infrastrukture (kojom upravljaju korporacije koji nisu želele ni da prijave napade, ni da plaćaju za poboljšanja, ili da bilo koji deo deo svoje autonomije prenesu na vladu).

Tako nastavljamo hakerskim putem, pa šta bude – biće!

Kratak pogovor

Prvi broj časopisa naše edicije Vidici i putokazi koju smo 2010, godine pokrenuli u saradnji sa ženevskim Demokratskim centrom za kontrolu oružanih snaga (DCAF) bavio se izazovima sajber bezbednosti i problemima mogu li odgovori na te izazove biti u okvirima demokratske kontrole i transparentnosti.

Nastavljajući ovu ediciju s proleća 2013. godine u ovom izdanju pokazuje se da su tadašnja strahovanja bila više nego opravdana.

Tekst dr Sue Halpern, koji nam je za objavljivanje ljubazo ustupio The New York Times, nije samo intrigantno naslovljen i atraktivno napisan, on pre svega pokazuje da sve, manje vise, ide u neželjenim pravcima; i kada je reč o izazovima sajber bezbednosti, ali, nažalost, isto tako i kada su u pitanju odgovori na njih.

Milan Jovanović
direktor FBD

FORUM ZA BEZBEDNOST I DEMOKRATIJU
EDICIJA VIDICI I PUTOKAZI, BROJ 3
mart 2013.

Naslov originala
Sue Halpern, Are Hackers Heroes
The New York Times, 27th September 2012.