BRIAN KREBS

NAȚIUNEA SPAM

Din culisele criminalității informatice

Traducere din limba engleză
DAN DRUMUR

Prefață
EUGEN GLĂVAN

CORINT BOOKS
2019

CUPRINS

Capitolul 1

PARAZIT

BMW-ul 760 bleumarin s-a oprit la o trecere de pietoni semaforizată din centrul Moscovei. Un Porsche Cayenne negru s-a oprit alături. Era duminică, 2 septembrie 2007, ora 14, iar străzile, în mod obișnuit aglomerate, din apropierea faimoasei Piețe Suharevskaia erau aproape lipsite de trafic, cu excepția turiștilor și a localnicilor care se plimbau pe trotuarele late de pe ambele părți ale bulevardului. Soarele după-amiezii, care încălzise străzile pe tot parcursul zilei, începea să proiecteze pe stradă umbrele lungi ale clădirilor istorice din apropiere.

Șoferul BMW-ului, un escroc local notoriu, cunoscut ca hacker sub pseudonimul „Jaks", devenise tată în ziua aceea și, împreună cu pasagerul, băuse o cantitate impresionantă de votcă în cinstea nou-născutului. Era momentul și locul perfect pentru tranșarea unei rivalități mocnite cu șoferul automobilului Porsche: trebuia să afle care dintre mașini e mai rapidă. Ambii șoferi au ambalat motoarele într-o înțelegere nerostită de a se întrece pe distanța scurtă care-i despărțea de piața mare aflată chiar în față.

Când s-a aprins lumina verde a semaforului, scârțâiturile produse de cauciucuri pe beton s-au auzit la sute de metri depărtare în Suharevskaia. Pietonii s-au întors să vadă automobilele performante care au țâșnit din intersecție unul lângă celălalt și au atins o viteză amețitoare.

Trecând cu peste 200 km/h de mijlocul distanței, Jaks a pierdut deodată controlul volanului, a atins cealaltă mașină și a intrat într-un uriaș stâlp metalic de iluminat. Într-o clipă, întrecerea s-a sfârșit fără niciun învingător. BMW-ul era rupt în două, iar Porsche-ul, făcut ferfeniță, ardea mocnit în apropiere. Ambii șoferi s-au îndepărtat șchiopătând de locul accidentului, dar pasagerul din BMW – Nikolai McColo, o tânără speranță a Internetului în vârstă de 23 de ani – a murit pe loc, aproape decapitat, prins sub mașina de lux.

„Kolea", așa cum îi spuneau prietenii, era o mică celebritate în lumea subterană a criminalității informatice, cel mai tânăr angajat al firmei de familie McColo Corp., care furniza servicii de găzduire web. Într-un moment în care autoritățile din toată lumea începeau să-și dea seama de pericolele de ordin financiar și organizațional ale criminalității informatice, McColo Corp. devenise cunoscută drept unul dintre centrele acesteia: un loc în care escrocii de pe internet își puteau începe afacerile fără să se teamă că investițiile și planurile lor on-line vor fi descoperite sau puse în pericol de diverse autorități străine.

În momentul morții lui Kolea, serverele familiei sale găzduiau cele mai mari afaceri din lume implicate în distribuirea de e-mailuri nesolicitate sau „spam" prin intermediul rețelelor automate. Aceste rețele, denumite „botneturi", sunt grupuri de computere personale care au fost piratate și în care a fost instalat software rău intenționat – „malware" – ce le permite atacatorilor să controleze de la distanță sistemele respective. De obicei, proprietarii nu au habar că acele computere sunt controlate de altcineva.

Aproape toate botneturile controlate de McColo erau create pentru a distribui reclamele nedorite care ne umplu zilnic conturile de e-mail și suprasolicită filtrele antispam. Serverele lui McColo nu generau și nu pompau ele însele spam – acest lucru ar fi atras atenția așa-zișilor gardieni ai internetului

și poliției din țările occidentale. Ele erau folosite doar de afacerile botmaster pentru a manipula milioane de computere de pe întreg globul și a le transforma în zombi distribuitori de spam.

În timp ce personalul de pe ambulanță termina de curățat zona accidentului, imagini groaznice ale carnajului erau încărcate pe forumuri de internet obscure din Rusia, frecventate de prietenii și clienții lui McColo. Printre primele care au difuzat știrea morții lui Kolea s-a aflat Crutop.nu, un forum rusesc de hackeri, care număra între cei 8 000 de membri ai săi pe unii dintre cei mai importanți spammeri din lume. Membrii Crutop.nu care au difuzat poze și informații despre eveniment erau unii dintre cei mai buni clienți ai lui McColo; mulți s-au simțit obligați (iar dacă n-au făcut-o, li s-a bătut obrazul în mod public de către administratorii forumurilor) să ajute cu bani familia lui Kolea pentru organizarea funeraliilor. Înmormântarea acestuia a fost un eveniment important în lumea subterană a criminalității informatice.

Câteva zile mai târziu, membrii comunității pestrițe a spammerilor din Moscova s-au adunat pentru a-i aduce un ultim omagiu. Ceremonia a avut loc în aceeași biserică în care Kolea fusese botezat cu aproape 23 de ani în urmă. Printre cei prezenți s-au numărat Igor „Desp" Gusev și Dmitri „SaintD" Stupin, administratori ai SpamIt și GlavMed, până de curând cei mai mari sponsori de spam* din lume și două personaje ce vor juca un rol-cheie în această carte.

La înmormântare a participat și hackerul Dmitri „Gugle" Necivolod, pe atunci în vârstă de 25 de ani, care avea o legătură strânsă cu botnetul Cutwail, un monstru care a infectat zeci de milioane de calculatoare din întreaga lume și

* Ar trebui amintit că Gusev a negat în mod public faptul că a difuzat spam și s-a ocupat de SpamIt, deși n-a făcut acest lucru în discuțiile pe care le-am avut cu el.

le-a folosit pentru a distribui spam. Necivolod câștigase deja milioane de dolari folosind botnetul pentru a trimite e-mailuri nesolicitate în beneficiul GlavMed și SpamIt către milioane de persoane din întreaga lume. În prezent, Cutwail a rămas unul dintre cele mai mari și mai active botneturi de spam – deși acum este administrat cu siguranță de mai multe persoane (despre acest lucru, a se vedea capitolul 7, „Să-i cunoaștem pe spammeri").

De ce trebuie să amintim de prezența acestor trei indivizi la un eveniment atât de important pentru criminalitatea informatică? Fiindcă activitatea lor (asemenea celei a lui Kolea și a sute de alți indivizi) ne afectează zi de zi într-un mod bizar, dar semnificativ: spamul.

Spamul a devenit impulsul principal al dezvoltării de malware – programe care ne atacă zilnic calculatoarele și care vizează identitatea, siguranța, banii, familiile și prietenii noștri. Aceste botneturi sunt paraziți virtuali care trebuie îngrijiți și hrăniți în mod constant pentru a rămâne cu un pas înaintea antivirușilor și a firmelor de securitate care încearcă să le distrugă. Pentru ca aceste colonii de PC-uri controlate să prospere, spammerii (sau botmasterii – termenii sunt sinonimi) trebuie să răspândească și să modifice în permanență erorile digitale cu care se hrănesc. Deoarece antivirușii curăță în mod regulat calculatoarele infectate, folosite pentru expedierea de spam, operatorii botneturilor trebuie să atace continuu, să capete controlul asupra unor computere noi și să creeze alte modalități de infiltrare în cele infectate anterior.

Această cursă a înarmării tehnologice necesită dezvoltarea, producerea și distribuirea de malware tot mai greu detectabil, care să poată scăpa de antivirușii și instrumentele antispam care evoluează la rândul lor. Hackerii aflați în spatele acestor botneturi gigantice folosesc spamul și ca o formă de autoapărare. Aceleași botneturi care difuzează spam învechit sunt

utilizate pentru a distribui e-mailuri nesolicitate care conțin versiuni noi de malware, ajutând la răspândirea infecției. Spammerii reinvestesc adesea câștigurile obținute din spam în crearea de malware mai bun, mai puternic, mai bine disimulat, în stare să evite antivirușii, programele antispam și firewallurile. Ecosistemul spam este o mașinărie infracțională tehnico-socială în continuă evoluție, care se autoalimentează.

Deocamdată, răufăcătorii care au dezlănțuit această molimă digitală reușesc să fie net superiori industriei de securitate. Companiile antivirus informează că se străduiesc să clasifice și să combată în *medie 82 000 de noi variante de malware care atacă zilnic computerele*, iar un procent important din aceste tulpini este menit să transforme computerele infectate în zombi de spam, care pot fi apoi controlați de la distanță de atacator. Cei de la McAfee, marele producător de programe de securitate, au declarat că au detectat 14 milioane de malwareuri noi numai în primul trimestru al anului 2013.

Desigur însă că toate astea au un preț și pentru spammeri. În cazul lui Cutwail, întreținerea rețelei presupune existența unor echipe de dezvoltatori de software și de personal tehnic care lucrează 24 de ore pe zi, 7 zile pe săptămână. Asta se datorează faptului că programul care pune în mișcare botneturi de felul lui Cutwail este în mod obișnuit închiriat de alți spammeri, care solicită frecvent modificări ale codului sau add-onuri capabile să ajute programele bot să funcționeze corespunzător în infrastructura lor infracțională.

Abia trecut de 30 de ani, moscovitul Igor Vișnevski a fost unul dintre cei câțiva hackeri care au avut o colaborare strânsă cu Necivolod la Cutwail. (Vișnevski a pornit în cele din urmă pe cont propriu, creând o versiune rivală a lui Cutwail, pe care obișnuia de asemenea s-o utilizeze pentru spam și s-o închirieze altor spammeri. A acceptat să fie pentru noi un fel de

Vergiliu* virtual și să ne conducă prin această ciudată și nefamiliară lume subterană a spammerilor, motiv pentru care este menționat în toată cartea.) „Am avut un birou pentru Gugle [Necivolod, pronunțat asemenea cuvântului englezesc «Google»], cu programatori și personal de asistență tehnică. Uneori treceam pe acolo, dar n-am lucrat de acolo", își amintea Vișnevski într-o conversație pe chat. Spunea că biroul lui Gugle avea minimum cinci programatori cu normă întreagă și tot atâția oameni care se ocupau cu asistența tehnică. Aceștia lucrau non-stop, în ture, inclusiv în weekend, pentru a răspunde cât mai bine cerințelor clienților.

Firme de găzduire precum McColo au atras clienți ca producătorii lui Cutwail deoarece au rămas on-line în ciuda presiunilor semnificative exercitate de autoritățile interne și externe în vederea suprimării siteurilor dubioase sau ilicite pe care le găzduiau. Potrivit lui Vișnevski, serverele lui McColo erau bine cunoscute pentru viteza lor constantă și pentru că erau „bulletproof" (blindate), adică imune la cererile de închidere depuse de alți furnizori de servicii de internet (ISP) sau de autorități străine.

La scurt timp după moartea lui Kolea, McColo s-a grăbit să asigure comunitatea criminalității informatice că, deși cel mai cunoscut membru al companiei murise, aceasta avea să-și continue activitatea ca până atunci. Partenerul lui Kolea, Aleksei, a răspândit mesajul pe mai multe forumuri frecventate de infractorii informatici, încercând să-i asigure pe clienții companiei că neplăcutul eveniment nu va duce la întreruperea serviciului.

Comunitatea criminalității informatice nu trebuia convinsă ca să rămână. Serviciul era găzduit mai ales în SUA și era ieftin, fiabil și rapid. În anul care a urmat morții lui Nikolai, Necivolod

* Aluzie la faptul că, în celebrul poem al lui Dante, *Divina Comedie*, marele poet roman Vergiliu apare drept călăuză a autorului în infern și purgatoriu (n. red.).

și majoritatea principalilor botmasteri de spam aveau să-și păstreze la McColo serverele folosite la controlul botneturilor.

Asta până în seara zilei de 11 noiembrie 2008, când un reportaj apărut în *Washington Post* despre concentrarea masivă de activități rău intenționate la furnizorul de servicii de găzduire i-a determinat pe cei doi furnizori ai conexiunii McColo la internet să decupleze simultan compania. Într-o clipă, volumul de spam a scăzut cu până la 75% în toată lumea, deoarece milioane de boți de spam au fost deconectați de la serverele lor și împrăștiați în cele patru colțuri ale lumii ca niște oi lipsite de păstor.

Închiderea lui McColo a lovit direct la buzunar botmasteri ca Necivolod și Vișnevski. Spammerii care închiriau botneturi au asaltat cu plângeri Crutop.nu și alte forumuri dedicate fraudelor, arătând că au pierdut sume substanțiale și vrând să știe ce măsuri se vor lua.

„În cazul McColo, aveam servere din SUA care posedau o viteză bună, își amintea Vișnevski. Când McColo a fost închisă, a trebuit să închiriem servere mult mai lente din China și alte țări care sunt praf" în ceea ce privește capacitatea de a face față unor plângeri privind abuzurile.

Dornici să demonstreze că puțini credeau că McColo va dispărea vreodată – chiar și după moartea lui Kolea – mulți spammeri au păstrat direct pe serverele companiei o altă componentă majoră și costisitoare a operațiunilor lor: liste imense cu adrese de e-mail.

„Toți și-au pierdut listele acolo", a spus Vișnevski, subliniind că, după închiderea lui McColo, el și Necivolod au pierdut o listă foarte mare și valoroasă, cu peste două miliarde de adrese de e-mail.

Moartea lui Kolea și desființarea lui McColo au fost momente hotărâtoare, deoarece au însemnat începutul sfârșitului unei ere în care spammerilor și baronilor crimei informatice li

se îngăduise să opereze într-o siguranță relativă. Pe vremea aceea, peste 90% din totalul e-mailurilor trimise în întreaga lume erau nesolicitate, iar majoritatea făceau reclamă unor presupuse siteuri farmaceutice. În următorii patru ani, închiderea altor ISP-uri ilicite, furnizori de găzduire web și mari botneturi de spam avea să reducă masiv volumul de e-mail nesolicitat și să coincidă cu arestarea sau condamnarea la închisoare a câtorva spammeri de marcă.

Desființarea companiei McColo a reprezentat de asemenea începutul unei noi ere a spamului, prin declanșarea unui îndelungat și costisitor conflict pentru supremație pe care îl vom analiza în această carte. „Războiul farma", așa cum i-au spus cei din lumea criminalității informatice și a securității informatice, a irupt sub forma unei încleștări sălbatice între doi dintre cei mai mari sponsori ai spamului farmaceutic – care a prins la mijloc utilizatori ca mine și ca dumneavoastră, care nu au bănuit nimic.

De o parte s-au aflat Dmitri Stupin și Igor Gusev, menționați mai înainte, și operațiunile lor farmaceutice, GlavMed și SpamIt. De cealaltă parte s-a aflat Rx-Promotion, o afacere farmaceutică ilicită de pe internet, inițiată de fostul partener de afaceri al lui Gusev, moscovitul de 35 de ani Pavel Vrublevski. În mod oficial, Vrublevski era directorul executiv al companiei ChronoPay, una dintre cele mai mari firme rusești de procesare a plăților on-line, pe care acesta a fondat-o împreună cu Igor Gusev.

În secret, Vrublevski avusese legături strânse cu lumea subterană a criminalității informatice, ajutând tot soiul de tâlhari on-line să obțină procesarea cardurilor de credit pentru afacerile lor dubioase și încasând o parte însemnată din câștig. Tot Vrublevski este cofondatorul și administratorul popularului forum pentru spammeri Crutop.nu și o altă figură centrală a războaielor informatice care ne-au transformat în prezent într-o națiune a spamului – ba chiar într-o lume a spamului.

În 2010, cercetam deja de peste un an și scriam despre acuzațiile de corupție aduse lui Vrublevski, ca și despre presupusele sale legături cu spammerii care lucrau pentru programul farmaceutic ilicit Rx-Promotion, mai întâi ca reporter de investigații pentru *Washington Post* și apoi pentru propriul meu site de informații despre securitatea informatică, KrebsOnSecurity.com. Pe măsură ce am avansat însă, am vrut să aflu mai multe despre e-mailurile nesolicitate și despre problema securității informatice: cine o provoca și cum putea fi rezolvată. Era clar că și alții gândeau ca mine.

Înainte de războiul de uzură dintre baronii spamului pe care îl vom analiza în această carte, au existat surprinzător de puține informații publice sigure pentru a putea răspunde la întrebările esențiale referitoare la problema spamului, cum ar fi:

• Cine cumpără produsele promovate în e-mailurile nesolicitate, cum ar fi Viagra, medicamente care se eliberează pe bază de rețetă, chiar și poșete Gucci? Ce îi determină pe oameni să cumpere și să înghită niște pastile cărora le fac reclamă vânzători agresivi și necunoscuți?

• Sunt aceste medicamente reale sau sunt falsuri ineficiente și, posibil, mortale?

• Cine profită de pe urma distribuirii spamului? Cum sunt împărțite profiturile și unde merg banii?

• De ce industria farmaceutică – una dintre cele mai bogate și mai influente din lume – este aparent neputincioasă în ceea ce privește oprirea hoției și a însușirii ilegale a produselor, mărcilor și clienților săi?

• De fapt, de ce este atât de ușor să plătești cu un card de credit aceste medicamente contrafăcute cărora li se face masiv reclamă prin spam?

• Conturile clienților care folosesc cardul de credit sunt sparte sau revândute după ce au cumpărat de la spammeri?

Capitolul 12

FINAL DE PARTIDĂ

În iunie 2011, Vrublevski a făcut a doua călătorie neprogramată în Maldive din anul acela. De data aceasta, a fugit din Moscova fiindcă fusese anunțat că procurorii pregăteau împotriva lui acuzații penale în legătură cu un atac informatic lansat în iulie 2010 asupra sistemelor companiei Aeroflot de vânzare a biletelor.

Anchetatorii îi arestaseră deja pe frații Igor și Dmitri Artimovici, care se pare că realizaseră și administraseră împreună botnetul Festi. Ambii au negat că ar fi administrat un botnet sau că ar fi expediat spam și au susținut că poliția rusă a pus dovezi în computerele lor. Procurorii ruși obținuseră o mărturisire semnată de Igor, în care acesta afirma că Vrublevski îl angajase ca să atace compania Assist, care procesa plăți pentru Aeroflot. În momentul atacului, ChronoPay se număra printre companiile care licitau pentru obținerea unui contract profitabil de procesare a plăților pentru Aeroflot, iar procurorii susțineau că atacul fusese menit să împiedice Assist să primească din nou contractul. În mod paradoxal, la o lună după atac, Aeroflot n-a acordat contractul niciuneia dintre cele două companii, ci lui Alfa Bank, cea mai mare bancă privată din Rusia.

Autoritățile ruse i-au reamintit lui Pavel că, în Maldive, putea fi arestat și de autoritățile americane sau de alte autorități naționale, așa că s-a întors de bunăvoie la Moscova.