Parmy Olson

Wij zijn Anonymous

Een inside verslag van de
beruchte hackersbeweging

BOEKERIJ

Voordat u dit boek leest

Namen

Het merendeel van de werkelijke namen en *nicknames* die in dit boek worden gebruikt, is echt, op een klein aantal na. Alle gefingeerde namen in dit boek hebben betrekking op 'William', een jongeman die in het Verenigd Koninkrijk woont en wiens nachtelijke streken en pogingen om mensen voor de gek te houden en te terroriseren ons een kijkje gunnen in de wereld van /b/, het populairste discussieforum op 4chan. Zijn naam en de namen van zijn slachtoffers zijn veranderd.

Bronnen

De meeste informatie en anekdotes in dit boek zijn rechtstreeks afkomstig uit interviews met mensen die een sleutelrol in het verhaal speelden, zoals Hector 'Sabu' Monsegur en Jake 'Topiary' Davis. Hackers staan er echter om bekend dat ze soms nicknames van anderen gebruiken in een poging hun identiteit te verhullen – of gewoon keihard liegen. Ik heb dan ook zo veel mogelijk geprobeerd de verhalen bevestigd te krijgen. Wat de persoonlijke anekdotes betreft – Sabu's ervaring met het preventief fouilleren door de NYPD bijvoorbeeld – heb ik aangegeven dat dit het verhaal is van de hackers zelf. Gedurende het jaar waarin ik onderzoek deed voor dit boek hebben bepaalde hackers zich betrouwbaarder betoond dan andere. Ook heb ik de getuigenis van bronnen die ik geloofwaardiger achtte, zwaarder laten wegen. Kanttekeningen bij de bronnen van belangrijke informatie, berichten uit de media en statistische gegevens zijn achter in dit boek te vinden.

Spelling

Om het verhaal zo leesbaar mogelijk te houden, heb ik de spelling en de grammatica in citaten afkomstig van chatlogs opgeschoond en gebruikt voor dialogen tussen de personages. Ook in gevallen waar ik mensen via Internet Relay Chat heb geïnterviewd, heb ik de spelling verbeterd. Soms, als door een bron woorden werden overgeslagen, heb ik de geïmpliceerde tekst tussen vierkante haken [ ] gezet.

Mensen

Enkele mensen die in dit boek voorkomen zijn boegbeelden van Anonymous, hoewel ze niet representatief zijn voor de beweging als geheel. Het is belangrijk om dat te herhalen: ze zijn niet representatief voor Anonymous als geheel. Bepaalde sleutelfiguren, zoals William of Sabu, zijn nogal opvliegend van aard, en als u over hun buitengewone belevenissen leest, zullen de verhalen over *social engineering,* het hacken van computers, het kraken van internetaccounts en de opkomst van de online-*disruptor* misschien meer voor u gaan leven dan wanneer alleen de technieken zouden worden beschreven. Er zijn bij Anonymous veel redelijke mensen betrokken die nooit met de politie in aaraking zijn geweest, zoals sommige personen in dit boek; mensen die ernaar streven om op legale wijze politiek activisme te bedrijven. Lees voor een andere kijk op Anonymous het werk van Gabriella Coleman, een academica die Anonymous al jarenlang volgt, en het boek van Gregg Housh en Barrett Brown over Anonymous, dat gepland staat voor 2012. Ook de documentaire *We Are Legion* van Brian Knappenberger geeft een goed beeld van het politiek activisme van Anonymous.

1

De raid

Op zondag 6 februari 2011 installeerden miljoenen Amerikanen zich op de bank met zakken nacho's en bier in plastic bekers ter voorbereiding op het belangrijkste sportevenement van het jaar: de Super Bowl. Terwijl de Green Bay Packers de Pittsburgh Steelers inmaakten, moest digitaal beveiligingsexpert Aaron Barr hulpeloos toekijken hoe zeven mensen die hij nooit had ontmoet zijn wereld op zijn kop zetten. Super Bowl Sunday was de dag waarop hij persoonlijk met Anonymous werd geconfronteerd.

Tegen het einde van dat weekend had het woord 'Anonymous' een nieuwe betekenis gekregen. De definitie in het woordenboek – 'zonder bekendmaking van de naam' – kon worden uitgebreid met de omschrijving van een onduidelijke, sinistere hackersgroep die vastbesloten was om vijanden van vrije informatie aan te vallen, met inbegrip van personen als Barr, een getrouwd man en vader van een tweeling, die de fout had gemaakt een poging te wagen erachter te komen wat Anonymous eigenlijk was.

Het feitelijke keerpunt was de lunch, met nog zes uur te gaan tot de aftrap van de Super Bowl. Terwijl Barr op de bank zat in de woonkamer van zijn huis in een buitenwijk van Washington DC, gemakkelijk gekleed in een T-shirt en jeans, merkte hij dat zijn iPhone, die hij in zijn zak had, al een half uur niet had gezoemd. Normaal gesproken kreeg hij elk kwartier wel een e-mail. Hij viste de telefoon uit zijn zak en tikte op de app om zijn berichten op te halen. Er verscheen een donkerblauw venster met drie woorden die zijn leven zouden veranderen: E-MAIL OPHALEN MISLUKT. De *e-mailclient* vroeg vervolgens het juiste wachtwoord in te geven. Barr ging naar de accountinstellingen en toetste zorgvuldig in: 'kibafo33'. Het werkte niet. Zijn berichten kwamen niet binnen.

Hij keek wezenloos naar het schermpje en werd een tintelend gevoel van angst gewaar toen hij besefte wat dit betekende. Nadat hij enkele uren eerder had gechat met Topiary, een hacker van Anonymous, was hij ervan

overtuigd geweest dat het gevaar was geweken. Iemand had zijn HBGary Federal-account gehackt; iemand die nu toegang had tot tienduizenden interne e-mails en hem had geblokkeerd. Het betekende dat iemand ergens geheimhoudingsclausules en gevoelige documenten had gezien die een multinationale bank, een gerespecteerde Amerikaans overheidsinstantie en zijn eigen bedrijf in diskrediet konden brengen.

Een voor een kwamen in zijn geest herinneringen bovendrijven aan specifieke geheime documenten en berichten; herinneringen die hem in golven van ziekmakende angst onderdompelden. Barr stormde de trap op naar zijn werkkamer en ging achter zijn laptop zitten. Hij probeerde in te loggen op zijn Facebook-account om met een hacker te spreken die hij kende, iemand die misschien in staat was om hem te helpen. Maar het netwerk waarop hij een paar honderd vrienden had, was geblokkeerd. Hij probeerde zijn Twitter-account met enkele honderden volgers. Niets. Vervolgens Yahoo!. Hetzelfde. Vrijwel al zijn webaccounts waren geblokkeerd, zelfs de online-*roleplayinggame* World of Warcraft. Barr sloeg zich in stilte voor zijn hoofd omdat hij voor elk account hetzelfde wachtwoord had gebruikt. Hij wierp een blik op zijn WiFi-router en zag de lichtjes druk knipperen. Mensen probeerden hem te overladen met internetverkeer in een poging zijn eigen netwerk nog verder binnen te dringen.

Hij boog zich naar voren en trok de stekker eruit. De lichtjes doofden.

Aaron Barr had een militaire achtergrond. Zijn brede schouders, het gitzwarte haar en de zware wenkbrauwen deden vermoeden dat zijn voorouders afkomstig waren uit het Middellandse Zeegebied. Na twee semesters op de universiteit had hij beseft dat leren niks voor hem was, waarna hij zich bij de Amerikaanse marine had aangemeld. Daar schopte hij het al snel tot *signals intelligence officer* (SIGINT) met een unieke specialisatie: het analyseren van informatie. Barr werd uitgezonden naar het buitenland. Hij zat vier jaar in Japan, drie jaar in Spanje en werd overal in Europa gedetacheerd, van Oekraïne tot Portugal en Italië. Hij werd gestationeerd op amfibie-landingsvaartuigen en kwam onder vuur te liggen in Kosovo, op het vasteland. Deze ervaring maakte hem verbitterd over het feit dat de oorlog soldaten gevoelloos maakte voor menselijk leven.

Na twaalf jaar bij de marine accepteerde hij een vaste baan bij defensiecontractor Northrop Grumman. Hij stak zich in het pak, begon zich op te werken en stichtte een gezin. In november 2009 greep hij zijn kans toen een beveiligingsconsultant genaamd Greg Hoglund hem vroeg of hij hem wilde helpen een nieuw bedrijf op te zetten. Hoglund was al eigenaar van een digitale beveiligingsorganisatie genaamd HBGary Inc. Met het oog op

Barrs militaire achtergrond en zijn kennis van cryptografie stelde Hoglund hem voor een zusterbedrijf op te zetten dat zich zou specialiseren in het leveren van diensten aan de Amerikaanse overheid. Het bedrijf zou HBGary Federal worden genoemd, en HBGary Inc. zou 10 procent bezitten. Barr greep deze kans om eigen baas te zijn met beide handen aan. Door vanuit huis te werken zou hij bovendien zijn vrouw en zijn twee kleine kinderen vaker zien.

In het begin beviel het werk hem uitstekend. In december 2009 kon hij drie nachten achtereen niet slapen omdat hij bezig was met ideeën voor nieuwe contracten. Rond half twee 's nachts kroop hij achter zijn computer om Hoglund een e-mail te sturen met een aantal voorstellen. Maar een jaar later hadden Barrs ideeën nog niets opgeleverd. Barr was wanhopig op zoek naar opdrachten, en hij hield het bedrijfje met drie werknemers in leven door het geven van socialemediatrainingen voor leidinggevenden, wat 25.000 dollar per keer opleverde. Dit waren geen lessen in het onderhouden van Facebook-vriendschappen, maar in het gebruik van socialenetwerksites zoals Facebook, LinkedIn en Twitter om informatie over mensen te verzamelen – als spionagemiddelen.

In oktober 2010 leek eindelijk de redding nabij. Barr begon gesprekken met Hunton & Williams, een advocatenfirma met klanten – waaronder de Amerikaanse Kamer van Koophandel en de Bank of America – die hulp nodig hadden bij het aanpakken van hun opponenten. Zo had WikiLeaks er bijvoorbeeld op gezinspeeld dat het over een schat aan vertrouwelijke informatie van de Bank of America beschikte. Barr en twee andere beveiligingsfirma's maakten powerpointpresentaties waarin onder meer werd voorgesteld om desinformatiecampagnes te beginnen om verslaggevers in diskrediet te brengen die WikiLeaks steunden en cyberaanvallen uit te voeren op de website van WikiLeaks. Barr had zijn nep-Facebook-profielen van stal gehaald en liet zien hoe hij de opponenten kon bespioneren. Als voorbeeld had hij 'vriendschap' gesloten met personeelsleden van Hunton & Williams zelf, wat hem in staat stelde informatie over hun privéleven te verzamelen. De advocatenfirma leek geïnteresseerd, maar in januari 2011 was er nog geen contract gesloten, en HBGary Federal had geld nodig.

Toen kwam Barr op een idee. In San Francisco zou een conferentie voor beveiligingsprofessionals worden gehouden die B-Sides heette. Als hij een lezing zou geven waarin hij onthulde hoe hij door te snuffelen in de sociale media nieuwe informatie over een geheimzinnig onderwerp boven tafel had weten te krijgen, zou hij plotseling heel geloofwaardig zijn en daardoor misschien zijn accounts kunnen binnenhalen.

Barr besloot dat er geen beter doelwit was dan Anonymous. Ongeveer een maand tevoren, in december 2010, hadden de nieuwsmedia bol gestaan van de verhalen over een grote en mysterieuze hackersgroep die een aanval op de websites van MasterCard, PayPal en Visa had uitgevoerd als vergeldingsactie voor het feit dat ze alle donaties aan WikiLeaks hadden geblokkeerd. WikiLeaks had eerder duizenden geheime diplomatieke berichten gepubliceerd, en de oprichter en hoofdredacteur, Julian Assange, was gearresteerd in het Verenigd Koninkrijk, ogenschijnlijk wegens seksuele intimidatie.

Het woord 'hackers' was berucht om zijn ambiguïteit. Het kon van alles betekenen, van enthousiaste programmeur tot cybercrimineel. Maar mensen van Anonymous – Anons – werden vaak 'hacktivisten' genoemd: militante hackers met een politieke boodschap. Ze waren van mening dat alle informatie gratis moest zijn, en als je het daar niet mee eens was, konden ze zomaar je website platleggen. Ze beweerden geen structuur of leiders te hebben. Ze beweerden bovendien geen groep te zijn, maar 'alles en niets'. De beste omschrijving leek 'soort' of 'collectief'. De weinige regels die ze hadden, deden denken aan de film *Fight Club:* praat niet over Anonymous, onthul nooit je ware identiteit en hack nooit de media, want die zouden wel eens een belangrijk bericht kunnen verspreiden. Door de anonimiteit was het natuurlijk gemakkelijker om af en toe illegale activiteiten te ontplooien, in te breken op servers, klantgegevens van een bedrijf te stelen of een website plat te leggen en vervolgens te *defacen* (de homepage te veranderen). Dingen waarvoor je zomaar een gevangenisstraf van tien jaar aan je broek kon krijgen. Maar de Anons leken zich daar niet druk om te maken. Ze waren machtig omdat ze met zovelen waren en ze plaatsten hun dreigende slogan op blogs, gehackte websites en overal waar ze maar konden:

We are Anonymous
We are Legion
We do not forgive
We do not forget
Expect us.

Op hun digitale flyers en berichten stond een logo van een man in kostuum met een vraagteken als hoofd, omringd door palmtakken – zoals in het symbool voor de Verenigde Naties –, vermoedelijk gebaseerd op het surrealistische schilderij van de man met de bolhoed en de appel van René Magrit-

te. Het ging vaak vergezeld van het boosaardig grijnzende masker van Guy Fawkes, de Londense revolutionair uit de film *V for Vendetta*, tegenwoordig het symbool van een gezichtloze rebellenmeute. Het was onmogelijk om te bepalen hoeveel aanhangers Anonymous had, maar het was duidelijk dat het niet om slechts tientallen of zelfs honderden mensen ging. In december 2010 hadden duizenden mensen uit de hele wereld de belangrijkste chatrooms bezocht om deel te nemen aan de aanvallen op PayPal. Daarbij bezochten duizenden gebruikers regelmatig aan Anonymous gerelateerde blogs en nieuwe sites als anonnews.org. Iedereen die ook maar iets met *cybersecurity* te maken had, sprak over Anonymous, hoewel niemand leek te weten wie deze mensen waren.

Barr was gefascineerd. Hij had gezien hoe de wereld deze mysterieuze beweging aandachtig gadesloeg. In de Verenigde Staten en Europa waren al tientallen meldingen geweest van invallen en arrestaties. Maar er was niemand veroordeeld en de leiders waren niet gevonden. Barr was ervan overtuigd dat hij het beter kon dan de FBI – misschien kon hij het Bureau zelfs helpen met zijn ervaring als socialemediasnuffelaar. Achter Anonymous aangaan was riskant, maar hij dacht dat als het collectief zich tegen hem zou keren, ze hooguit de website van HBGary Federal een paar uur plat zouden kunnen leggen – of maximaal een paar dagen.

Hij was begonnen als *lurker* op de online-chatrooms waar de aanhangers van Anonymous bijeenkwamen en bedacht een nickname. Eerst AnonCog, vervolgens CogAnon. Hij mengde zich in de discussies, gebruikte het jargon van de groep en deed alsof hij een jonge rekruut was die stond te popelen om een paar bedrijven omver te gooien. Ondertussen noteerde hij de nicknames van anderen in de chatroom. Het waren er honderden, maar hij besteedde vooral aandacht aan de frequente bezoekers en degenen die de meeste aandacht kregen. Hij hield ook in de gaten op welk tijdstip deze mensen de chatrooms verlieten. Vervolgens schakelde hij over naar Facebook. Barr had ondertussen verschillende nep-accounts op Facebook aangemaakt en zich 'bevriend' met tientallen mensen van vlees en bloed die openlijk beweerden Anonymous te steunen. Wanneer een van die vrienden, kort nadat een nickname de chatrooms van Anonymous had verlaten, plotseling actief werd op Facebook, nam Barr aan dat hij een match had.

Tegen het einde van januari legde hij de laatste hand aan een twintig pagina's tellend document met namen, beschrijvingen en contactinformatie van vermoedelijke aanhangers en leiders van Anonymous. Op 22 januari 2011 stuurde Barr een e-mail naar Hoglund, vicepresident Penny Leavy van

HBGary Inc. (tevens Hoglunds echtgenote) en zijn eigen assistent, Ted Vera, in verband met zijn lezing over Anonymous op B-Sides. Vooral de aandacht van de pers zou het praatje de moeite waard maken. Hij zou onder een valse naam ook een paar mensen van Anonymous op de hoogte brengen van het onderzoek, dat was uitgevoerd door de zogenaamde 'cybersecurity-expert' Aaron Barr.

'Dit wordt een hot item in de chatrooms van Anonymous, en de pers leest daar ook mee,' zei Barr tegen Hoglund en Leavy. Ergo, nog meer publiciteit. 'Maar,' zo voegde hij eraan toe, 'het maakt ons ook tot doelwit. Wat denken jullie ervan?'

Hoglunds antwoord was kort: 'Ik heb weinig zin om ge-DDOS'tte worden, maar stel dat het toch gebeurt, wat doen we dan? Hoe maken we daar gebruik van?' Hoglund had het over een *Distributed Denial of Service*-aanval, een situatie waarin een grote hoeveelheid computers gelijktijdig een website met zo veel data bombardeerde dat hij tijdelijk offline ging. Het was de populairste aanvalsstrategie van Anonymous – zoiets als iemand een blauw oog bezorgen; het zag er lelijk uit en het deed flink pijn, maar je ging er niet aan dood.

Barr besloot dat hij de pers maar beter vóór de lezing op de hoogte kon stellen. Hij nam contact op met Joseph Menn, een in San Francisco werkende verslaggever van de *Financial Times*, en bood hem een interview aan over de manier waarop zijn gegevens konden leiden tot meer arrestaties van 'grote spelers' binnen Anonymous. Hij gaf Menn een voorproefje van zijn bevindingen: van de meerdere honderden deelnemers aan de cyberaanvallen van Anonymous waren er maar ongeveer dertig doorlopend actief, terwijl slechts tien oudgedienden de meeste beslissingen namen. Barrs informatie en het verhaal over zijn onderzoek leken er voor het eerst op te wijzen dat Anonymous een hiërarchie was die bovendien niet zo 'anoniem' was als over het algemeen werd gedacht. De krant bracht het verhaal op vrijdag 4 februari met de kop 'Cyberactivisten Gewaarschuwd voor Arrestatie' en citeerde Barr.

Barrs hart maakte een sprongetje toen hij het artikel las, en hij zond Hoglund en Leavy een e-mail met in de onderwerpregel: 'Het verhaal begint echt vorm te krijgen.'

'We moeten dit op de voorpagina zetten en er wat tweets tegenaan gooien,' antwoordde Hoglund. '"HBGary Federal gaat de barricaden op als privé-inlichtingendienst." Woordgrapje.'

In de loop van de vrijdag hadden agenten van de FBI-afdeling e-crime het artikel gelezen. Ze namen contact op met Barr om te vragen of hij zijn

informatie met hen wilde delen. Hij stemde ermee in om hen de maandag erop te ontmoeten, de dag na de Super Bowl. Rond diezelfde tijd had een klein groepje hackers van Anonymous het verhaal ook gelezen.

Het waren drie mensen uit drie verschillende delen van de wereld, en ze waren uitgenodigd in een online-chatroom. Hun nicknames waren Topiary, Sabu en Kayla, en zeker twee van hen, Sabu en Topiary, spraken elkaar voor het eerst. De persoon die had hen uitgenodigd noemde zichzelf Tflow. Ook hij bevond zich in de chatroom. Niemand wist hoe de anderen in werkelijkheid heetten, hoe oud ze waren, waar ze zich bevonden of van welke kunne ze waren. Twee van hen, Topiary en Sabu, gebruikten hun nicknames pas sinds een maand of twee in de openbare chatrooms. Ze hadden van elkaar gehoord en wisten van elkaar dat ze in Anonymous geloofden. Dat was de kern van het verhaal.

Het was een 'gesloten' chatroom, wat betekende dat je er alleen op uitnodiging gebruik van kon maken. Het gesprek verliep in eerste instantie nogal stroef, maar binnen enkele minuten praatte iedereen met elkaar. Persoonlijkheden begonnen zichtbaar te worden. Sabu was assertief en onbezonnen, en hij gebruikte straattaal als '*yo*' en '*my brother*'. Geen van de anderen in de chatroom was ervan op de hoogte, maar hij was een geboren en getogen New Yorker van Puerto Ricaanse afkomst. Hij had als tiener geleerd hoe hij computers moest hacken. Ooit had hij de telefoonlijn van zijn familie zodanig gemanipuleerd dat ze gratis toegang kregen tot het internet. Gedurende de late jaren negentig had hij in hackersfora nog veel meer trucjes geleerd. Rond 2001 was de nickname Sabu ondergronds gegaan, maar nu, bijna tien jaar later, was hij terug. Sabu was de veteraan van de groep, een echte zwaargewicht.

Kayla was aardig en kinderlijk, maar enorm slim. Ze beweerde dat ze een meisje was en – desgevraagd – 16 jaar oud. Veel mensen gingen ervan uit dat het een leugen was. Hoewel Anonymous veel jonge hackers kende en veel vrouwelijke aanhangers had, waren maar weinig van die jonge hackers vrouwen. Hoe dan ook, als ze inderdaad loog, deed ze het met verve. Ze was spraakzaam en vertelde kleurrijke verhalen over haar privéleven: ze had een baan in een schoonheidssalon, paste op als bijverdienste en ging op vakantie in Spanje. Ze beweerde zelfs dat Kayla haar echte naam was, en iedereen die probeerde haar ware identiteit te achterhalen, kreeg een 'fuck you' voorgeschoteld. Paradoxaal genoeg was ze geobsedeerd door de privacy van haar computer. Ze typte nooit haar naam op haar netbook in voor het geval ze werd gekeylogged, ze had geen fysieke harde schijf en ze startte

op van een micro-SD-kaartje dat ze kon inslikken voor het geval de politie ooit voor de deur mocht staan. Er werd zelfs gefluisterd dat ze een mes in haar webcam had gestoken om te voorkomen dat iemand die haar pc overnam haar ongemerkt zou filmen.

Topiary was wat hacken betrof het minst ervaren van de groep. Hij bezat echter een ander talent om dat gemis goed te maken: zijn gevatheid. Topiary was stronteigenwijs en zat boordevol ideeën. Hij had gebruikgemaakt van zijn mooie praatjes om zich heel behendig een weg te banen naar de regionen waar de geheime plannen van het Anonymous-netwerk werden gemaakt. Terwijl anderen hun uiterste best moesten doen om aan de deur mee te luisteren, werd Topiary direct binnengevraagd. Ze waren hem zo gaan vertrouwen dat de netwerkbeheerders hem hadden gevraagd de officiële verklaringen van Anonymous te schrijven voor elke aanval op PayPal en MasterCard. Hij was bij toeval op zijn nickname gekomen. Een van zijn favoriete films was *Primer*, een lowbudgetproductie met tijdreizen als thema. Toen hij erachter kwam dat de regisseur aan een nieuwe film werkte met de titel *A Topiary,* vond hij dat een mooi woord. Hij was zich er niet van bewust dat 'topiary' zoveel betekende als 'gesnoeide sierheesters' of 'vormtuin'.

Tflow, de man die iedereen in de chatroom had uitgenodigd, was een ervaren programmeur. Hij had een vrij rustig karakter en hield zich strikt aan de gewoonte van Anonymous om nooit over jezelf te praten. Hij was al minstens vier maanden bij Anonymous, lang genoeg om de cultuur en de belangrijkste personen te leren kennen. Hij kende de communicatiekanalen en de hackers die de beweging steunden beter dan de meeste anderen. Hij kwam dan ook snel ter zake. Iemand moest iets doen aan die Aaron Barr en dat 'onderzoek' van hem. Barr had beweerd dat Anonymous leiders had, wat niet zo was. Dat betekende dat zijn onderzoek waarschijnlijk bagger was. Dan was er nog dat stukje uit de *Financial Times* waarin Barr stelde dat hij 'informatie over de belangrijkste leiders had verzameld, waaronder veel van hun echte namen, en dat ze konden worden gearresteerd als de politie ook over die gegevens beschikte.'

Dat laatste betekende een volgend probleem: als Barrs informatie wél correct was, konden de Anons in moeilijkheden raken. De groep begon plannen te maken. Eerst moesten ze de server waarop de website van HBGary Federal draaide scannen op kwetsbaarheden in de broncode. Als ze geluk hadden, vonden ze een lek dat gebruikt kon worden om het systeem over te nemen en Barrs website te vervangen door een groot logo van Anonymous en een schriftelijke waarschuwing om hun collectief met rust te laten.

Die middag googelde iemand 'Aaron Barr', met als resultaat een officiële bedrijfsfoto: naar achteren gekamd haar, een pak en een intense blik die recht in de lens keek. De leden van het groepje lachten toen ze de foto zagen. Hij zag er zo… serieus uit, bijna onschuldig. Sabu begon hbgaryfederal.com te scannen, op zoek naar een lek. Het bleek dat Barrs site op een publishingsysteem draaide dat door een externe ontwikkelaar was gebouwd en een enorme bug had. Bingo.

Hoewel HBGary Federal andere bedrijven hielp zich tegen cyberaanvallen te beschermen, was de eigen server kwetsbaar voor een eenvoudige aanvalsmethode die 'SQL-injectie' werd genoemd en op databases van webapplicaties was gericht. Databases behoorden tot de belangrijkste technologieën waarop het internet was gebouwd. Er werden wachtwoorden, zakelijke e-mails en een breed scala aan andere data in opgeslagen. Het gebruik van Structured Query Language (SQL, vaak foutief uitgesproken als 'sequel') was een populaire manier om je toegang te verschaffen tot informatie uit databases en die vervolgens te manipuleren. Een SQL-injectie was het invoeren van SQL-instructies in de server waarop de website stond om verborgen informatie op te halen. In feite werd de programmeertaal hierbij tegen zichzelf gebruikt. Het gevolg was dat de server ingevoerde tekens niet als tekst las, maar als instructies die moesten worden uitgevoerd. Soms kon dit worden gedaan door gewoon instructies in het zoekveld van een homepage in te typen. De truc was om het zoekveld of tekstvak te vinden waar het lek zat.

Dit kon een bedrijf kapotmaken. Als je DDOS'en vergeleek met een onverwachte stomp in je gezicht, was een SQL-injectie het ongemerkt verwijderen van iemands vitale organen terwijl hij sliep. De taal die daarvoor nodig was – een verzameling symbolen en sleutelwoorden als 'select', 'null' en 'union' – waren voor mensen als Topiary Chinees, maar Sabu en Kayla spraken het vloeiend.

Nu ze binnen waren, gingen de hackers op zoek naar de namen en wachtwoorden van mensen als Barr en Hoglund, die de servers van de site beheerden. Opnieuw bingo. Ze vonden een lijst met gebruikersnamen en wachtwoorden voor medewerkers van HBGary. Maar er was een struikelblok. De wachtwoorden waren gecodeerd – *gehasht* – met behulp van een standaardtechniek die MD5 heette. Als alle beheerderswachtwoorden lang en ingewikkeld waren, was het misschien niet mogelijk om ze te kraken en zou het uit zijn met de pret.

Sabu selecteerde drie *hashes,* lange reeksen van willekeurige getallen die correspondeerden met de wachtwoorden van Aaron Barr, Ted Vera en nog

een leidinggevende, genaamd Phil Wallisch. Hij nam aan dat ze erg lastig te kraken waren, en toen hij ze aan de anderen in het team gaf, verbaasde het hem niet dat niemand er iets mee kon. In een laatste wanhoopspoging uploaddde hij ze naar een forum voor wachtwoordkrakers dat populair was onder hackers: hashkiller.com. Binnen een paar uur waren alle drie de hashes gekraakt door willekeurige anonieme vrijwilligers. Een ervan zag er als volgt uit:

```
24036d5fe575fb46f48ffcd5d7aeeb5af: kibafo33
```

Rechts van de string, achter de dubbele punt, stond het wachtwoord van Aaron Barr. Toen ze op Google Apps kibafo33 intoetsten om toegang te krijgen tot Barrs e-mail van HBGary Federal, waren ze binnen. De groep kon zijn geluk niet op. Die vrijdagavond lazen ze mee terwijl een zich van geen kwaad bewuste Barr met zijn collega's mailde over het artikel in de *Financial Times*.

In een opwelling besloot een van hen te controleren of kibafo33 misschien nog voor iets anders werkte behalve Barrs e-mailaccount. Het was de moeite waard om het te proberen. Het was onvoorstelbaar, maar deze cybersecurity-specialist die onderzoek deed naar een explosief onderwerp als Anonymous, gebruikte dezelfde eenvoudig te kraken wachtwoorden voor vrijwel al zijn webaccounts, waaronder Twitter, Yahoo!, Flickr, Facebook en zelfs World of Warcraft. Dat betekende dat het tijd was voor onvervalste 'lulz'.

Lulz was een variatie op het acroniem 'lol' – 'laughing out loud' – dat de internetgemeenschap al sinds jaren achter grappig bedoelde uitspraken plakte. Lulz, een recentere toevoeging aan de 'webspraak', ging nog een stapje verder en betekende zoveel als vermaak op kosten van een ander. De FBI bellen met een onzinverhaal was lol. De FBI bellen en ze een SWAT-team naar het huis van Aaron Barr laten sturen, was lulz.

Ze besloten Barr niet direct aan te pakken, en ook niet de dag erop. Ze zouden hem in het weekend bespioneren en alle e-mails downloaden die hij ooit had verzonden of ontvangen sinds hij bij HBGary Federal was gaan werken. Maar er moest wel snel actie worden ondernomen. Ze begonnen de berichten door te spitten en lazen dat Barr de maandag erop een afspraak had met de FBI. Toen ze alles hadden wat ze konden vinden, besloten ze dat de hel zou losbarsten bij de aftrap op Super Bowl Sunday. Ze hadden nog zestig uur te gaan.

Die zaterdag begon voor Barr als elke andere. Terwijl hij tijdens het ontbijt met zijn gezin nietsvermoedend het nieuws las op zijn iPhone, verdiepte een zevenkoppig team van Anonymous zich in zijn e-mails, opgewonden over wat ze hadden ontdekt. Hun laatste ontdekking: Barrs eigen onderzoek naar Anonymous. Het was een PDF-document dat begon met een korte, heel behoorlijke uitleg van wat Anonymous was. Er werden websites opgesomd, er was een tijdlijn van recente cyberaanvallen en naast een overzicht van nicknames was een groot aantal reallife-namen en -adressen geplaatst. De namen Sabu, Topiary en Kayla stonden er niet bij. Aan het eind waren haastige notities gemaakt, zoals 'Mmxanon – staten… getto'. Het zag er onaf uit. Al snel beseften ze dat Barr gebruik had gemaakt van Facebook in een poging om echte mensen te identificeren. Zo te zien had hij geen flauw benul van waar hij mee bezig was en zou hij wel eens onschuldige mensen in de problemen kunnen brengen.

Ondertussen had Tflow Barrs e-mails naar zijn server gedownload. Hij wachtte ongeveer vijftien uur alvorens hij er een *torrent* voor aanmaakte. Dit kleine bestandje linkte naar een groter bestand op een externe hostcomputer, in dit geval die van HBGary. Het was een proces dat miljoenen mensen wereldwijd dagelijks gebruikten om illegale software, muziek en films te up- en downloaden. Tflow was van plan om zijn torrent op de populairste torrenttracker te plaatsen: The Pirate Bay. Dit betekende dat iedereen het zou kunnen downloaden en de meer dan 40.000 e-mails van Aaron Barr kon lezen.

Die ochtend, ongeveer dertig uur voor de aftrap, deed Barr een aantal checks op hbgaryfederal.com. Er was – zoals hij al had verwacht – meer verkeer dan anders. Niet omdat er meer legitieme bezoekers waren, maar omdat Anonymous was gestart met zijn DDOS-aanval. Hoewel dat niet het einde van de wereld betekende, meldde hij zich bij Facebook aan via zijn nepprofiel Julian Goodspeak om contact te zoeken met een van zijn aanspreekpunten bij Anonymous, een schijnbaar ouder type dat de nickname CommanderX gebruikte. Zijn onderzoek en de gesprekken met CommanderX hadden hem doen geloven dat de echte naam van de man 'Benjamin Spock de Vries' was, hoewel dat niet klopte. CommanderX, die er geen idee van had dat een groepje hackers inmiddels druk in de weer was met Barrs e-mails, reageerde op Barrs chatverzoek. Barr vroeg beleefd of CommanderX iets kon doen aan het extra verkeer op zijn server.

'Ik ben klaar met mijn onderzoek. Het is niet mijn bedoeling om jullie te beschadigen,' lichtte Barr toe. 'Mijn focus ligt op kwetsbaarheden van sociale media.' Barr bedoelde dat zijn onderzoek alleen maar probeerde aan te geven hoe organisaties konden worden geïnfiltreerd door informatie te

verzamelen via Facebook-, Twitter- en LinkedIn-profielen.

'Daar ga ik niet over,' zei CommanderX eerlijk. Hij had even naar de website van HBGary Federal gekeken en wees Barr erop dat die er in elk geval niet bepaald solide uitzag. 'Ik hoop dat je goed wordt betaald.'

Op zondagochtend, met nog elf uur te gaan tot de aftrap, had Tflow alle e-mails van Barr en de twee andere directeuren, Vera en Wallisch, verzameld. Het torrent-bestand was klaar voor publicatie. Nu werd het pas echt interessant: ze gingen Barr vertellen wat ze hadden gedaan. Om dit goed te spelen, zouden de hackers hem natuurlijk niet onmiddellijk het hele verhaal vertellen. Je had veel meer lulz als je eerst een tijdje met iemand speelde. Inmiddels hadden ze ontdekt dat Barr de nickname CogAnon gebruikte om met mensen in de chatrooms van Anonymous te praten en dat hij in Washington DC woonde.

'We hebben alles, van zijn social-securitynummer tot aan zijn carrière in het leger, zijn bevoegdheden,' zei Sabu tegen de anderen, 'en hoe vaak hij per dag schijt.'

Zondagochtend om ongeveer acht uur 's ochtends Eastern Standard Time besloten ze hem een beetje paranoïde te maken voorafgaand aan de aanval. Toen Barr als CogAnon op het chatnetwerk van AnonOps inlogde, stuurde Topiary hem een privébericht.

'Hallo,' zei Topiary.

'Hi,' antwoordde CogAnon.

In een andere chatvenster leverde Topiary doorlopend commentaar aan de andere Anons, die lachten om wat hij deed.

'Zeg dat je hem nodig hebt voor een nieuwe missie,' zei Sabu.

'Doe voorzichtig,' zei een ander. 'Hij mag geen nattigheid voelen.'

Topiary ging terug naar zijn gesprek met de beveiligingsspecialist en deed nog steeds alsof hij geloofde dat CogAnon een echte aanhanger van Anonymous was. 'We zoeken mensen voor een nieuwe operatie in de buurt van Washington. Interesse?'

Het duurde twintig seconden voordat Barr antwoordde. 'In principe wel. Hangt ervan af wat het is,' zei hij.

Topiary copypastte het antwoord naar de andere chatroom.

'Hahahahhaa,' toetste Sabu in.

'Moet je zien hoe die flikker probeert informatie van me te psyopsen,' zei Topiary, verwijzend naar de tactiek van psychologische oorlogvoering. Het woord flikker – *faggot* – werd in Anonymous zo royaal gebruikt dat het niet eens meer als een echte belediging werd gezien.

'Aan je host te zien, zit je in de buurt van ons doelwit,' zei Topiary tegen Barr.

In Washington DC hield Barr zijn adem in. 'Fysiek of virtueel?' typte hij terug, hoewel hij heel goed wist dat het virtueel was, maar hij wist niet wat hij anders moest zeggen. 'Eh ja… Ik zit in de buurt…' Hoe wisten ze eigenlijk dat hij in DC zat?

'Virtueel,' antwoordde Topiary. 'Alles staat al klaar.'

Topiary gaf het door aan de Anons. 'Ik lach me dood als hij daar een e-mail over gaat sturen,' zei hij.

Ze konden niet geloven wat ze lazen. 'WAT IS DIE GAST EEN ONWIJZE LUL,' riep Sabu uit.

'Laten we hem in zijn reet naaien,' antwoordde Topiary. Servers 'naaien' was een uitdrukking die werd gebruikt voor het hacken van een netwerk. Tflow maakte een nieuwe chatroom aan op het netwerk van Anonymous, noemde het #ophbgary en nodigde Topiary uit om mee te doen.

'Jongens,' meldde een hacker met de naam AVunit zich. 'Gebeurt dit echt? Want dit is vette shit.'

In het gesprek probeerde Barr behulpzaam te klinken. 'Ik kan over een paar uur in de stad zijn… afhankelijk van het verkeer lol.'

Topiary besloot hem nog wat verder op te fokken: 'Ons doelwit is een beveiligingsbedrijf,' zei hij.

Barrs maag draaide zich om. Oké, dus dit betekende dat Anonymous zijn pijlen daadwerkelijk op HBGary Federal had gericht. Hij opende zijn e-mailclient en typte snel een bericht naar andere managers van HBGary, onder wie Hoglund en Penny Leavy.

'We liggen nu echt onder vuur,' schreef hij. 'Ik bespreek het morgen met de FBI wanneer ik ze ontmoet.' Sabu en de anderen keken zwijgend toe hoe hij het bericht verzond.

Barr klikte weer in de chat met Topiary. 'Oké, laat het maar weten,' schreef hij. 'Ik weet alleen niet hoe ik jullie kan helpen.'

'Dat hangt ervan af,' zei Topiary. 'Wat voor vaardigheden heb je? We hebben informatie nodig over een beveiligingsbedrijf, ligatt.com.'

Barr slaakte een diepe zucht van verlichting. Ligatt deed hetzelfde soort werk als HBGary Federal, dus het zag er (voorlopig tenminste) naar uit dat het doelwit toch niet zijn bedrijf was.

'Ah, oké. Dat moet lukken,' antwoordde Barr bijna dankbaar. 'Het is alweer een tijdje geleden dat ik ze heb gecheckt. Iets specifieks?' Hij was blij dat hij iets kon doen wat HBGary uit de schijnwerpers hield, al was het maar gewoon het spelletje meespelen.

Er kwam geen antwoord.

Hij typte: 'Ik wist niet dat ze in DC zaten.'

Een minuut later voegde hij eraan toe, 'Man, ik zit hier mijn hersenen te pijnigen, maar ik kan me niet herinneren waarom ze een tijdje terug zo populair waren. Ik weet nog wel dat er een hoop weerstand tegen ze was.'

Niets.

'Ben je daar nog?' vroeg Barr.

Topiary was bezig de zaak te plannen met de anderen. Er was niet veel tijd meer, en hij moest de officiële Anonymous-verklaring schrijven die de homepage van hbgaryfederal.com zou gaan vervangen.

Ongeveer drie kwartier later antwoordde Topiary eindelijk. 'Sorry – blijf nog even hangen.'

'Oké,' schreef Barr.

Een paar uur later – ongeveer zes uur tot de aftrap van de Super Bowl – was het tijd voor de lunch. Barr zat in zijn woonkamer en staarde in angstige fascinatie naar zijn telefoon nadat hij had beseft dat hij niet meer bij zijn e-mail kon. Hij rende naar boven en probeerde contact te zoeken met CommanderX op Facebook, maar dat werkte ook niet. Toen hij zag dat zijn Twitter-account door iemand anders werd gebruikt, realiseerde hij zich hoe ernstig dit was – en hoe enorm pijnlijk het misschien kon worden.

Hij pakte de telefoon en belde Greg Hoglund en Penny Leavy om ze te laten weten wat er gaande was. Hij telefoneerde ook met zijn systeembeheerders, die zeiden dat ze contact op zouden nemen met Google om te proberen hbgaryfederal.com weer onder controle te krijgen. Maar ze konden niets aan de gestolen e-mails doen.

Om 14:45 uur kreeg Barr nog een bericht van Topiary: 'Oké, er gaat vandaag iets gebeuren. Ben je de hele avond beschikbaar?'

Er waren nog maar een paar uur te gaan, en hij wilde dat Barr op de eerste rang zat om het einde van zijn carrière te aanschouwen.

Terwijl aan de oostkust de zondagavond naderde, maakten de Anons zich in hun eigen huizen en tijdzones, verspreid over de wereld, op voor de aanval. Het Cowboys Stadium in Arlington, Texas, begon vol te lopen. De Black Eyed Peas speelden een paar nummers en Christina Aguilera gooide de woorden van het volkslied door elkaar. Ten slotte kwam de toss. Een speler van de Green Bay Packers haalde uit met zijn voet en trapte het varkensleer over het veld.

Aan de andere kant van de Atlantische Oceaan keek Topiary naar zijn laptop terwijl de voetbal door de lucht vloog. Hij zat in zijn zwarte leren

gamestoel en had een enorme koptelefoon op zijn hoofd. Hij opende een nieuw venster en meldde zich aan bij Barrs Twitter-account. Hij had Barr zes uur geleden afgesneden van het wachtwoord kibafo33, en nu de Super Bowl eindelijk was begonnen, besloot hij dat het tijd was om te gaan *posten*. Hij voelde geen remmingen en vond niet dat hij zich moest inhouden bij deze man. Hij zou Barr eens flink op zijn donder geven: 'Oké mede-Anonymous-flikkers,' schreef hij via Barrs Twitter-account, 'we zijn momenteel bezig het puikje van de lulz voor jullie te organiseren. Blijf hangen!'

En vervolgens: 'Sup, motherfuckers, ik ben directeur van een shitty bedrijfje en ik ben een gigantische kut van een mediahoer. LOL, check de site van mijn *nigga* Greg: rootkit.com.' Het waren uitspraken die Topiary nooit hardop zou hebben gedaan, of tegenover Barr. In het echte leven was hij rustig en beleefd en vloekte hij zelden.

Rootkit.com was van Hoglund. De website was gespecialiseerd in geavanceerd onderzoek naar softwaretools die volledige toegang gaven tot computernetwerken. Ironisch genoeg hadden Sabu en Kayla inmiddels ook roottoegang tot rootkit.com. Barr was namelijk beheerder van het e-mailsysteem waardoor ze met 'kibafo33' ook de wachtwoorden van andere inboxen hadden kunnen resetten – inclusief die van Hoglund.

Zodra hij in Hoglunds mailbox zat, stuurde Sabu een e-mail namens Hoglund naar een van HBGary's systeembeheerders, een Finse veiligheidsspecialist genaamd Jussi Jaakonaho. Sabu wilde roottoegang tot rootkit.com.

'ik zit in europa en heb ssh-toegang tot de server nodig,' schreef Sabu in zijn e-mail naar Jaakonaho. Hij gebruikte geen hoofdletters, hetgeen suggereerde dat hij haast had. SSH stond voor 'secure shell' en verwees naar een manier van inloggen op een server vanaf een externe locatie. Toen Jaakonaho vroeg of Hoglund (Sabu) achter een openbare computer zat, zei Hoglund (Sabu): 'nee ik heb het openbare ip-adres momenteel niet hier want ik heb zo een vergadering en ik heb haast. reset mijn wachtwoord anders maar naar changeme123 en geef me het ip-adres, dan ssh ik en reset ik mijn pw [password].'

'Oké,' antwoordde Jaakonaho. 'Je wachtwoord is changeme123.' Hij voegde er met een smiley aan toe: 'In Europa, maar niet in Finland?'

Sabu speelde het spelletje mee. 'als ik de tijd een beetje slim indeel, kunnen we misschien wat afspreken… ik zit eerst een tijdje in duitsland. bedankt.' Het wachtwoord werkte niet eens direct, en Sabu moest Jaakonaho nog een paar keer e-mailen met vragen, waaronder de vraag of zijn eigen

gebruikersnaam greg was, of…? Jaakonaho gaf aan dat het 'Hoglund' was. Sabu was binnen. Dit was een perfect voorbeeld van *social engineering* – de kunst om iemand zo te manipuleren dat hij geheime informatie weggaf of iets deed wat hij normaal gesproken nooit zou doen.

Nu hadden Sabu en Kayla de volledige controle over rootkit.com. Eerst logden ze in met de gebruikersnaam en het wachtwoord van iemand die zich ooit op de site had aangemeld en vervolgens verwijderden ze de complete inhoud. Er bleef alleen een lege pagina over waarop was te lezen: 'GREG HOGLUND = OWNED'. Sabu merkte dat hij het leuk vond om met Kayla samen te werken. Ze was vriendelijk en beschikte over uitzonderlijke technische vaardigheden. Sabu vertelde later aan anderen dat *zij* Jussi Jaakonaho de informatie had ontfutseld, mede omdat het idee dat een meid van zestien HBGary had *geowned* het bedrijf nog meer in verlegenheid zou brengen.

Sabu en Kayla gingen aan de slag met hbgaryfederal.com. Ze haalden de homepage weg en vervingen hem door het Anonymous-logo met de hoofdloze man in het pak. In plaats van het hoofd was er een vraagteken. Onderaan stond een link die meldde: 'Download HBGary's e-mails' – Tflows torrent-bestand. Het lezen van de vertrouwelijke e-mails die Barr aan zijn klanten had gestuurd, was nu even eenvoudig als een song downloaden van iTunes – maar dan gratis. Op de nieuwe homepage stond ook een verklaring die door Topiary was geschreven:

> *Dit domein is in beslag genomen door Anonymous op grond van artikel #14 van de Regels van het Internet. Beste HBGary (een computer'beveiligings'-bedrijf). Jullie recente claims met betrekking tot het 'infiltreren' van Anonymous vinden we amusant, evenals jullie pogingen om Anonymous in te zetten als middel om de aandacht van de pers op jullie te vestigen. Wat dachten jullie van déze aandacht? Als je in de hand van Anonymous bijt, kun je een mep in je gezicht verwachten.*

Om 18:45 uur Eastern Standard Time, 24 minuten na de aftrap van de Super Bowl, was het hacken grotendeels achter de rug. In de verte klonk geen gejuich en gejoel van buren die naar de wedstrijd keken – het waren grotendeels jonge gezinnen. De wereld om Barr heen leek vreemd stil. Met enige schroom logde hij opnieuw in de chatroom van Anonymous in om de confrontatie met zijn aanvallers aan te gaan. Ze zaten al op hem te wachten. Barr zag een berichtje verschijnen, een uitnodiging voor een nieuwe chatroom met de naam #ophbgary. Hij zag een lijstje met meerdere nick-

names. Sommige herkende hij van zijn onderzoek en andere waren nieuw. Behalve Topiary, Sabu en Kayla zag hij Q, Heyguise, BarrettBrown en cos. De laatste nick was Gregg Housh, een oudgediende Anon halverwege de dertig die had geholpen bij de coördinatie van de eerste golf van grote DDOS-aanvallen door Anonymous in 2008 tegen de Scientology Church (COS).

Topiary was de eerste die iets zei. 'Nu bedreigen ze ons rechtstreeks,' zei hij tegen Barr, de eerdere e-mail citerend. 'Heb ik gelijk?'

Barr reageerde niet.

'Ik hoop dat je naar de Super Bowl zit te kijken,' zei Q.

'Hallo, Mr. Barr,' zei Tflow. 'Sorry voor wat er met u en uw bedrijf gaat gebeuren.'

Eindelijk reageerde Barr. 'Ik dacht al dat er zoiets aan zat te komen,' typte hij.

'Je gaat dit niet fijn vinden,' zei Topiary.

Barr probeerde de aanwezigen ervan te overtuigen dat hij het beste met ze voorhad. '*Dude*… je snapt het gewoon niet,' protesteerde hij. 'Ik heb onderzoek gedaan naar kwetsbaarheden van sociale media. Ik ben nooit van plan geweest om jullie namen openbaar te maken.'

'LEUGENAAR.' Dat was Sabu. 'Had je maandagochtend geen afspraak met de FBI?'

'Zeker weten, Sabu,' zei Topiary.

'Oké… Klopt,' bekende Barr. 'Ze hebben me gebeld.'

'Jawel, mensen. Daar komt de kers op de taart,' zei Topiary.

Het was aan Tflow om de bom te laten barsten.

'Ik heb de e-mails van Barr, Ted en Phil,' zei hij. 'Alle 68.000.'

'Dat wordt lachen,' zei Housh.

'Lol,' antwoordde Barr om onverklaarbare reden. Hij leek het gesprek luchtig te willen houden, of hij wilde zichzelf ervan overtuigen dat het allemaal wel mee zou vallen. 'Oké mensen,' voegde hij eraan toe, 'jullie hebben me te pakken :).'

Dat hadden ze inderdaad. Topiary bracht zijn afscheidsgroet. 'Nou Aaron, bedankt voor je deelname aan dit onderzoekje om te zien of je het "nieuws" over Anon aan je bedrijf zou doorspelen. Dat heb je inderdaad gedaan, wij hebben het *geleecht* en we hebben erom gelachen.' Hij zweeg even. 'Krijg de tering. Je bent de lul.'

Het was nu in de vroege uurtjes van de maandagochtend. Barr zat thuis op zijn kantoor achter de laptop. Zijn hoop op een verbetering van de situatie

was inmiddels gedaald tot het nulpunt. Aan de muur tegenover hem hing een foto die hij in oktober 2011 in New York had gekocht. De herinneringen aan de aanslagen van 11 september waren nog vers, en na een bezoek aan Ground Zero was hij een kleine galerie binnen gegaan waar amateurfoto's werden verkocht die tijdens de aanslagen waren gemaakt. Eén foto sprong eruit. Op de achtergrond was de chaos van de ingestorte wolkenkrabbers: overal papier en steen, en verdwaasde forenzen onder het stof. In het midden stond *Double Check* van John Seward Johnson, het beroemde bronzen beeld van een zakenman in kostuum die op een bankje in het park zat en in zijn geopende aktetas keek. Iets in de ongerijmdheid ervan bekoorde hem. Nu was Barr die man, zo verstrikt in zijn ambities dat hij zich niet bewust was van de chaos om zich heen.

Zijn openbare Twitterfeed – een tool die belangrijk was voor zijn naam bij het publiek, zijn klanten en de pers – was nu een obscene zwijnenstal. Topiary had tientallen tweets met scheldwoorden en racistische opmerkingen geplaatst. In zijn bio stond nu: 'CEO HBGary Federal. Cyberveiligheid en Information Operations Specialist en ONWIJS HOMOGAY.' Op zijn foto was met dikke rode kliederletters het woord 'nigger' geschreven. Topiary vond zichzelf geen racist – niemand in zijn groep vond dat. De graffiti was perfect in harmonie met de undergroundcultuur van rauwe humor en cyberpesten die als een rode draad door Anonymous liep.

Topiary voelde iets van verrukking toen hij Barrs huisadres postte. Hij twitterde Barrs social-securitynummer en vervolgens het nummer van zijn mobiele telefoon. Iedereen met een internetverbinding kon dit lezen. 'Hé, mensen, laat een voicemail achter!' Toen het nummer. Ten slotte: '#belme.'

Al snel wisten honderden en vervolgens duizenden mensen die de chatrooms, blogs en Twitterfeeds van Anonymous afstruinden wat er met Aaron Barr was gebeurd. Ze klikten op links naar Barrs website, die nu een wit scherm was met het logo en de verklaring van Anonymous. Ze lazen de Twitterfeeds en belden zijn nummer. Diverse mensen sloopten zijn nette profielfoto of knipten het hoofd uit en plakten het op een poster van een James Bond-film om de draak te steken met Barrs spionagetactieken. Iemand blies zijn kin op waardoor hij op een groteske karikatuur leek uit de bekende *rage comic* 'Forever Alone'.

Barr was er niet in geslaagd zich los te maken van de chatroom, gebiologeerd als hij was door mensen die grapjes maakten over de 'flikker' Barr en elkaar aanmoedigden zijn mobiele nummer te bellen. Zijn telefoon ging de hele nacht. Hij nam een keer op en hoorde een vrouwenstem iets onver-

staanbaars zeggen en ophangen. Er waren een paar geluidloze voicemails en iemand die iets zong wat klonk als 'Never Gonna Give You Up', een nummer van Rick Astley uit 1987. Het was een hommage aan een populaire grap onder aanhangers van Anonymous: iemand *rickrollen*.

Barr had om versterking gebeld. Penny Leavy was online gegaan in een poging de Anons stroop om de mond te smeren. Ze waren in eerste instantie vriendelijk en beleefd tegen haar, maar haar verzoeken werden met kille antwoorden tegemoet getreden.

'Zet alsjeblieft de e-mails van HBGary niet online,' had ze gesmeekt. 'Er staat privé-informatie van klanten in.'

'Dan moet je maar geen e-mails versturen die je moeder niet mag lezen,' had Heyguise gezegd. Daarbij was er al een torrent voor de e-mails op The Pirate Bay gezet.

'Er hadden tientallen onschuldige mensen naar de gevangenis kunnen gaan,' zei Sabu boos. Vóór hun aanval had de nieuw gevormde clique van Anons – die elkaar te midden van honderden anderen in het chatnetwerk van Anonymous had gevonden – er geen idee van gehad dat Barrs onderzoek zo vol fouten zat of dat zijn e-mails zo eenvoudig konden worden gehackt. Ze hadden niet eens geweten dat Barr een overheidsinstelling en een grote bank een voorstel had gedaan om een smerige campagne tegen de vakbonden en WikiLeaks te gaan voeren. Ze waren gemotiveerd door wraak en een verlangen, dat versterkt werd door de psychologie van de groep, om iemand die het kennelijk verdiende op zijn lazer te geven. Zodra genoeg mensen Barrs e-mails hadden doorgespit en erachter waren wat hij Hunton & Williams had geflikt, zou de aanval plotseling meer dan gerechtvaardigd lijken en voor hen misschien zelfs noodzakelijk. Binnen de gemeenschap van Anonymous zouden Sabu, Kayla, Topiary en de anderen heldhaftige verspreiders worden van vigilante rechtvaardigheid. Barr was een terecht mikpunt geweest. Hij had een wereld getart waar treiteren, liegen en stelen de normaalste zaak van de wereld waren. Een wereld die euforische hoogtepunten, lol en voldoening bracht, eigenlijk zonder dat daar in de echte wereld consequenties aan waren verbonden.

Terwijl Barr de volgende dag besteedde aan het pareren van telefoontjes van journalisten en wanhopige pogingen om de brokken te lijmen, ontmoetten Topiary, Sabu, Kayla en Tflow elkaar opnieuw in hun geheime chatroom. Ze vierden hun succes, bespraken wat er gebeurd was, lachten en voelden zich onoverwinnelijk. Ze hadden een beveiligingsbedrijf geowned. Ergens wisten ze dat agenten van het Federal Bureau of Investigation naar ze op zoek zouden gaan. Maar later zouden de leden van het kleine

team tot de conclusie komen dat ze bij Barr zo goed hadden samengewerkt dat ze ermee door moesten gaan en andere doelen moesten aanvallen – voor de lulz, voor Anonymous en voor eventuele andere goede zaken die zich aandienden. Geen prooi zou te groot zijn: een groot mediabedrijf, een entertainmentreus en zelfs de FBI.