Kultura Bezpieczeństwa
Nauka – Praktyka – Refleksje
Nr 30, 2018 (210–244)
ISSN 2299-4033 DOI: 10.5604/01.3001.0012.5890

HNUTIE ANONYMOUS A INFORMAČNÁ BEZPEČNOSŤ

ANNONYMOUS AND INFORMATION SECURITY

Peter ROZEMBERG
Ministerstwo Obrony Republiki Słowackiej

ABSTRACT:

Anonymous could call movement, activists, community or idea. They have no leader, no structure, yet have in the past influenced the decisions of thousands of people around the world. Media is often referred to as hackers, because the greatest attention they raise is their attacks, which are mainly fighting for freedom of the Internet or against various social phenomena. In addition to hackers, the movement itself creates, in addition to hackers, people who either share ideas of movement or use various programs to attack and shut down the servers of organizations, institutions, governments, or websites of various security agencies such as the FBI or the CIA.

KEY WORDS:

Anonymous, information securiy, cyberspace, ethics

ABSTRAKT:

Anonymous by sme mohli označiť za hnutie, aktivistov, spoločenstvo či myšlienku. Nemajú žiadneho vodcu, žiadnu štruktúru no aj napriek

tomu v nedávnej minulosti ovplyvnili rozhodnutia tisícov ľudí po celom svete. Média ich často označujú aj za hackerov, pretože najväčšiu pozornosť vzbudzujú práve svojimi útokmi, ktorými bojujú predovšetkým za slobodu internetu alebo proti rôznym spoločenským javom. Hnutie samo o sebe tvoria okrem hackerov aj ľudia, ktorí buď zdieľajú myšlienky hnutia alebo pomocou rôznych programov atakujú a vypínajú servery organizácií, inštitúcií, vlád či webstránky rôznych bezpečnostných zložiek ako FBI či CIA.

KĽÚČOVÉ SLOVÁ:

Anonymous, informačná bezpečnosť, kyberpriestor, etika

Do širšieho povedomia internetovej komunity sa Anonymous dostali v roku 2003 prostredníctvom internetového obrázkového fóra 4chan.org. Na ňom používatelia anonymne publikovali (publikujú) príspevky či obrázky pod označením Anonymous, čo priamo viedlo k vzniku názvu a samotnej skupiny, ktorá sa postupne rozšírila mimo toto fórum.Anonymous si neskôr vyslúžili pozornosť médií vďaka reportáži televízie Fox v roku 2007, ktorá ich označila ako „hackerov na steroidoch" či „domácich teroristov". Reportáž sa týkala viacnásobného útoku na účet používateľa služby MySpace, ktorému mal člen Anonymous na profil popridávať obrázky z gay porna. Prvou ostro sledovanou akciou Anonymous sa stal projekt Chanológia z roku 2008, v ktorom členovia skupiny protestovali proti praktikám scientologickej cirkvi. Neskôr, v roku 2009 po sporných iránskych prezidentských voľbách a následných masových demonštráciách, sa hnutie Anonymous spoločne s portálom The Pirate Bay zapojilo do boja proti internetovej cenzúre v Iráne. Logo The Pirate Bay sa vtedy zmenilo na The Persian Bay (Perzská zátoka) a pribudol nápis „Klikni sem pre pomoc Iránu". Po kliknutí na tento odkaz sa používateľ dostal na stránku iran.whyweprotest.net, na ktorej sa nachádzal návod, ako sa na internete pohybovať anonymne.

Anonymous sa ozvali aj na konci roka 2010, kedy reagovali na cenzúru serveru Wikileaks a stíhanie jeho zakladateľa Juliana Assangeho. Vtedy napadli a na nejaký čas odstavili internetové stránky spoločností Visa a MasterCard, ktoré prestali podporovať platby pre Wikileaks. Terčom útoku sa stal aj web švédskej vlády, ktorá na Assangeho vydala zatykač za podozrenie zo sexuálnych zločinov. Samotní predstavitelia Wikileaks sa ale

od Anonymous dištancovali. Americký Federálny úrad pre vyšetrovanie (FBI) vtedy zatkol 16 osôb podozrivých z hackerských útokov, ktorí mali byť členmi Anonymous. Hnutie sa hlásilo aj k útokom na webstránky vlád Egypta či Tuniska v roku 2011, ktoré sa násilím bránili proti protestom nespokojných obyvateľov počas takzvanej Arabskej jari. A naposledy vyhlásilo hnutie vojnu militantom z džihádistickej skupiny Islamský štát.

Ako teda v skutočnosti funguje toto hnutie? Čo je jeho skutočným cieľom? A čo, alebo kto im dáva právo nabúravať sa do súkromných elektronických účtov a e-mailov tisícok až miliónov osôb a organizácií a kradnúť im odtiaľ ich dôverné údaje? Je to morálne aj napriek tomu, že Anonymous vyhlasujú, že to robia v mene všeobecného záujmu ľudstva. A dáva im pocit anonymity pri páchaní trestných činov falošný pocit moci a beztrestnosti? Na tieto a ďalšie otázky sa pokúsi v krátkosti zodpovedať tento článok.

ZÁKLADNÁ TERMINOLÓGIA[1]

Aby sme mohli lepšie pochopiť činnosť hnutia Anonymous, musíme sa zoznámiť so základnou terminológiou, ktorú členovia tohto hnutia používajú pri komunikácii medzi sebou.

Anonymous: Označenie odkazujúce na skupinu ľudí, ktorí budia rozruch na internete a vyvádzajú rôzne kúsky na protest proti tomu či onomu. Názov, ktorý v preklade jednoducho znamená „anonymní", sa odvíja od vynútenej anonymity užívateľov obrázkového fóra 4chan a v posledných siedmych rokoch začal by spájaný s významnými počítačovými útokmi na rôzne spoločnosti a vládne agentúry. Skupina nemá jasne vymedzenú hierarchiu ani pravidlá členstva a existuje len ako premenlivé zoskupenie ľudí, ktorí vyznávajú nejasnú sadu zásad odvodenú od 47 pravidiel internetu. V realite zoskupenie dostáva rôzne podoby, podľa toho, kto sa práve k názvu prihlási – príkladom môžu byť organizátori operácie Chanológia z roku 2008, alebo hackeri zo skupiny LulzSec.

Antisec (Anti Security): Internetové hnutie *black hat* hackerov, ktorí na prelome tisícročia protestovali proti tomu, aby firmy z odboru počítačovej bezpečnosti verejne publikovali zoznamy odhalených bezpečnostných slabín. Hnutie v roku 2011 znovu oživila skupina LulzSec so zahmleným cieľom napádať vládne agentúry či dôležité organizácie a odhaľovať ich, často domnelú, korupciu.

---

[1] P. Olsonová, *Jsme Anonymous. Uvnitř hackerského světa Anonymous, LulzSec a globálne internetové vzbury*, Vydavateľstvo Práh 2012, s. 489–494.

4chan: Obľúbené obrázkové fórum, ktoré každý mesiac navštívi 22 miliónov unikátnych užívateľov. Pôvodne bol 4chan zamýšľaný ako diskusný portál o japonskom anime, ale postupom času toto zameranie stratil a stal sa miestom pre diskusie všetkého typu. Mimo iné sa tu organizujú internetové žartíky alebo raidy (nájazdy) proti iným osobám či webovým stránkam. Kľúčovým rysom je vynucovaná anonymita používateľov, ktorí tak môžu prispievať bez zábran a strachu zo zodpovednosti.

/b/ : Najpopulárnejšia sekcia obrázkového fóra 4chan, ktorú navštevuje asi tretina všetkých užívateľov. Keď Christoper „mooť" Poole zakladal stránky 4chan, sekciu /b/ vyhradil diskusiám na náhodné, nezaradené témy. Na tejto nepopísanej doske internetu sa potom zrodila drvivá väčšina internetových memov, medzi nimi napríklad *lolcats*, humorné obrázky mačiek. Obecne sa má za to, že práve tu sa vyvinulo „kolektívne vedomie" Anonymous, a mnohí priaznivci tohto hnutia tvrdia, že po prvý krát sa o Anonymous dozvedeli práve cez /b/. Sekcia je preslávená úplnou absenciou moderátorov.

Botnet: Sieť tzv. „zombie" počítačov, ktoré boli infikované vírom alebo podvodným softwarom a pomocou nich potom prepojené. Botnety spravidla ovláda jeden človek, ktorý potom dokáže tisícom, niekedy aj miliónom počítačov naraz zaveliť, aby hromadne vykonávali internetové príkazy.

DDoS (distribuované odmietnutie služby): Útok na webovú stránku alebo sieťový zdroj, pri ktorom veľké zoskupenie počítačov vyradí stránku z prevádzky tým, že ju preťaží zbytočnými žiadosťami. Útok môže byť prevedený buď skupinou dobrovoľníkov, z ktorých každý má vlastný počítač (pozri heslo LOIC), alebo sieťou počítačov, ktoré boli infikované a zoskupené do botnetu.

Dox: „Doxovať" znamená zisťovať niečie osobné údaje, ako sú napríklad skutočné meno a priezvisko, telefónne číslo alebo adresu domov, a to obvykle pomocou sociálneho inžinierstva alebo vyhľadávaním na Googli. Získané informácie potom predstavujú „dox" danej osoby. Doxovanie sa medzi Anonymous a v iných hackerských komunitách často používa ako vyhrážka, nakoľko ľudia sa tu skrývajú za prezývkami a takmer nikdy neprezrádzajú svoje skutočné identity.

Hacker: Termín s nejasnou definíciou, ktorý sa v kontexte Anonymous používa k označeniu ľudí, ktorí sa vďaka technickým znalostiam dokážu nabúravať do počítačových sietí. V širšom slova zmysle môžu označovať tiež počítačových nadšencov alebo programátorov, ktorí sa

radi šťúrajú v interných systémoch a vymýšľajú rôzne zlepšováky alebo nové systémy.

IRC (Internet Relay Chat): Pravdepodobne najrozšírenejší spôsob komunikácie medzi priaznivcami Anonymous, existujúci už od konca 80. rokov minulého storočia. IRC chaty, na rozdiel od obrázkových fór, umožňujú užívateľom komunikovať pomocou textových správ v reálnom čase. Diskusie sa odohrávajú v chatovacích miestnostiach, alebo „kanáloch". Každá IRC sieť združuje komunity so spoločnými záujmami, napríklad na IRC sieti AnonOps sa schádzajú ľudia, zaujímajúci sa o Anonymous. Diskusie v chatovacích miestnostiach moderujú „operátori" jednotlivých sietí a kanálov, pričom úloha operátora býva chápaná ako užívateľ vyššieho postavenia.

LOIC (nízkoorbitálny iontový kanón): Open source aplikácia pôvodne vytvorená k záťažovému testovaniu serverov. Medzi priaznivcami Anonymous sa ale preslávila ako elektronická zbraň, ktorú je možné použiť k prevádzaniu DDoS útokov – avšak za predpokladu, že ju bude používať dosť ľudí naraz.

Raid: V doslovnom preklade „nájazď". Raid je slovo, ktorým sa v komunite Anonymous a na 4chane označujú koordinované útoky, spravidla organizované verejne v diskusnej sekcii /b/. V raidoch obvykle nejde o nič iného ako užiť si trochu zábavy na cudzí účet a raid pritom nemusí byť nutne hackerský útok – často ide len o žarty typu premaľovania fotografií alebo spamovanie konkurenčných fór obrázkami.

Sociálne inžinierstvo: Klamanie či komunikácia pod falošnou identitou alebo nepravdivou zámienkou s cieľom vytiahnuť z obete informácie.

Troll: Človek, ktorý na internete anonymne zosmiešňuje alebo obťažuje inú osobu alebo skupinu, veľmi často zanechávaním provokatívnych komentárov na internetových fórach, vzácnejšie potom nabúravaním sa do účtov na sociálnych sieťach. „Trollovanie" ale môže znamenať aj zosnovávanie úmyselných klamstiev. Tak či onak je konečným cieľom rozhnevať alebo zosmiešniť. Pre úplný slovníček základných pojmov pozri Prílohu č. 1 tohto článku.

CIEĽ ANONYMOUS

O čo vlastne členom Anonymous ide? Nakoľko vo väčšine prípadov na chatovacích fórach surfujú znudení mladí ľudia, ich cieľom je podľa au-

torky knihy o tomto hnutí Parmy Olsonovej najmä užiť si zábavu, hlasno sa rehotať a baviť sa na cudzí účet. Ako Oslonová uvádza:

> termín lol – „laugh out loud" alebo hlasito sa rehotať – sa už roky pripisuje za ľahkovážne frázy typu „Prečo byť skromný, lol." Novším prírastkom do internetového žargónu bol termín „lulz", ktorý pôvodnú myšlienku ďalej rozvíjal a v podstate znamenal baviť sa na cudzí účet. Žartovný telefonát do FBI je lol. Žartovný telefonát do FBI, v ktorého dôsledku by do domu Aarona Barra (jedna z obetí Anonymous, o ktorom píšeme nižšie – poznámka autora) prišla jednotka rýchleho nasadenie SWAT je lulz[2].

Ďalšou vecou, ktorá priťahovala (a stále priťahuje) ľudí na anonymné internetové fóra bola skutočnosť, že prostredníctvom vyhrážok skutočným osobám kdekoľvek na svete, ktorým predstavitelia hnutia Anonymous doxli (nabúrali) ich e-maily a ukradli ich obsah, ich dokázali ovládať a prinútiť ich k činom, ktoré by inak nevykonali. Napríklad primäť človeka na opačnom konci sveta urobiť niečo, čo by ho inak ani vo sne nenapadlo. Povedzme napríklad, donútiť ho vyzliecť sa a urobiť fotku samého seba a následne ju odoslať úplne cudziemu človeku. Skrátka skupina Anonymous ponúkala jedinečný zážitok z moci a nepredvídateľnosť. A táto skutočnosť ľudí k Anonymous pritiahla a už ich nepustila.

Aj keď sme v úvode článku uviedli, že Anonymous nemajú pevnú štruktúru, existovali (existujú) v rámci tohto hnutia aj vodcovské typy, ktoré udávali (udávajú) smer ostatným jej členom a prichádzajú s nápadmi na koho uskutočniť raid (nájazd). Kto však boli tieto vodcovské typy a aké povahové vlastnosti ich predurčili k tomu, že si ich ostatní členovia hnutia vybrali za svojich vodcov?

Podľa Olsonovej boli asi traja až piati. Jednou z ústredných postáv Anonymous od roku 2008 do roku 2011 bol aj mladík s prezývkou Topiary. Jeho civilné meno bolo, ako sa neskôr ukázalo, Jake Davis a pochádzal z Veľkej Británie. Keď mal šesť rokov odsťahoval sa s matkou na Shetlandské ostrovy, ležiace severne od Škótska. Ako uvádza Olsonová:

> V škole ale Jakea šikanovali spolužiaci. Bol síce neuveriteľne chytrý, ale zároveň trpel amblyopiou (tupozrakosťou) ľavého oka. Vychádzať s inými deťmi bola drina, a tak zanedlho dospel k záveru, že jednoduchšie bude sa o kamarátov ani nepokúšať. Bol zamĺkly a od spolužiakov si udržoval odstup. Keď sa mu niekto posmieval, zotrel ho na oplátku britkou poznámkou, a pokiaľ sa tomu ostatní začali smiať, pridal sa k zábave. Výsledná absencia kama-

[2] Ibidem, s. 21.

> rátov ho po väčšinou netrápila… Škola a predpísaná výučba mu pripadala stále zbytočnejšia a zbytočnejšia. Keď prestúpil na druhý stupeň, začal sa búriť, otvorene spochybňoval tvrdenia učiteľov a snažil sa len na hodinách, kde ho učiteľ obvinil, že nedokáže látku zvládnuť… Vo februári 2004 keď Jakeovi bolo trinásť rokov, sa prihodilo nešťastie. Jeho nevlastný otec Allie mal na jednej z úzkych uličiek ostrova autonehodu a zomrel. Aby sa to ešte viac skomplikovalo, rodine bolo navyše povedané, že nesmú viac žiť v doterajšom dome. Dom totiž pripadol jeho bývalej manželke, ktorá pani Jennifer Davisovú a jej dvoch synov vyzvala, aby sa vysťahovali. Nakoniec sa im podarilo zohnať štátom podporované bývanie. Jakem tento zážitok natoľko otriasol, že sa rozhodol, nevrátiť sa do školy… V tom čase už doma mali vytáčané pripojenie k internetu… Získať si kamarátov na internete pritom bolo tak ľahké. Jeho amblyopia nebola vidieť a ľudia si omnoho viac vážili jeho inteligencie a kreativity. Jake si upevnil sebavedomie a vytríbil si zmysel pre humor[3].

Zatiaľ čo Topiary (ktorého prezývka v angličtine znamená umelecké tvarovanie stromov) už na 4chane zabával a rozosmieval /b/tardov, internetová entita známa pod prezývkou Kayla sa práve učila, ako vŕtať diery do kyberpriestoru. Ako pokračuje Olsonová: „Jej cesta do sveta Anonymous začala – aspoň podľa jej rozprávania – osamelosťou, pokračovala objavom hackerov na internete a vyvrcholila účasťou na vzostupe hacktivizmu"[4]. Podľa Olsonovej však Kayla mala jednu charakteristickú vlastnosť, s ktorou sa čoskoro hocikto zoznámil. Klamala. Inak to bola schopná hackerka, ktorá o sebe tvrdila, že je šestnásťročné dievča a že jej rodičia sa rozviedli, keď jej bolo jedenásť. V jej podaní bol otec tým spoľahlivejším rodičom, preto dostal dcéru do svojej starostlivosti a následne sa s ňou odsťahoval do odľahlého mestečka, kde nežilo veľa iných detí jej veku. Nakoľko nemala nič iného na práci, začala si so svojimi niekdajšími kamarátmi chatovať cez MSN Messenger. Jej otec bol údajne informatik a pracoval z domu, takže v celom dome sa váľali knihy o programovaní linuxového kernelu, Intelu či práci so sieťou. Kayla si ich prečítala a otca sa vypytovala na jeho prácu. Toho jej záujem nadchol a tak s dcérou sedával pri počítači a učil ju, ako nachádzať chyby v zdrojovom kóde C, ako ich využívať a ako ich obísť. Čoskoro sa tak Kayla vŕtala v skriptovacích jazykoch ako sú Perl, Python, alebo PHP a učila sa napádať webové databázy pomocou metódy SQL injekcie. Bolo to však viac menej neškodné počínanie, avšak v štrnástich už vraj písala skriptá pre automatizáciu počítačových útokov. Ako

[3] Ibidem, s. 54–56.

[4] Ibidem, s. 62.

sama uviedla: „Neškodné to bolo do chvíle, než som si skúsila nájsť tzv. hackerské fóra. Na jednom z nich som sa zaregistrovala a oni mi povedali: Bež preč dievčatko, toto nie je pre teba. Jasné, že mi bolo iba štrnásť, ale toto ma fakt naštvalo!"[5]. O niečo neskôr sa však na základe svojich znalostí údajne pomocou SQL injekcie nabúrala do jedného fóra a zmazala väčšinu jeho obsahu. Bol to útok, aký nikto z návštevníkov ešte nevidel. Jeden hacker údajne uviedol: „tebe je štrnásť a už vieš toto?"[6] A pozval ju do niekoľkých súkromných kanálov na EFnete, jednej z najstarších IRC sietí vôbec. Videl v Kayle potenciál, dával jej cenné rady a povzbudzoval ju, aby si prečítala ďalšie knihy o programovaní, s ktorých sa toho naučí viac. Navyše jej meno jasne ukazovalo na to, že je dievča a tak budila v hackerskej (výrazne mužskej) komunite pozornosť. A preto ako aj väčšiu šancu dostať sa k nejakej hackerskej akcii. Ženy boli v hackerskej komunite a na obrázkových fórach vzácnosťou –odtiaľ ostatne poučka, že na internete nie sú žiadne dievčatá a preto bolo vydávanie sa za dievča oddávna obľúbenou taktikou internetových trollov. Ako sa však neskôr ukázalo, jej pohlavie bolo v skutočnosti mužské.

Tretím do partie bol človek s prezývkou Sabu. Bol asertívny, úsečný a na internetových fórach používal mnoho slangových slov typu „yo" alebo „brácho". Ako dopĺňa Olsonová:

> Nikto z ostatných to nevedel, ale Sabu sa narodil a vyrástol v New Yorku a jeho predkovia pochádzali z Portorika. Počítače sa naučil hackovať už ako pubertiak, keď sa povŕtal v internetovom pripojení v dome rodičov a zariadil tak internet zadarmo. Ďalšie triky sa naučil koncom deväťdesiatych rokov na hackerských fórach. Zhruba v roku 2001 zmizol užívateľ Sabu zo scény, ale teraz, takmer po desiatich rokoch, bol zase späť. Sabu bol v porovnaní s ostatnými ostrieľaný veterán[7].

A ďalším bol hacker pod prezývkou Tflow, ktorý bol skúseným programátorom a ako pokračuje Olsonová:

> skôr tichý človek, ktorý striktne dodržoval jedno z pravidiel Anonymous a nikdy o sebe nehovoril. Medzi Anonymous sa pohyboval prinajmenšom štyri mesiace, teda dosť dlho na to, aby pochopil tunajšiu kultúru a zoznámil sa s kľúčovými aktérmi. Komunikačné kanály Anonymous a sympatizujúcich hackerov poznal lepšie, než väčšina ostatných. Príznačne to bol práve on, kto

[5] Ibidem, s. 63.

[6] Ibidem, s. 64.

[7] Ibidem, s. 17.

ako prvý prešiel k veci. Bolo nutné niečo urobiť s Aaronom Barrom a tým jeho „výskumom". Barr prehlasoval, že hnutie Anonymous má vodcu, čo nebola pravda. To znamená, že jeho výskum bol pravdepodobne mylný. Avšak v úryvku z článku The Financial Times stálo, že Barr „zhromaždil informácie o hlavných lídroch Anonymous, vrátane celej rady ich skutočných mien, takže keby sa tieto údaje dostali do rúk polície, mohli by byť zatknutí[8].

PRVÝ SPOLOČNÝ ÚTOK

A kto to vlastne je Aaron Barr? Aaron Bar bol americký vojak. Po dvoch semestroch na univerzite si uvedomil, že štúdium nie je nič pre neho a zapísal sa k námorníctvu. Čoskoro sa stal dôstojníkom spravodajskej služby pracujúcim s chránenými informáciami SIGINT a začal sa špecializovať na analýzu informácií. Slúžil na výsadkových lodiach a pri jednej pozemnej operácii v Kosove po ňom strieľali. Vďaka tejto skutočnosti začal nenávidieť vojakov, s akou ľahkosťou pristupujú k životu. Po dvanástich rokoch u námorníctva odišiel do civilu. V novembri 2009 sa Barrovi naskytla šanca. Oslovil ho bezpečnostný konzultant Greg Holland s otázkou, či by mu nepomohol založiť novú firmu. Holland, ktorý už šéfoval firme HBGary Inc. zaoberajúcou sa digitálnou bezpečnosťou, sa dozvedel o Barrových znalostiach kryptológie. Po Barrovi chcel, aby založil sesterskú spoločnosť, ktorá by sa špecializoval na poskytovanie služieb americkej vláde. Spoločnosť by niesla meno HBGary Federal a firma HBGary Inc. by v nej mala 10% podiel. Barrovi sa zaľúbila príležitosť byť vlastným šéfom a zároveň možnosť pracovať z domu a tráviť tak viac času zo svojou ženou a deťmi a tak po tejto ponuke skočil. Spočiatku bol Barr plný nápadov a niekedy ani nespal celé noci. Avšak ani po roku jeho práce žiadny z jeho nápadov ešte nezarábal. Nad vodou ho držali kurzy, ktoré klientov učili, ako využívať sociálne siete ako Facebook, LinkedIn či Twitter k získavaniu informácií o ľuďoch – ako špionážne nástroje. Každý takýto kurz mu priniesol zisk 25 000 amerických dolárov (USD). V decembri 2010 sa konečne objavila záchrana. Barr začal rokovať s právnickou firmou Hunton&Williams, ktorej klienti – medzi ktorých patrili napríklad Americká obchodná komora a Bank of America – potrebovali pomoc pri rokovaniach s protivníkmi. Nedávno napríklad organizácia WikiLeaks naznačila, že disponuje celým radom informácií získaných z Bank of America. Barr a ďalšie dve bezpečnostné firmy pripravili powerpointové prezentácie, v ktorých mimo iné navrhovali spustiť dezinformačné kampane vedúce k zdiskredito-

[8] Ibidem, s. 18–19.

vaniu novinárov podporujúcich WikiLeaks, alebo zaútočiť na webové stránky WikiLeaks. A potom Barra niečo napadlo. V San Franciscu sa mala konať konferencia B-Sides určená profesionálom z oblasti bezpečnosti. Keby a mu podarilo na konferencii predviesť, ako vďaka svojmu pátraniu na sociálnych sieťach našiel informácie o záhadných subjektoch, získal by vierohodnosť a s ňou možno aj vytúžených klientov. Barr dospel k názoru, že neexistuje lepší cieľ ako Anonymous. Zhruba pred mesiacom, v decembri 2010, boli médiá plné správ o veľkej a záhadnej skupine hackerov, ktorá začala napádať stránky spoločností MasterCard, PayPal a Visa ako pomstu za to, že bránili financovaniu WikiLeaks. WikiLeaks, totiž práve zverejnila tisícky tajných diplomatických depeší a jej zakladateľ a šéfredaktor Julian Assange bol vo Veľkej Británii zatknutý, údajne za sexuálne napadnutie. A ako pokračuje Olsonová:

> Slovo hacker je preslávené svojou nevyhranenou definíciou. Môže označovať nadšeného programátora aj internetového zločinca. Ale ľudia z Anonymous, alebo Anonovia, bývali často označovaní ako hacktivisti – hackerovia s aktivistickým poslaním. Podľa všetkého verili, že všetky informácie by mali byť voľne dostupné, a nebáli sa napadnúť stránky kohokoľvek, kto s nimi nesúhlasil. Prehlasovali o sebe, že nemajú žiadnu hierarchiu, ani vedenie. Dávali najavo, že nie sú skupina, ale všetko a nič. Najlepšie by sa možno dali označiť slovom „uskupenie" alebo „obchodná značka". Tých pár pravidiel, ktorými sa riadili, silne pripomínalo film Klub bitkárov: nikdy nehovor o Anonymous, nikdy neprezraď svoju skutočnú identitu a neútoč na médiá, pretože tie ti môžu pomôcť šíriť tvoje posolstvá. V prostredí anonymity bolo samozrejme ľahké sem tam skĺznuť k nejakej tej ilegálnej akcii, nabúrať sa do cudzích serverov, kradnúť spoločnostiam údaje o klientoch alebo vyradiť niečie webové stránky z prevádzky a potom ich zhanobiť. Za čokoľvek z toho mohol ísť človek na desať rokov sedieť. Ale Anonom to zrejme bolo jedno. Ich množstvo im koniec koncov dodávalo silu a pocit bezpečia. A tak na blogy, hacknuté stránky a všade, kde to len šlo, umiestňovali svoj zlovestný nápis:
>
> Sme Anonymous,
>
> Sme légia,
>
> Neodpúšťame,
>
> Nezabúdame,
>
> Očakávajte nás[9].

[9] Ibidem, s. 13–14.

Tou dobou všetci bezpečnostní špecialisti o Anonymous hovorili, ale nikto v skutočnosti presne nevedel, kto za týmto hnutím vlastne stojí. Barra to veľmi zaujalo. Sledoval, ako svet venuje tejto záhadnej skupine čoraz väčšiu pozornosť a hltal správy o desiatkach raidov a zatýkaní v Spojených štátoch amerických a v Európe. Nikto zo zatknutých však nebol odsúdený a nepodarilo sa ani odhaliť lídrov tohto hnutia. Barr bol presvedčený, že vďaka svojim skúsenostiam zo zdieľania na sociálnych sieťach by si viedol lepšie než agenti z FBI a možno by im mohol pomôcť. Pátrať po Anonymous bolo veľmi riskantné, ale hovoril si, že keby sa dostal do ich hľadáčiku, nanajvýš mu môžu iba ak na niekoľko hodín, nanajvýš niekoľko dní, zablokovať firemné stránky HBGary Federal. Vytvoril si prezývku, najprv AnonCog a potom CogAnon, a začal navštevovať internetové chaty, na ktorých sa stretávajú priaznivci Anonymous. Oslovil si ich spôsob komunikácie, situoval sa do úlohy nového mladého priaznivca netrpezlivo sa trasúceho na to, že odpáli nejakú firmu a podarilo sa mu medzi ostatných zapadnúť. Zapisoval si prezývky účastníkov, avšak pozornosť venoval iba tým najaktívnejším. Ako náhle sa však niekto z týchto ľudí odhlásil z chatu, poznamenal si Barr jeho prezývku a čas. Potom sa pripojil na Facebook. Mal tam totiž niekoľko falošných profilov a v tom čase mal už medzi „priateľmi" desiatky skutočných ľudí, ktorí hnutie Anonymous skutočne podporovali. Ak však niektorý z týchto priateľov začal byť na Facebooku aktívny iba chvíľu po tom, ako nejaká prezývka opustila chatovaciu miestnosť Anonymous, Barr si vydedukoval, že je to ten istý človek. Koncom januára 2011 dokončoval Barr dvadsaťstránkový dokument obsahujúci mená, popis a kontaktné údaje osôb, ktoré by mohli byť členmi hnutia Anonymous, alebo dokonca stáť v jeho čele. Dňa 22.1. 2011 potom poslal e-mail Hoglundovi, v ktorom ho informoval, že na blížiacej sa konferencii B-Sides bude prednášať o Anonymous, od čoho si sľubuje predovšetkým pozornosť médií. O výskume tzv. „bezpečnostného experta" Aarona Barra potom prostredníctvom svojho falošného profilu informoval aj niekoľkých ľudí z Anonymous. Holland mu však obratom odpísal, že by sa nerád stal terčom DDoS útokov. Barr sa teda rozhodol, že najlepšie bude kontaktovať nejakých novinárov ešte pred svojou prednáškou. Spojil sa s Josephom Mennom, novinárom zo San Francisca, píšucim pre The Financial Times a ponúkol mu rozhovor v ktorom by mu objasnil, ako môžu ním získané informácie prispieť k zatknutiu „veľkých rýb" z Anonymous. Novinára navyše navnadil, že za väčšinou útokov stojí iba asi desať ľudí, a že hnutie

nakoniec nie je až tak nehierarchické a anonymné, ako by sa mohlo zdať. Článok, ktorý niesol názov Kyberaktivisti varovaní pred zatknutím, vyšiel v piatok 4. februára a citoval Barra. Popoludní toho istého dňa sa Barrovi ozvali aj agenti FBI so žiadosťou, či by im nemohol získané informácie poskytnúť. Dohodli si s ním schôdzku na pondelok, teda deň po Superbowle. Avšak zhruba v rovnakú dobu si článok prečítalo aj niekoľko hackerov z Anonymous. A boli to práve vyššie uvedení hackeri: Topiary, Kayla, Sabu a Tflow.

Po dlhšej vzájomnej debate sa hackeri zhodli na tom, že ak by boli Barrove informácie správne, niektorým Anonom hrozí vážny problém. A tak sa skupina pustila do plánovania. Najprv museli preskúmať server, na ktorom bežali stránky HBGary Federal a pokúsiť sa odhaliť slabiny v zdrojovom kóde. Za pár minút sa ukázalo, že Barrove stránky bežia na verejne prístupnom redakčnom systéme, v ktorom bola zásadná programová chyba. Bingo! Aj keď úlohou spoločnosti HBGary Federal bolo pomáhať iným spoločnostiam s ochranou pred počítačovými útokmi, firma sama si nezabezpečila svoje vlastné stránky pred jednoduchou formou útoku, nazývanou „SQL injekcia", pomocou ktorej sa napádajú databázy. Databázy sú totiž jednou z mnohých kľúčových technológií umožňujúcich fungovanie internetu. Ukladajú sa do nich heslá, firemné e-maily a celý rad ďalších druhov údajov. Obľúbeným nástrojom pre čítanie a upravovanie informácií obsiahnutých v databázach je programovací jazyk Structured Query Language (SQL). Tento jazyk je však možné obrátiť proti nemu samému. Útočník musí iba prinútiť server, aby si vykladal napísané znaky nie ako text, ale ako SQL otázky, ktoré má vykonať. Takýto útok potom môže byť pre firmu zničujúci.

Naši hackeri teda prenikli do vnútra serveru, avšak objavil sa problém. Heslá boli zašifrované, alebo ako sa hovorí zahašovené, pomocou bežnej techniky zvanej MD5. Keby všetci administrátori používali dlhé a zložité heslá, hackerom by sa nepodarilo rozšifrovať ich. Avšak Sabu sa nevzdával. Vybral si tri haše a nahral ich do programu nazvaného HashKiller. A za pár hodín, už náhodní anonymní dobrovoľníci rozlúskli všetky haše. Výsledok vypadal asi takto: 4036d5f575fb46f48ffcd5d7aeeb5af:kibafo33

Na samom konci reťazca písmen a čísiel bolo heslo Aarona Barra. Hackeri sa pomocou helsa „kibafo33" skúsili prihlásiť k e-mailovému účtu HBGary Federal, ktorý bol hosťovaný na Google Apps a podarilo sa. Hackeri nemohli uveriť svojmu šťastiu. V piatok večer, už sledovali nič ne-

tušiaceho Barra, ako si spokojne e-mailuje so svojimi kolegami ohľadne článku v The Financial Times. Jedného z našich hackerov potom napadlo skúsiť, či im toto heslo neumožní prístup ešte k inému jeho účtu. Za pokus to stálo. A akokoľvek sa to u odborníka na počítačovú bezpečnosť, šťúrajúceho do ľahko výbušného hnutia Anonymous zdalo nepravdepodobné, Barr toto ľahko rozlúštiteľné heslo používal na takmer všetkých svojich internetových účtoch, vrátane Twitteru, Yahho!, Flickri, Facebooku a dokonca aj u hry World of Warcraft! To znamenalo, že sa tu otváral priestor pre čisté a ničím nerušené lulz.

Pre Barra sa nasledujúca sobota začala ako každá iná. Trávil čas s rodinou, vybavil si pár e-mailov cez svoj iPhone, a vôbec netušil, že skupina hackerov z hnutia Anonymous je zaneprázdnená prechádzaním jeho e-mailovej schránky a raduje sa nad svojimi objavmi. Jej najnovším objavom boli samotné výsledky Barrovho výskumu o Anonymous. Šlo o dokument vo formáte PDF, ktorý obsahoval chronologický prehľad nedávnych útokov Anonymous a množstvo prezývok priradených ku skutočným menám a adresám. Avšak prezývky Sabu, Topiary, či Kayla tam chýbali. Začalo byť zjavné, že Barr strieľa od boku. Hacker Tflow následne stiahol všetky Barrove emaily na svoj server a potom asi 15 hodín čakal, než sa z nich skomprimuje torrent. Tflow mal v úmysle umiestniť tento torrentový súbor na zďaleka najobľúbenejší internetový portál – The Pirat Bay. Znamenalo by to, že viac ako štyridsať tisíc e-mailov odborníka na počítačovú bezpečnosť, Aarona Barra, by si mohol prečítať ktokoľvek.

V nedeľu ráno, asi 11 hodín pred výkopom Superbowlu mal už Tflow usporiadané všetky e-maily Barra. Torrentový súbor bol pripravený a hackerov čakala príjemná správa oznámiť Barrovi, čo mu vyviedli. Avšak Barr po zapnutí svojho počítača a načítaní svojej stránky zistil, že stránka sa otvára veľmi pomaly. Začal tušiť, že sa stal obeťou DDoS útoku. Hackeri začali s ním viesť rozhovor a navrhli mu, či by sa nedal nahovoriť na jeden útok v okolí New Yorku. Topiary navyše uviedol, že ich cieľom je jedna bezpečnostná spoločnosť v okolí New Yorku. To už Barrovi vyschlo v krku a začal tušiť, že je zle. V následných rozhovoroch s Topiarym sa snažil vysvetliť, že on nemá nič proti Anonymous. Výsledkom bolo, že spoločne s výkopom Superbowlu hackeri z Anonymous vyvesili na webovú stránku Barrovej firmy HBGary Federal nasledujúce vyhlásenie:

> Tejto domény sa zmocnili Anonamous v súlade zo 14. bodom pravidiel internetu. Zdravíme HBGary (počítačovú bezpečnostnú firmu). Vaše nedávne

> tvrdenia, že ste „infiltrovali" Anonymous nás úprimne pobavili, rovnako ako váš pokus zneužiť Anonymous k prilákaniu médií. Ako sa vám páči takáto pozornosť? Chceli ste zahryznúť Anonymous do ruky, ale teraz vás táto ruka preplieskáva po ksichte"[10].

Po tomto útoku Anonymous sa Barr nedokázal odlepiť od chatovacích miestností Anonymous. Navyše, Barr hypnotizovane sledoval, ako si návštevníci chatovacích miestností robili z neho žarty. Telefón mu neprestával zvoniť celú noc. Občas mu prišla nejaká hlasová správa, vrátane naspievanej pesničky Never Gonna Give You Up, od Ricka Astleyho z roku 1987. Šlo o obľúbený žart Anonymous.

Ako uvádza Olsenová:

> Týmto činom sa Sabu, Kayla, Topiary a ďalší hackeri v komunite Anonymous preslávili ako hrdinní vymáhači spravodlivosti. Barr dostal čo mu patrilo. Odvážil sa provokovať svet, v ktorom výsmech, klamstvá a krádeže, boli na dennom poriadku. Svet v ktorom si človek mohol užiť euforických zážitkov, srandy a pocitu zadosťučinenia, bez toho, aby mu – teoreticky – v reálnom svete hrozili akékoľvek následky[11] .

Hackeri práve zostrelili bezpečnostnú spoločnosť. Napriek tomu, že v skryte duše tušili, že po nich ihneď začnú pátrať agenti FBI, postupom času dospeli k názoru, že keď sa im na prípade Barr spolupracovalo tak dobre, musia teraz pokračovať a útočiť na ďalšie a ďalšie ciele… v mene lulz, v mene Anonymous, v mene akéhokoľvek vyššieho poslania, ktoré sa im cestou vyskytne. Nezľaknú sa žiadneho cieľa, ani svetoznámej inštitúcie, ani giganta zábavného priemyslu, ani samotnej FBI.

ŠTÝL ÚTOKOV

Väčšina útokov hackerov z hnutia Anonymous bola organizovaná buď útokmi DDoS, alebo útokmi typu botnet, či útokmi pomocou nízkoorbitálneho iontového kanónu (LOIC).

DDoS útoky sa dajú charakterizovať ako keď internetový obchod vyhlási 75% zľavu a potom nezvládne príval zákazníkov. Môže sa to zdať banálne, pretože každý, kto niekedy surfoval po internete, má zo špatným spojením a chybovými stránkami skúsenosť. Keď sú stránky vyťažené z dôvodu veľkej prevádzky na niekoľko hodín alebo dokonca dní, môže to firmu

[10] Ibidem, s. 29.

[11] Ibidem, s. 32.

stáť pekný balík peňazí. Keď sa do útoku zapojilo dosť ľudí a zahltilo cieľové stránky zbytočnou prevádzkou, vznikol rovnaký efekt, ako keby sa 15 tlstých chlapov snažilo v rovnakú dobu prejsť otočnými dverami. Všetko jednoducho zamrzlo. Zúčastňovať sa DDoS útokov je navyše nezákonné. V USA sa tým porušuje zákon nazvaný „Computer Fraud and Abuse Act a vo Veľkej Británii Zákon o polícii a súdnictve z roku 2006. V obidvoch krajinách hrozí páchateľom až desať rokov odňatia slobody.

Botnet je zariadenie, ktoré (ako bolo vyššie uvedené) predstavuje sieť tzv. „zombie" počítačov, ktoré boli infikované vírom alebo podvodným softwarom a pomocou nich potom prepojené. Botnety spravidla ovláda jeden človek, ktorý potom dokáže tisícom, niekedy aj miliónom počítačov naraz zaveliť, aby hromadne vykonávali internetové príkazy. V rámci hnutia Anonymous sa v rokoch 2010–2011 objavili dvaja hackeri, ktorí vlastnili takúto sieť botnetov, pomocou ktorých vykonávali útoky. Podľa Olsonovej to boli

> Civil (písané Civill) a Switch. Boli to botmajstri. Každý z nich ovládal svoj vlastný botnet, v tom Civilovom bolo päťdesiatpäť tisíc nakazených počítačov, v Switchovom okolo sedemdesiatpäť tisíc. Anonovia vlastniaci botnety požívali medzi Anonymous zvláštnej úcty, nakoľko niekoľkými kliknutiami dokázali dočasne vyradiť z prevádzky internetovú sieť, IRC sieť alebo čokoľvek iného, čo si zmysleli[12].

Nešlo teda o dobrovoľných účastníkov útokov. Ľuďom, ktorí sa do útoku zapojili dobrovoľne nepatril ani jeden z počítačov. Boli to tzv. „zombie" počítače. A úlohou botmajstrov bolo sledovať, kedy nejaký človek (ktorý nemal ani potuchy, že jeho počítač je infikovaný), išiel spať, vypol svoj vlastný (infikovaný) počítač. Lebo tým sa znížil výkon botnetu o jeden počítač. Z tohto dôvodu Civil nerád používal všetkých päťdesiatpäť tisíc svojich botov naraz. Miesto toho ich používal len pár tisíc a každých 15 minút ich menil. Ako náhle totiž botnet začal útočiť, majitelia nakazených počítačov zaznamenali, že sa im spomalilo internetové pripojenie. Väčšinou si mysleli, že problém je v ich routeri, a začali sa vŕtať v nastavení, poprípade vypli počítač úplne. Cieľom neustáleho obmeňovania botov bolo zaistiť, aby majitelia svoje počítače nevypli, alebo aby nezavolali technikov, čo by bolo ešte horšie.

Útok typu LOIC. Tento, pôvodne open source projekt, dokáže na určený server posielať zbytočné otázky, alebo tzv. „pakety". Pakety sú súčasťou

[12] Ibidem, s. 122–123.

všetkého, čo človek na internete robí. Prehliadanie internetových stránok, alebo posielanie e-mailov znamená prijať sériu paketov, pričom typický paket má 1000–1500 bajtov. Pakety by sme mohli prirovnať k bežným obálkam posielaných poštou. Takzvaný „packet sniffing", alebo očmuchávanie paketov, potom označuje snahu zistiť, čo sa nachádza vo vnútri listu a to iba za použitia údajov nachádzajúcich sa na obálke. Ak sa do tohto útoku zapojilo dostatočné množstvo ľudí, dokázali cieľovú stránku zahltiť veľmi rýchlo a tak ju dočasne vyradiť z prevádzky. Hlavným rozdielom od botnetu bolo to, že tu sa nezapájali cudzie počítače, ale iba počítače členov hnutia Anonymous, ktorí sa do útoku zapojili dobrovoľne.

NAJZNÁMEJŠIE ÚTOKY ANONYMOUS

O najznámejších útokoch tohto hnutia bolo popísané veľmi veľa článkov, či už v novinách, alebo na rôznych internetových stránkach. Nakoľko rozsah tohto článku nám nedovoľuje dopodrobna rozobrať všetky útoky tohto hnutia, základné údaje o najznámejších útokoch sa nachádzajú v Prílohe Časová os na konci tohto článku.

Z hľadiska informačnej bezpečnosti si však určite zaslúži pozornosť útok hnutia Anonymous na webovú stránku spoločnosti PayPal, ktorá odmietla realizovať transakcie na podporu spoločnosti WikiLeaks. Z tohto dôvodu sa hnutie rozhodlo, že na túto stránku zaútočiť. To sa im aj podarilo a hackeri Anonymous slávili zostrelenie najväčšej platobnej spoločnosti na svete. Hlavné spravodajské servery od BBC cez The New York Times až po The Guardian informovali, že stránky PayPalu vyradili z prevádzky hackeri z globálnej skupiny Anonymous. Tu však nastal problém. Ako uvádza Olsonová:

> Sean-Paul Correl zo spoločnosti Panda Security sa pod prezývkou muihtil (lithium odzadu) prihlásil na IRC sieť a poslal odkaz samotnému Switchovi. Vysvetlil mu, že je bezpečnostný analytik a rád by sa dozvedel veľkosť jeho botnetu. Switch bol až prekvapivo zhovievavý. Povedal Correlovi, že jeho kamarát (pravdepodobne Civil) do útoku zapojil tridsať tisíc botov, skupina útočiaca pomocou LOIC mala päťsto počítačov a on sám ich zapojil tisiítristo[13].

To len potvrdilo skutočnosť, že pri útoku na stránky PayPal.com až 90% celkovej palebnej sily nepochádzalo od dobrovoľníkov z radov Anonymous, ale od tzv. zombie počítačov. Topiary začal následne v tichosti pre-

[13] Ibidem, s. 126.

mýšľať o skutočnej sile davu. Keď sa pred pár dňami po prvý krát pripojil na veliteľský kanál command, myslel si, že za DDoS útokmi Anonymous stáli predovšetkým tisícky ľudí s programom LOIC a že tajomné botnety hrali iba podpornú úlohu. Teraz mu došlo, že je to presne naopak. Keď prišli na rad útoky na veľké stránky ako PayPal.com skutočnými útočníkmi boli botnety.

Tu sa dostávame do súladu s tvrdeniami odborníkov na informačnú bezpečnosť, že celkový počet hackerov na svete je od niekoľkých desiatok po niekoľko stoviek osôb. Nie viac. Tieto slová potvrdzuje aj slovenský odborník na informačnú bezpečnosť a prorektor Univerzity Komenského v Bratislave profesor Daniel Olejár. V relácii Téma dňa v televízii TA3 zo dňa 6.6. 2017 uviedol:

> Vo všeobecnosti sa má za to, že masový útok (v tomto konkrétnom prípade išlo o masový útok na jednu slovenskú nemocnicu – poznámka autora) spôsobila veľká skupina útočníkov. Nie, toto je asymetrická vojna. Je pár šikovných ľudí, ktorí sa vyznajú v informatike, v informačných systémoch dostatočne nato, aby vedeli nájsť chyby, ktoré unikajú aj tvorcom týchto systémov. No a žiaľ, zverejnia, podelia sa o svoje informácie aj s širokou hackerskou verejnosťou a využijú ich na útok na nič netušiacich používateľov[14].

Na otázku redaktora koľko takýchto útočníkov sa útoku zúčastňuje, profesor Olejár odpovedal: „Kamaráti pôsobiaci v brandži, vo firme hovoria, že sa nejedná o nejaké masové počty. Napríklad v oblasti malwearu sa môže jednať o desiatky až stovky ľudí na celom svete"[15].

Ide teda o niekoľko desiatok, maximálne stoviek ľudí na celom svete. Čo je teda príčinou takýchto útokov? Ako sme mohli vyššie vidieť, naši hackeri väčšinou pochádzajú z neúplných (rozvedených) rodín, pričom ich rodičia nemali dostatok času na ich riadnu výchovu a vzdelanie. Navyše, sami budúci hackeri nejavili prílišný záujem o štandardný systém školského vzdelávania. Poväčšinou ešte aj trpeli nejakou fyzickou, alebo psychickou chorobou, ktorá im bránila v utváraní si prirodzených sociálnych vzťahov s ľuďmi z reálneho sveta. A títo ľudia po získaní prístupu na internet zrazu objavili pre seba priestor, ktorý im umožňoval sebarealizáciu bez toho, aby niekto poukazoval na ich fyzické alebo psychické nedostatky, a vytváral im možnosti plne sa realizovať v oblastiach v ktorých mali predpoklady

[14] Dostupné online: http://www.ta3.com/clanok/1106873/specialny-prokurator-v-parlamente-kyberneticka-bezpecnost-cierna-hora-je-clenom-nato.html

[15] Ibidem.

byť veľmi úspešní. Nakoľko však vo väčšine prípadov odmietali štandardné autority reálneho sveta (učiteľov, kňazov, vychovávateľov, či trénerov), ktorí počas povinnej školskej dochádzky formujú morálku a svetonázor väčšiny mladých ľudí, hackeri si svoj svetonázor utvárali na základe dostupných (často pochybných) informácií na internete.

Ako príklad si môžeme vziať aj mediálne známu osobnosť tzv. whistleblowera – informátora Edwarda Snowdena, ktorý na otázku redaktora Greenwalda o tom, kto alebo čo utváral jeho vlastný morálny profil odpovedal: „Podľa jeho vlastných vyjadrení jeho morálny profil sa kreoval z rôznych zdrojov a skúseností"[16]. Počas detstva a dospievania čítal veľa kníh o gréckej mytológii a ovplyvnilo ho i dielo Josepha Campbella Tisíc tvárí hrdinu, ktoré vraj nachádza metaforickú niť osudu spájajúcu naše životné príbehy. Jedným z hlavných ponaučení, ktoré si z neho zobral, bolo, že „my sami vdychujeme životu zmysel svojimi činmi a vytvárame tak vlastný príbeh"[17]. Ľudia nadobúdajú obsah a sebaurčenie prostredníctvom vlastného konania. „Nechcem aby sa zo mňa stal človek, ktorý sa bojí konať v mene obrany svojich princípov"[18].

Tento leitmotív – mravný rámec hodnotenia vlastnej identity a hodnoty, bol jeho pravidelným spoločníkom pri budovaní svojej osobnosti. Ale kto sa ešte podieľal na formovaní jeho morálneho profilu? Ako on sám trošku zahanbene priznáva: „Čerpal som z videohier"[19]. A Greenwald pokračuje:

> Pohrúžený do hier sa naučil, že aj jeden jediný človek, zdanlivo úplne bezmocný, dokáže vzdorovať veľkej nespravodlivosti. Hlavným hrdinom (hovorí Snowden) je zvyčajne bežný človek, na ktorom spáchajú mocné sily smrteľnú krivdu. Má na výber: buď stiahne chvost a utečie, alebo sa otvorene postaví na obhajobu svojich ideálov. V dejinách tiež nájdeme príklady, keď navonok obyčajní ľudia, dostatočne odhodlaní brániť spravodlivosť, dokázali poraziť aj tých najhrozivejších protivníkov[20].

Greenwald ďalej priznáva, že Snowden nebol jediným v jeho kariére novinára, kto mu potvrdil, že jeho svetonázor sa utváral prostredníctvom videohier.

---

[16] G. Greenwald, *Nikto sa neskryje – Edward Snowden, NSA a americké systémy hromadného odpočúvania*, Tatran 2015, s. 57.

[17] Ibidem.

[18] Ibidem.

[19] Ibidem.

[20] Ibidem.

> Pred rokmi by som si z toho isto robil žarty. Doba sa však zmenila a v generácii Snowdenových rovesníkov zohrali hry pri tvarovaní politického vedomia, hodnôt a chápaní seba samého prinajmenšom rovnakú úlohu ako knihy, televízia či filmy. Videohry, podobne ako iné typy umenia, často prinášajú zásadné morálne konflikty a nútia ľudí, ktorí začínajú inak uvažovať, aby sa zamysleli nad platnosťou všeobecne prijímaných dogiem[21].

Snowdenove názory o podstate morálky sa teda formovali na základe spomínaných vyššie uvedených diel a vytvorili, ako sám uviedol „vzor človeka, akým sa chcem stať". Spočiatku mladícke úvahy v dospelosti prerástli do seriózneho hĺbania o etických povinnostiach a vnútorných rozporoch, ktoré bránia človeku konať v ich záujme. Ako popisuje Snowden: „Ľudia sú často pasívni a poslušní, lebo sa boja negatívnych následkov, ak vyjadria nesúhlas, ale keď sa raz vzdáme lipnutia na veciach, na ktorých v podstate vôbec nezáleží – na peniazoch, kariére, či fyzickej bezpečnosti – získame slobodu a zbavíme sa strachu"[22]. A mladý človek, ktorý nedokončil ani len strednú školu, sa tak dostáva do morálnej dilemy, ktorú musí riešiť.

Navyše, ústrednú úlohu vo vývoji jeho osobnosti zohral aj internet. Rovnako ako pre jeho rovesníkov aj preňho znamenal internet oveľa viac, ako len akýsi príležitostný pracovný nástroj. Ako popisuje Greenwald: „Bol to jeho celý svet, priestor, v ktorom sa vyvíjala osobnosť a formulovali názory, miesto poskytujúce slobodu, nekonečné možnosti poznania a intelektuálneho rastu"[23]. Jedinečné príležitosti, ktoré internet ponúkal, mali pre Snowdena nevyčísliteľnú hodnotu, a bolo ho preto treba chrániť za každú cenu. Ako tínedžer spoznával prostredníctvom internetu svet a hovoril s ľuďmi zo všetkých jeho končín, ktorí často pochádzali z úplne iného prostredia ako on. Bez internetu by nemal takúto možnosť. Ako spomína Snowden:

> Internet mi v podstate umožnil zažiť skutočnú slobodu a spoznať seba samého ako ľudskú bytosť… Pre mnohé detská je internet hlavným zdrojom sebapoznania. Umožňuje im zistiť, kto vlastne sú a kým sa chcú stať, ale podarí sa to len vtedy, ak konajú v súkromí, anonymne, ak smú spraviť chyby bez toho, aby ich prenasledovali do konca života. Obávam sa, že moja generácia je posledná, ktorá si užíva takúto slobodu… Nechcem žiť vo svete, v ktorom

[21] Ibidem.

[22] Ibidem, s. 57–58.

[23] Ibidem, s. 58.

niet súkromia ani slobody, vo svete, kde sa degraduje a potláča jedinečný potenciál internetu[24].

Snowden teda cítil povinnosť urobiť všetko preto, aby tomu zabránil, presnejšie, aby umožnil ľuďom vybrať si, či chcú, alebo nechcú brániť tieto hodnoty. Snowden opakovane zdôrazňoval, že jeho cieľom nie je zničiť metódy, ktoré Národná bezpečnostná agentúra (NSA) používa na elimináciu súkromia. Práve naopak. Chcel, aby sa americkí občania a ľudia na celom svete dozvedeli, čo sa im za chrbtom deje so súkromím. Chcel len informovať. „Nemám v úmysle zničiť systémy, ale chcem, aby sa verejnosť slobodne rozhodla, či majú pokračovať, alebo nie"[25].

Tieto, alebo podobné pohnútky boli s vysokou pravdepodobnosťou aj motívom hackerov zo skupiny Anonymous pri uskutočňovaní cielených útokov voči jednotlivcom a organizáciám, ktoré sa snažili o ochranu citlivých údajov. A pocit masovosti tohto hnutia im pravdepodobne dával pocit slobody a beztrestnosti, aj keď si určite uvedomovali, že páchajú trestné činy. Avšak ich hlavným motívom tejto činnosti bol lulz.

Asi najlepšie to dokumentuje útok na americkú verejnoprávnu televíziu PBS, ako odplatu za to, že vo svojom hlavnom spravodajskom programe Frontline sa v máji 2011 negatívne vyjadrila o osobnosti Juliana Assangeho. Preto sa Sabu a Topiary rozhodli, že sa nabúrajú do ich redakčného systému spravodajského programu NewsHour, cez ktorý PBS publikovala články na svojom webe. A Topiary si uvedomil, že takto vlastne môže napísať zdanlivo legitímny článok priamo na hlavnej stránke NewsHour. Nakoniec sa rozhodol, že napíše článok o americkom rapperovi Tupacovi Shakurovi, ktorý bol v roku 1996 zastrelený v Las Vegas, avšak doteraz o ňom kolujú legendy, že v skutočnosti stále žije. Topiary preto napísal článok, že rapper stále žije na Novom Zélande. Po zverejnení tejto správy nastal v radoch čitateľov veľký záujem zistiť, či je to pravda a redaktori PBS nestíhali odpovedať na telefonáty čitateľov. Darmo sa bránili, že ide o hack, článok na stránkach verejnoprávnej televízie vzbudzoval dôveryhodnosť. Počas jednej hodiny bola zmienka o tomto článku zaznamenaná na Twitteri viac ako 150 krát. Tento počin sa dostal aj do hlavných amerických spravodajských médií ako sú noviny The New York Times, či The Wall Street Journal. Anonymous po útoku poskytli jediný rozhovor a to časopisu Forbes. V ňom sa útočníci nechali počuť, že na PBS zaútočili z dvoch

[24] Ibidem.

[25] Ibidem.

dôvodov: „Kvôli lulz a kvôli spravodlivosti. Aj keď naším hlavným cieľom je šíriť zábavu, zároveň si prajeme, aby sa o tomto dopočul Bradley Manning a možno sa aj pousmial"[26]. Niekoľko odporcov obviňovalo Anonymous, že používajú k útokom jednoduché SQL injekcie. A Topiary mal chuť im to vyvrátiť. A preto napísal správu: „Drahí trollovia, na PBS.org sme sa dostali cez 0day, ktorý sme objavili v mt4, teda MoveableType4…Aj v tomto prípade sme sa mohli siete zmocniť hlavne kvôli tomu, že mnohí zamestnanci PBS, ktorí mali prístup k zabezpečenejším častiam siete, použili to isté heslo na niekoľkých miestach"[27].

Topiary bol ako vo vytržení. Nemal chuť do jedla, nechcelo sa mu spať, nezaujímalo ho nič iné než pozdvihnutie, ktoré vyvolali spolu so Sabuom, Kaylou a ďalšími, ku ktorým patril. Aj kvôli jeho brilantnému písaniu odkazov vonkajšiemu svetu, teraz pôsobili skôr ako rocková kapela, než ako skupinka hackerov[28].

ZÁVER

Cieľom tohto článku bolo poukázať na fenomén hackerského hnutia Anonymous a v krátkosti predstaviť jeho ciele, hlavných aktérov a spôsoby, ako podnikali (podnikajú) útoky voči organizáciám, ktoré podľa ich presvedčenia bránia slobodnému prístupu k informáciám (najmä) na internete. Rozsah článku nedovoľuje rozobrať detailnejšie všetky útoky tohto hnutia, ani všetkých hlavných aktérov (z ktorých nami spomenutí boli všetci následne odhalení a stíhaní), ani presné motívy ich činov. Avšak aj z tohto krátkeho prehľadového článku je možné hodnotiť, že cieľom tohto hnutia je užiť si zábavu na účet niekoho iného, pričom aktérmi týchto útokov sú vo väčšine prípadov mladiství ľudia, pochádzajúci zo slabších sociálnych vrstiev, vyrastajúci často v neúplných rodinách, ktoré nemajú čas sa im plne venovať pri ich výchove. Často ide aj o ľudí, ktorí trpia nejakou psychickou, alebo fyzickou poruchou, pre ktorú sa reálnom živote nedokážu plnohodnotne uplatniť. O to väčší priestor im ponúka anonymné prostredie internetu a sociálnych sietí. Tu sa môžu ich schopnosti naplno prejaviť bez toho, aby niekto kritizoval ich fyzické, alebo psychické nedostatky. Navyše, medzi týmito ľuďmi hlavnú úlohy pri výchove zohrávajú informácie dostupné na internete a posolstvá ukryté vo videohrách, ktoré potom

[26] P. Olsonová, op. cit., s. 273.

[27] Ibidem, s. 274.

[28] Ibidem, s. 275.

následne utvárajú ich svetonázor a morálny profil. A na základe takto formovaných vlastností sa potom títo mladí ľudia zapájajú do rôznych skupín na chatovacích fórach a využívajú svoje (často veľmi pokročilé) počítačové schopnosti na nezákonné činnosti. A pocit anonymity a masovosti im dodáva pocit moci a beztrestnosti, akého sa im v reálnom živote nedostáva. Tých najschopnejších je však iba niekoľko desiatok či stoviek. Avšak títo jedinci dokážu k sebe pritiahnuť tisíce až milióny ďalších anonymných surferov po internete a získať ich pre svoju vec. A prostredníctvom nich sa nabúravať do nimi preferovaných stránok. Z pohľadu informačnej bezpečnosti je preto veľmi dôležité (ako to bolo v článku niekoľkokrát spomenuté), aby radoví užívatelia internetu neuľahčovali hackerom prácu a vytvárali si silné heslá a mali svoj počítač v poriadku zabezpečený maximálnou možnou ochranou. Nakoľko sami hackeri priznali, že ich najlepším pomocníkom je nedbalosť užívateľov a používanie toho istého (jednoduchého) hesla na viacerých účtoch.

Útokom takéhoto typu sa pravdepodobne nedá zabrániť. A budú sa objavovať v budúcnosti čoraz častejšie. Avšak dodržiavanie základných pravidiel informačnej bezpečnosti dokáže hackerom výrazne sťažiť ich prácu. Preto je len na každom z nás, aby sme sa nestali obeťou takéhoto útoku.

POUŽITÁ LITERATÚRA:

1. Greenwald G., *Nikto sa neskryje – Edward Snowden, NSA a americké systémy hromadného odpočúvania*, Tatran 2015.
2. Olsonová P., *Jsme Anonymous. Uvnitř hackerského světa Anonymous, LulzSec a globálne internetové vzbury*, Vydavateľstvo Práh 2012.
3. TA3.com, http://www.ta3.com/clanok/1106873/specialny-prokurator-v-parlamente-kyberneticka-bezpecnost-cierna-hora-je-clenom-nato.html

PRÍLOHA – SLOVNÍČEK POJMOV[29]

4chan: Obľúbené obrázkové fórum, ktoré každý mesiac navštívi 22 miliónov unikátnych užívateľov. Pôvodne bol 4chan zamýšľaný ako diskusný portál o japonskom anime, ale postupom času toto zameranie stratil a stal sa miestom pre diskusie všetkého typu. Mimo iné sa tu organizujú internetové žartíky aleob raidy proti iným osobám či webovým stránkam.

[29] P. Olsonová, op. cit., s. 489.

Kľúčovým rysom je vynucovaná anonymita používateľov, ktorí tak môžu prispievať bez zábran a strachu zo zodpovednosti.

Anonymous: Označenie odkazujúce na skupinu ľudí, ktorí budia rozruch na internete a vyvádzajú rôzne kúsky na protest proti tomu či onomu. Názov, ktorý v preklade jednoducho znamená „anonymní", sa odvíja od vynútenej anonymity užívateľov obrázkového fóra 4chan a v posledných siedmych rokoch začal byť spájaný s významnými počítačovými útokmi na rôzne spoločnosti a vládne agentúry. Skupina nemá jasne vymedzenú hierarchiu ani pravidlá členstva a existuje len ako premenlivé zoskupenie ľudí, ktorí vyznávajú nejasnú sadu zásad odvodenú od 47 pravidiel internetu. V reále zoskupenie dostáva rôzne podoby, podľa toho, kto sa zrovna k názvu prihlási – príkladom môžu byť organizátori operácie Chanológia z roku 2008, alebo hackeri zo skupiny LulzSec.

Antisec (Anti Security): Internetové hnutie *black hat* hackerov, ktorí na prelomu tisícročia protestovali proti tomu, aby firmy z odboru počítačovej bezpečnosti verejne publikovali zoznamy odhalených bezpečnostných slabín. Hnutie v roku 2011 znovu oživila skupina LulzSec so zahmleným cieľom napádať vládne agentúry či dôležité organizácie a odhaľovať ich, často domnelú, korupciu.

/b/ : Najpopulárnejšia sekcia obrázkového fóra 4chan, ktorú navštevuje asi tretina všetkých užívateľov. Keď Christoper „mooť" Poole zakladal stránky 4chan, sekciu /b/ vyhradil diskusiám na náhodné, nezaradené témy. Na tejto nepopísanej doske internetu sa potom zrodila drvivá väčšina internetových memov, medzi nimi napríklad *lolcats*, humorné obrázky mačiek. Obecne sa má za to, že práve tu sa vyvinulo „kolektívne vedomie" Anonymous, a mnohí priaznivci tohto hnutia tvrdia, že po prvý krát sa o Anonymous dozvedeli práve cez /b/. Sekcia je preslávená úplnou absenciou moderátorov.

Black hat: *Black hats*, v slovenčine „čierne klobúky", sú hackeri, ktorí využívajú znalosti programovania k škodlivým účelom, napríklad hanobeniu cudzích webových stránok, alebo kradnutiu databáz s osobnými údajmi užívateľov za účelom predaja niekomu ďalšiemu. *Black hat* hackerom sa niekedy hovorí aj „crackeri".

Botnet: Sieť tzv. „zombie" počítačov, ktoré boli infikované vírom alebo podvodným softwarom a pomocou nich potom prepojené. Botnety spravidla ovláda jeden človek, ktorý potom dokáže tisícom, niekedy aj miliónom počítačom naraz zaveliť, aby hromadne vykonávali internetové príkazy.

Chanológia: Niekedy tiež nazývaná projekt Chanológia. Šlo o celý rad počítačových útokov, žartov a protestov namierených proti Scientologickej cirkvi, ktoré poriadali priaznivci Anonymous počas veľkej časti roku 2008. Názov je zloženina zo slov „4chan" a „scientológia".

DDoS (distribuované odmietnutie služby): Útok na webovú stránku alebo sieťový zdroj, pri ktorom veľké zoskupenie počítačov vyradí stránku z prevádzky tým, že ju preťaží zbytočnými žiadosťami. Útok môže byť prevedený buď skupinou dobrovoľníkov, z ktorých každý má vlastný počítač (pozri heslo LOIC), alebo sieťou počítačov, ktoré boli infikované a zoskupené do botnetu.

Dox: „Doxovať" znamená zisťovať niečie osobné údaje, ako sú napríklad skutočné meno a priezvisko, telefónne číslo alebo adresu domov, a to obvykle pomocou sociálneho inžinierstva alebo vyhľadávaním na Googli. Získané informácie potom predstavujú „dox" danej osoby.Doxovanie sa medzi Anonymous a v iných hackerských komunitách často používa ako vyhrážka, nakoľko ľudia sa tu skrývajú za prezývkami a takmer nikdy neprezrádzajú svoje skutočné identity.

Encyklopedia Dramatica: Webová stránka, ktorá zaznamenáva veľkú časť diania okolo Anonymous a informuje napríkald o internetových memoch, 4chanovvom slangu alebo diskusiách medzi obľúbenými užívateľmi rôznych blogov a IRC sietí. Svojim spôsobom je Encyklopedia Dramitica paródiou na Wikipédiu – používa rovnaký vzhľad a rovnako ju môže upravovať ktokoľvek, akorát že jej štýl vyjadrovania sa je uštipačný, obhrublý a často aj absurdný, plný odkazov na ďalšie stránky a internetové vtipy, ktorým porozumejú len zasvätení.

Hacker: Termín s nejasnou definíciou, ktorý sa v kontextu Anonymous používa k označeniu ľudí, ktorí sa vďaka technickým znalostiam dokážu nabúravať do počítačových sietí (pozri tiež heslá black hat a white hat). V širšom slova zmysle môžu označovať tiež počítačových nadšencov alebo programátorov, ktorí sa radi šťúrajú v interných systémoch a vymýšľajú rôzne zlepšováky alebo nové systémy.

Hacktivista: Zložením slova „hacker" a „aktivista" odkazujúcich na niekoho, kto sa pomocou elektronických nástrojov snaží šíriť politické, alebo sociologické posolstvo. Hacktivisti môžu siahať po rôznych metódach, pričom medzi tie menej legálne patrí DDoS útoky, hanobenie webových stránok či zverejňovanie utajených údajov.

IP adresa: Unikátne číslo priradené každému zariadeniu, ktoré sa pripojí k počítačovej sieti, alebo k internetu. Každá IP adresa pozostáva zo štyroch čísiel (až trinásťciferných) oddelených bodkami. IP je skratka pre „internetový protokol".

IRC (Internet Relay Chat): Pravdepodobne najrozšírenejší spôsob komunikácie medzi priaznivcami Anonymous, existujúci už od konca 80. rokov minulého storočia. IRC chaty, na rozdiel od obrázkových fór, umožňujú užívateľom komunikovať pomocou textových správ v reálnom čase. Diskusie sa odohrávajú v chatovacích miestnostiach, alebo „kanáloch". Každá IRC sieť združuje komunity so spoločnými záujmami, napríklad na IRC sieti AnonOps sa schádzajú ľudia, zaujímajúci sa o Anonymous. Diskusie v chatovacích miestnostiach moderujú „operátori" jednotlivých sietí a kanálov, pričom úloha operátora býva chápaná ako užívateľ vyššieho postavenia.

LOIC (nízkoorbitálny iontový kanón): Open source aplikácia pôvodne vytvorená k zaťažovému testovaniu serverov. medzi praiznivcami Anonymous sa ale preslávila ako elktronická zbraň, ktorú je možné použiť k prevádzaniu DDoS útokov – avšak za predpokladu, že ju bude používať dosť ľudí naraz.

Lulz: Pozmenený variant známej internetovej skratky LOL („laugh out loud" – hlasito sa rehotať). Má sa za to, že v tejto podobe sa poprvý krát objavila v roku 2003 na nejakom IRC chate v reakcii na čosi obzvlášť vtipného. Dnes označuje pobavenie, ktoré človek zažíva po vydarenom žarte alebo internetovej vylomenine na cudzí účet. Skrátka baviť sa na cudzí účet.

LulzSec: Skupina hackerov, ktorí sa v lete 2011 odštiepili od Anonymous a podnikli celý rad cielenejších, vysoko medializovaných útokov proti spoločnostiam ako SONY alebo americkým vládnym agentúram ako FBI. Skupina, ktorú založili hacktivisti známi pod prezývkami Topiary a Sabu, mala šesť ústredných členov a premenlivý okruh zhruba desiatich až dvadsiatich vedľajších spolupracovníkov.

Lurker: Návštevník webovej stránky, IRC chatu alebo internetového fóra ako 4chan, ktorý si prehliada diskusie, ale sám neprispieva, často kvôli tomu, aby si vopred osvojil miestnu kultúru a nevyčnieval z davu ako nováčik. Na niektorých IRC sieťach môžu byť lurkeri, ktorí sa nikdy nezapoja do diskusie, považovaní za nežiadúcich.

Mem: Povedačka, alebo obrázok, ktorému sa vďaka virálnej povahe internetu dostalo neočakávanej popularity a význam ktorého nezasväteným užívateľom internetu spravidla uniká. Mnohé memy, napríklad „over9000"

(cez 9000) alebo „delicious cake" (lahodná torta) pramenia zo starých počítačových hier alebo sa vyvinuli v /b/ a medzi priaznivcami Anonymous sa často pretriasajú ako interné vtipy. ďalšie príklady: rickrollovanie alebo pedomáďa (Pedobear).

Morálbuzna (moralfag): Nálepka prisudzovaná tým užívateľom 4chanu alebo stúpencom Anonymous, ktorí po morálnej stránke nesúhlasia s určitým príspevkom, obrázkom, metódou trollovania, nápadom, raidom alebo aktivitou. Obvykle chápané ako hanlivý termín.

Novobuzna (newfag): Návštevník sekcie /b/ na fóre 4chan, ktorý je buď nový, alebo stále nepochopil zvyklosti komunity.

Obrázkové fórum (imageboard): Internetové diskusné fórum s vágnymi pravidlami, na ktorom užívatelia často pro podtrhnutie svojich kometárov používajú obrázky. Obrázkové fóra, ktorým sa hovorí „chany", sa ľahko vytvárajú a udržujú. Niektoré z nich sa špecializujú na konkrétne témy, napríklad 420chan je známy ako priestor k diskusiám o drogách.

OP: Skratka pre „original poster", voľne preložené ako „zakladateľ diskusie. Ide o osobu, ktorá na internetovom fóre zahájila určitú diskusiu. V kultúre 4chanu sa zakladateľom vždy hovorí „buzna".

Pastebin: Jednoduchá, avšak nesmierne populárna webová stránka, na ktorej môže ktokoľvek ukladať a zverejňovať texty. V posledných troch rokoch si ju obľúbili priaznivci Anonymous, ktorí ju používajú k publikovaniu ukradnutých údajov,napríklad dôverných e-mailov alebo hesiel vytiahnutých z webových databáz. Skupina LulzSec, ktorá sa odštiepila od hlavného prúdu Anonymous, používala Pastebin k vydávaniu tlačových správ počas svojej ehackerskej spanilej jazdy v lete roku 2011.

Pravidlá internetu: Zoznam 47 „pravidiel", ktoré podľa všetkého vznikli pri jednom rozhovere na IRC chate v roku 2006 a z ktorých pochádza aj motto Anonymous: „Neodpúšťame, nezabúdame". Pravidlá sa zaoberajú spoločenskými zvyklosťami na obrázkových fórach, ako je 4chan, a zároveň upozorňujú na to, čo má človek od internetových komunít očakávať – napríklad absenciu žien.

Raid: V doslovnom prekalde „nájazď". Raid je slovo, ktorým sa v komunite Anonymous a 4chane označujú koordinované útoky, spravidla organizované verejne v diskusnej sekcii /b/. V raidoch obvykle nejde o nič iného ako užiť si trochu zábavy na cudzí účet a raid pritom nemusí byť nutne hackerský útok – často ide len o žarty typu premaľovania fotografií alebo spamovanie konkurenčných fór obrázkami.

Server: Počítač, ktorý ostatným počítačom v sieti sprostredkováva prístup k centralizovaným zdrojom alebo službám.

Shell: Softwarové rozhranie, ktoré číta a vykonáva príkazy. U špatne zabezpečených webových stránok sa hacker môže skrz administračný ovládací panel dostať až k shellu servera, na ktorom sú stránky hosťované, a jeho prostredníctvom potom server ovládať.

Skript: relatívne jednoduchý počítačový program. Skripty sa často používajú k automatizácii rôznych úkonov.

Skripťáčik (script kiddie): Hanlivý termín označujúci niekoho, kto by sa rád považoval za black hat hackera, ale zatiaľ k napádaniu počítačových sietí používa len prefláknuté a voľne dostupné webové nástroje alebo skripty. Skripťáčkovia sa mnohokrát prostredníctvom hackovania chcú vydobyť viac rešpektu medzi kamarátmi.

Sociálne inžinierstvo: Klamanie či komunikácia pod falošnou identitou alebo nepravdivou zámienkou s cieľom vytiahnuť z obete informácie.

SQL injekcia: Tento termín, niekedy tiež skracovaný ako SQLi, označuje metódu útoku, pri ktorej hacker získa prístup do databázi zraniteľných stránok tým, že jej podsunie podvodný príkaz. Tento príkaz sa často dá poslať cez bežný webový formulár dostupný aj normálnym užívateľom. Pomocou tohto postupu môže hacker získať aj informácie, ktoré mali radovým užívateľom zostať skryté.

Starobuzna (oldfag): Návštevník /b/, ktorý už rozumie zvyklostiam komunity, spravidla v´daka tomu, že 4chan navštevuje už niekoľko rokov.

Troll: Človek, ktorý na internete anonymne zosmiešňuje alebo obťažuje inú osobu alebo skupinu, veľmi často zanechávaním provokatívnych komentárov na internetových fórach, vzácnejšie potom nabúravaním sa do účtov na sociálnych sieťach. „Trollovanie" ale môže znamenať aj zosnovávanie úmyselných klamstiev. Tak či onak je konečným cieľom rozhnevať alebo zosmiešniť.

VPN (virtuálna súkromná sieť): Sieťová technológia, ktorá cez internet poskytuje vzdialený a bezpečný prístup k sieti prostredníctvom procesu nazývaného „tunelovanie". Veľmi veľa organizácií používa VPN tomu, aby ich zamestnanci mohli pracovať z domova a zároveň sa bezpečne pripojovať k centrálnej firemnej sieti. Hackeri a priaznivci Anonymous však VPN siete používajú k maskovaniu svojich IP adries, aby ich nemohla vypátrať polícia alebo ostatní členovia komunity.

White Hat: *White hats*, po slovensky „biele klobúky", sú hackeri, ktorí sa síce dokážu nabúrať do počítačovej siete a ukradnúť informácie, avšak tieto svoje znalosti používajú len k tomu, aby firmám a webovým stránkam pomohli lepšie sa zabezpečiť.

Zhanobenie webovej stránky: Tu používame k označeniu útoku, kedy sa hacker nabúra na cudzie stránky a zverejní na nich obrázok s textom, ktorý oznamuje dôvod, prečo boli stránky napadnuté.

PRÍLOHA – ČASOVÁ OS[30]

5 novembra 1994 – V jednom z prvých známych prípadov hacktivizmu a internetovej neposlušnosti poriada skupina nazývaná Zippies DDoS útok na vládne stránky Veľkej Británie a počínajúc dňom Guya Fawkesa ich na týždeň vyradili z prevádzky.

1999 – Rodí sa hnutie Anti-security. Príspevok na stránkach anti.security.is vyzýva k ukončeniu praxe úplného zverejňovania známych bezpečnostných slabín webových stránok.

29 septembra 2003 – Christoper „mooť" Pole si registruje doménu 4chan.net (teraz prístupné na 4chan.org).

15 marca 2006 – Dvadsaťročný Jake Brahm posiela na 4chan fiktívne vyhrážky, podľa ktorých sa chystá odpáliť bomby na štadiónoch ligy amerického futbalu NFL. O dva roky neskôr je odsúdený k šiestim mesiacom väzenia.

12 júla 2006 – Užívatelia 4chanovej sekcie /b/ poriadajú raid na Habbo Hotel, virtuálny priestor, kde sa radi stretávajú tínedžéri. /b/ tardi sa do internetovej hry húfne hrnú s avatarmi černocha v šedom obleku a s afro účesom, zablokujú prístup k virtuálnemu bazénu a zoskupujú sa do hákových krížov. Tu sa rodí mem „bazén je uzatvorený".

január 2007 – Kontroverzný blogger a rozhlasový moderátor Hal Turner sa neúspešne pokúša žalovať používateľov 4chanu v reakcii na to, že sekcia /b/ usporiadal DDoS útok na jeho webové stránky.

7 júna 2007 – Partyvan zakladá stránku /i/ nsurgency (povstanie), ktorá slúži ako informačné stredisko o raidoch. Neskôr tu bude založená komunikačná IRC sieť Partyvan.

júl 2007 – Losangeleská pobočka Fox News popisuje Anonymous ako „hackerov na steroidoch" a „internetový stroj na nenávisť".

---

[30] P. Olsonová, op. cit., s. 431.

15 januára 2008 – Gawker zverejňuje video Toma Cruisa, ktoré sa Scientologická cirkev dovtedy snažila držať pod pokrievkou. Cirkev reaguje žalobou na YouTube za porušovanie autorských práv. V odpovedi na to, vyzýva zakladateľka diskusie na /b/ k tomu, aby 4chan „urobil niečo veľkého" a vyradil z prevádzky oficiálne stránky scientológov. Užívateľom /b/ sa s pomocou webového nástroja Gigaloader skutočne podarí zablokovať stránky Scientology.org a s prestávkami ich udržať mimo prevádzku až do 25. januára.

21 januára 2008 – Niekoľko účastníkov projektu Chanológia vystavuje na YouTube video, v ktorom robotický hlas vyhlasuje scientológom vojnu. Nasledujúceho dňa sa na IRC kanály, kde sa prejednávajú útoky Chanológie, hrnú tisícky nových ľudí.

24 januára 2008 – Anonymous zahajujú rozsiahly útok proti stránkam Scientology.org a vyraďujú ich z prevádzky.

10 februára 2008 – Sympatizanti Anonymous si nasadzujú masky s filmu V ako Vendetta a demonštrujú pred scientologickými strediskami vo veľkých mestách celého sveta, napríklad v New Yorku, Londýne, alebo v texaskom Dallase.

záver roka 2008 – Demonštrácie a počítačové útoky voči scientológom postupne odumierajú, pretože priaznivci pomaly strácajú záujem.

25 januára 2010 – Priaznivec Anonymous a vysokoškolský študent Brian Mettenbrink sa priznáva k stiahnutiu webového nástroja LOIC a jeho použitiu k útoku proti scientológom v rámci projektu Chanológia. Je odsúdený k jednému roku odňatia slobody.

17 septembra 2010 – Podporovatelia Anonymous zahajujú DDoS útok proti indickej softwarovej spoločnosti Aiplev, ktorá sa priznala k vlastným DDoS útokom na bittorentový portál The Pirate Bay. Anonymous následne pod záštitou operácie Odplata usporiadajú niekoľko ďalších útokov proti rozličným spoločnostiam brániacim autorské práva. Účastníci sa koordinujú na niekoľkých IRC sietiach.

október 2010 – FBI začína prešetrovať útoky Anonymous na spoločnosti chrániacej autorské práva, čo časom prerastie v plnohodnotné medzinárodné vyšetrovanie.

3 novembra 2010 – Priaznivci Anonymous disponujú vlastnými servermi zakladajú IRC sieť AnonOps, ktorá slúži ako stabilnejší chatovací priestor pre diskusie o operácii Odplata a ďalších akciách Anonymous.

28 novembra 2010 – Pätica svetových denníkov začína publikovať uniknuté americké depeše, ktoré im exkluzívne poskytla whistleblowerská organizácia WikiLeaks. V priebehu nasledujúcich dní zaháji hacktivista menom The Jester DDoS útok proti stránke WikiLeaks.org a vyradí ju z prevádzky.

3 decembra 2010 – Gigant internetových platieb PayPal na svojom blogu oznamuje, že sa rozhodol zmraziť účet organizácie WikiLeaks, ktorá pritom závisí na dobrovoľných príspevkoch. Onedlho potom, organizátori z kanálu #command na sieti AnonOps usporiadajú DDoS útok proti blogu PayPalu.

4 decembra 2010 – Oznámenie, vyvesené na Anonops.net dáva na vedomie, že Anonymous sa chystajú zaútočiť na „rôzne ciele súvisejúce s cenzúrou" a že operácia Odplata sa „na znamenie podpory WikiLeaks opäť rozbehla".

6 decembra 2010 – Organizátori z AnonOps zahajujú DDoS útok proti postFinance.ch, švajčiarskej spoločnosti sprostredkujúcej elektronické platby, ktorá taktiež zamedzila posielanie príspevkov pre WiliLeaks. Do chatovacej miestnosti #OperationPayback na AnonOps sa pripojuje zhruba 900 ľudí, z ktorých asi 500 sa pridá k útoku pomocou nízkoorbitálneho kanónu LOIC.

8 decembra 2010 – AnonOps poriada DDoS útok proti stránkam PayPal.com. Zapája sa síce 5400 dobrovoľníkov, avšak útok sa podarí až vo chvíli, kedy jeden človek disponujúci botnetom úplne vyradí stránky z prevádzky. Medzitým sa počet návštevníkov kanálu #OperationPayback rozrastie na 7800. Neskôr toho dňa zaútočí skupina na stránky MasterCard.com a Visa.com, ktorých materské spoločnosti taktiež odstrihli financovanie WikiLeaks, a obidve ich asi na dvanásť hodín vyradia z prevádzky.

9 decembra 2010 – Majitelia botnetov, ktorí doteraz pomáhali úročiť na ciele ako PayPal.com, MasterCard.com, alebo Visa.com, sa obracajú proti operátorom AnonOps a začínajú na túto IRC sieť útočiť, čím zmaria útok proti Amazonu, ktorý bol na tento deň naplánovaný.

11 decembra 2010 – Devätnásťročný mladík menom Martijn „Awinee" Gonlag je zatknutý holandskou políciou za používanie LOIC k účasti na DDoS útokoch Anonymous. Ide o jedno z prvých zatknutí, ktoré budú v Európe aj v Spojených štátoch amerických v priebehu ďalšieho roka nasledovať.

15 decembra 2010 – istý zamestnanec PayPalu zodpovedný za elektronické zabezpečenie predáva FBI prenosný USB flash disk obsahujúci IP adresy tisícov osôb, ktoré použili LOIC k útoku na PayPal.

polovica decembra 2010 – Administrátori AnonOps majú plné ruky práce s údržbou, nakoľko na ich sieť niekto permanentne útočí a nezostáva im žiadny čas na koordinovanie stratégie. V dôsledku toho sa operácie Odplata roztriešti do niekoľkých postranných operácií, napríklad operácie Leakspin, operácia OverLoad alebo útoku na oficiálne stránky Sarah Palinovej.

polovica decembra 2010 – Hŕstka technicky zdatných sympatizantov Anonymous zakladá súkromný IRC kanál mimo sieť AnonOps a pomenuje ho #InternetFeds. Schádza sa tu zhruba tridsiatka „black hat hackerov" – napríklad Sabu, Tflow, Kayla a ďalší zainteresovaní Anonovia, ktorí boli do kanálu pozvaní – a spoločne preberajú budúce operácie.

začiatok januára 2011 – Hackeri z #InternetFeds uvažujú o raidoch proti vládnym webovým stránkam z Blízkeho východu, napríklad Tuniska, kde práve zúri ľudové povstanie. Hacker menom Tflow vytvára webový skript, ktorý Tunisanom umožňuje obísť štátne sledovanie internetu, a Sabu pre zmenu napadá stránky tuniského premiéra a hanobí ju odkazom od Anonymous.

druhá polovica januára 2011 – Členovia #InternetFeds naďalej spolupracujú na hackovaní a hanobení webových stránok ďalších blízkovýchodných vlád, napríklad alžírskej alebo egyptskej.

27 januára 2011 – Britská polícia v spojitosti s útokmi operácie Odplata proti spoločnostiam PayPal, MasterCard a Visa zatýka päť mužov. Sú medzi nimi aj operátori siete AnonOps prezývaní Nerdo a Fennic.

4 februára 2011 – Malá skupinka hackerov a z #InternetFeds sa stretáva na inom súkromnom IRC kanáli a prejednáva útok na bezpečnostnú firmu HBGary Federal. Jej výkonný riaditeľ sa o niekoľko hodín skôr nechal v denníku The Financial Times počuť, že prešetruje uskupenie Anonymous a že už odhalil skutočné identity jeho ústredných vodcov.

6 februára 2011 – Média informujú o tom, že Anonymous ukradli desiatky tisíc firemných e-mailov Aarona Bara a dvoch vedúcich zamestnancov zo sesterskej spoločnosti HBGary Incorporated. Zároveň prevzali kontrolu nad jeho twitterovým účtom, vyradili jeho stránky z prevádzky a následne ich zhanobili.

prvá polovica februára 2011 – Tá istá skupina členov #InternetFeds zverejňuje súkromné e-maily Aarona Barra v špecializovanom prehliadači e-mailov. Novinári a priaznivci tak zisťujú, že Barr navrhoval kontroverzné počítačové útoky na WikiLeaks a odporcom Americkej obchodnej komory. Barr skladá funkciu.

24 februára 2011 – Anonymous v priamom prenose hackujú a hanobia webové stránky baptistického zboru vo Westbore, zatiaľ čo priaznivec Anonymous menom Topiary sa stretáva zo zástupkyňou westborského zboru v rozhlasovom vysielaní. Záznam programu umiestnený na YouTube časom zaznamená viac ako milión zhliadnutí.

druhá polovica februára 2011 – Jennifer Emicková, niekdajšia podporovateľka Chanológie a novo bojovníčka proti Anonymous, sa rozhodne vypátrať skutočné identity kľúčových hackerov a priaznivcov Anonymous. Podarí sa jej objaviť informácie o Sabuovi, občianskym menom Hectorovi Montsegurovi.

polovica marca 2011 – Emicková spolu s niekoľkými kolegami publikuje menom bezpečnostnej spoločnosti Backtrace zoznam sedemdesiatich mien vrátane Monsegurovho. Čoskoro potom, ju kontaktuje FBI.

1 apríla 2011 – priaznivci Anonymous zverejňujú digitálny letáčik oznamujúci vojnu proti spoločnosti Sony. Ide o reakciu na to, že Sony zažalovala hackera menom George „Geohotz" Hotz. Anonymous pokračujú DDoS útokom na stránky Sony a sieť PlayStation Network, čím značne popudia hráčsku komunitu.

7 apríla 2011 – Topiary a Sabu sa bavia o tom, že by sa oddelili od Anonymous, a nakoniec sa rozhodnú dať opäť dohromady tím zodpovedný za útok na HBGary a rozbehnúť ďalšie raidy. K Topiarymu zo Sabuom sa pridávajú hackeri Tflow a Kayla, spolu s nimi i ďalší priaznivec Anonymous s menom AVunit a neskôr aj írsky hacker menom Pwnsauce. Týchto šesť členov zakladá odštiepeneckú skupinu, ktorá sa nenechá viazať ani tými najmiernejšími zásadami Anonymous – napríklad tou o neútočení na mediálne spoločnosti. Skupinu nazývajú LulzSec a začínajú na významných webových stránkach pátrať po bezpečnostných skulinách, vďaka ktorým by „rooteri" ako Sabu alebo Kayla mohli následne ukradnúť údaje a zverejniť ich.

2 mája 2011 – Sony oznamuje, že v polovici apríla neznámi útočníci prenikli na jej sieť a získali prístup k osobným aj finančným údajom viac ako 75 miliónov užívateľských účtov PlayStation Network. Aj keď sa

Anonymous k zodpovednosti neprihlásili, Sony neskôr tvrdí, že hackeri po sebe zanechali súbor obsahujúci slová „Anonymous" a „Sme légia".

7 mája 2011 – Hackeri z LulzSecu prostredníctvom svojho nového twitterového účtu @lulzsec oznamujú, že sa im podarilo hacknúť stránky Fox.com a zverejnili utajovanú databázu potenciálnych účastníkov televíznej súťaže X Factor.

9 mája 2011 – Istý bývalý operátor AnonOps sa obracia proti svojím niekdajším kolegom a zverejňuje zoznam 653 užívateľských mien a IP adries, ktoré sa – ak neboli chránené VPN sieťou alebo proxy serverom – dajú použiť k identifikácii užívateľov.

30 mája 2011 – Po tom, čo televízna stanica PBS vo svojom programe NewsHour odvysiela dokument o WikiLeaks, hackeri z LulzSec sa nabúravajú do ich počítačovej siete s odôvodnením, že sa im dokument neľúbil. Následne zverejňujú zoznam e-mailových adries a hesiel zamestnancov PBS a Topiary naviac na webových stránkach NewsHour publikuje fiktívny spravodajský článok, podľa ktorého bol zavraždený rapper Tupac Shakur objavený živý a zdravý. Zakladatelia skupiny začínajú uvažovať o založení vonkajšieho okruhu dôveryhodných pomocníkov. Z veľkej časti má ísť o hackerov, ktorých Sabu pozná z minulosti.

2 júna 2011 – LulzSec oznamuje svoj hack stránok SonyPictures.com a tvrdí, že sa mu podarilo získať osobné účty viac ako miliónov užívateľov.

3 júna 2011 – LulzSec hanobí stránky spoločnosti Atlanta Infra-Grand, ktorá spolupracuje s FBI, a zverejňuje zoznam e-mailov a hesiel celkom 180 užívateľov. Figurujú medzi nimi aj agent FBI.

6 júna 2011 – LulzSec dostávajú dar vo výške 400 bitcoinov, čo pri vtedajšom kurze činilo 7800 amerických dolárov.

7 júna 2011 – Dvaja agenti FBi navštevujú Hectora „Sabua" Monsegura v jeho newyorskom byte a hrozia mu dvojročným väzením za krádeže údajov o kreditných kartách, pokiaľ s nimi nezačne spolupracovať. Monsegur súhlasí, že sa stane informátorom, a naďalej pokračuje v riadení LulzSecu.

8 júna 2011 – Členovia LulzSecu si všímajú, že Sabu sa už viac ako jeden deň nepripojil k internetu a začínajú sa obávať, že sa stal obeťou razie FBI. Neskôr tej noci (britského času) sa Topiarymu konečne podarí spojiť sa so Sabuom, ktorý tvrdí, že mu zomrela babička a že sa teraz na niekoľko dní nebude môcť LulzSecu venovať.

15 júna 2011 – LulzSec sa hlási k zodpovednosti za DDoS útok proti oficiálnej stránke CIA. Útok vykonal bývalý operátor AnonOps a zároveň botmaster menom Ryan, ktorý je teraz priaznivcom LulzSecu.

16 júna 2011 – Zástupcovia WikiLeaks kontaktujú Topiaryho a nechávajú sa počuť, že dva ich ústredná organizátori by si radi pohovorili s LulzSecom. Topiary zo Sabuom sa neskôr na IRC chate stretávajú s jedným zástupcom WikiLeaks a ďalšou osobou, ktorá sa označuje za Juliana Assangeho. Zástupca „potvrdí" Assangeho identitu tým, že na YouTube dočasne nahrá video, ktoré v reálnom čase zaberá obrazovku počítača s ich chatovou konverzáciou, následne sa pootočí a zaberie Assngeho sediaceho u svojho notebooku. Skupina rozoberá možnosť prípadnej spolupráce.

19 júna 2011 – LulzSec vydáva tlačovú správu, v ktorej sa snaží podnietiť znovuzrodenie hnutia Anti-Security (AntiSec) a v ktorom obhajuje počítačové útoky proti webovým stránkam vlád a ich agentúr.

20 júna 2011 – Ryan, uchvátený prekvapivo veľkou odozvou na výzvu k oživeniu hnutia Antisec, používa svoj botnet k DDoS útoku proti niekoľkým významným webovým stránkam vrátane britskej Agentúry pre závažný organizovaný zločin. Neskôr toho istého dňa, o 22:30 britského času, ho v jeho dome zatýka polícia.

23 júna 2011 – LulzSec zverejňuje citlivé dokumenty ukradnuté arizonskej polícii, v ktorých sa objavujú aj mená aj adresy celej rady policajtov. Niektorí členovia LulzSecu ako Topiary či Tflow majú dojem, že tentokrát zašli príliš ďaleko, a bavia sa o možnom rozpustení skupiny.

24 júna 2011 – Topiary s Tflowom oznamujú Avunitovi a Sabuovi, že by chceli ukončiť LulzSec. Rozbieha sa vášnivá hádka.

26 júna 2011 – LulzSec oznamuje, že po „50 dňoch lulz" ukončuje svoje aktivity.

18 júla 2011 – LulzSec sa vracia, aby previedol ešte jeden posledný hack. Tentokrát na domovskú stránku popredného britského bulvárneho denníka The Sun vyvesuje vyfabulovaný článok o smrti jeho vlastníka a majiteľa skupiny News International, Ruperta Murdocha.

19 júla 2011 – Britská polícia oznamuje zatknutie šestnásťročného mladíka, ktorý je podľa nej hackerom z LulzSecu známym pod prezývkou Tflow.

27 júla 2011 – Polícia zatýka obyvateľa Shetlandských ostrovov Jakea Davisa, ktorého podozrieva z toho, že pod menom Topiary vystupoval v LulzSecu.

2 septembra 2011 – Britská polícia zatýka dvadsaťštyriročného Ryana Ackroyda, ktorý údajne mal byť Kayla.

24 decembra 2011 – Zoskupenie Anonymous ohlasuje, že sa mu podarilo ukradnúť tisícky e-mailov a ďalších dôverných údajov americkej bezpečnostnej a spravodajskej spoločnosti Stratfor. Akcia je opatrená nálepkou „Vianoce Lulz". Operáciu zo súkromných chatovacích kanálov sladuje Sabu, ktorý o sebe prehlasuje, že navzdory zatknutiu ostatných členov LulzSecu je sám ešte na slobode. Informácie o organizátoroch útoku predáva polícii.

6 marca 2012 – Médiá informujú o tom, že v uplynulých ôsmych mesiacoch Hector Monsegur pracoval ako informátor FBI a pomohol zhromaždiť dôkazy potrebné k obvineniu Jeremyho Hammonda z Chicaga a ďalších piatych ľudí spolupracujúcich s LulzSecom.

CITE THIS ARTICLE AS:

P. Rozemberg, *Hnutie Anonymous a informačná bezpečnosť*, „Kultura Bezpieczeństwa. Nauka – Praktyka – Refleksje", 2018, no 30, p. 210-244, DOI: 10.5604/01.3001.0012.5890.