BRIAN KREBS

NAȚIUNEA SPAM

Din culisele criminalității informatice

Traducere din limba engleză
DAN DRUMUR

Prefață
EUGEN GLĂVAN

CORINT BOOKS
2019

PREFAȚĂ

Fiecare epocă istorică are drept principală caracteristică mijlocul tehnologic dominant de comunicare și fiecare societate s-a clădit pe capacitatea de a produce cunoaștere. Capacitatea de a transmite informații populației și generațiilor viitoare a fundamentat constituirea civilizațiilor, iar manuscrisele care limitau cunoașterea la un cerc de inițiați au reprezentat primele forme de control al informației. Tiparul a generalizat accesul și a pus bazele alfabetizării. Fotografia a fixat imaginea, iar telefonul și radioul au purtat pe unde cuvântul și muzica. Televiziunea a integrat cuvântul, imaginea și sunetul, devenind mijlocul de comunicare specific în societățile moderne.

În prezent, internetul reprezintă modalitatea informațională și comunicațională predominantă la scară planetară, înglobând interacțiunea mediată în timp real. Toate aceste tehnologii au avut nevoie de timp pentru a fi acceptate în societate și au produs schimbări majore. Fiecare a generat câștigători și perdanți, legi și fărădelegi, eroi și tâlhari. Este momentul să facem cunoștință cu un aspect negativ al internetului, trimiterea de mesaje electronice nesolicitate sau spamul, care, în 2013, reprezenta 70% din volumul total de e-mailuri expediate zilnic.

Națiunea Spam este povestea unor personaje dubioase care, într-o societate permisivă și lipsită de capacitatea și

interesul de a impune legea, au elaborat planuri sofisticate de fraudare bazate pe e-mailurile nesolicitate. Bazându-se pe slăbiciunile sistemelor de operare ale computerelor, încălcând legi naționale sau exploatând zone insuficient de bine definite ale criminalității transfrontaliere, acești hoți informatici au creat programe informatice specializate, care, prin infectarea computerelor și preluarea controlului acestora, se constituie în botneturi. Controlate de spammeri, acestea trimit reclame nesolicitate prin intermediul mesajelor electronice.

Citind această carte, vom face cunoștință cu Pavel „RedEye" Vrublevski, lăudărosul și instabilul artizan al ChronoPay și Rx-Promotion, și competitorii acestuia, Igor „Desp" Gusev și Dmitri „SaintD" Stupin, creatorii SpamIt și GlavMed. În momentul scrierii volumului de față, acesta era cel mai mare program farmaceutic ilicit on-line de pe planetă. Miza concurenței dintre ei o reprezintă controlul asupra unei industrii rentabile, de sute de milioane de dolari, care intermediază vânzarea de medicamente ce necesită rețetă. Angrenate în dispută sunt organizații antispam, firme de plăți on-line, companii medicale și servicii de securitate. Fundalul este societatea rusă incapabilă să impună aplicarea legilor, măcinată de corupție, dezinteresată de activitățile infracționale care aduc pagube cetățenilor și instituțiilor străine.

Autorul cărții, Brian Krebs, este un jurnalist american de investigații, reporter, între 1995 și 2009, la ziarul *Washington Post*. Fiind specializat în criminalitatea informatică și securitatea computerelor, el identifica și demasca, în articolele publicate pe această temă, o serie de activități ilicite care exploatau slăbiciunile internetului pentru profit. Constatând că abordarea jurnalistică clasică față de fraudele cibernetice nu este adecvată, acesta demisionează și creează propriul blog de investigații în domeniul securității pe internet, KrebsOnSecurity.com. Un indicator relevant al profesionalismului lui Brian Krebs este faptul că, în 2016, după publicarea

cărții, blogul său a fost ținta celui mai mare atac DDoS până la data respectivă.

Apărut în 2014, volumul de față se referă la un episod specific, definit în timp al constantului război dintre autorități, companii, organizațiile de securitate cibernetică și infractori, care se rezumă la controlul informației pe internet. E-mailurile nesolicitate sunt create de către hackeri și conțin oferte de produse cum ar fi medicamente, pornografie, materiale piratate. Subiectul principal al cărții este reprezentat de apariția farmaciilor on-line ilicite și a rețelelor din spatele acestora, de la creatorii de malware până la consumatorul final. Prima observație pe care trebuie să o facem este aceea că, deși scrisă într-un ritm alert și având aerul unei povești neverosimile, cartea nu este una de ficțiune sau speculativă. Prezentarea subiectului este rezultatul unei investigații jurnalistice riguroase, în care autorul citează surse, discută cu martori, studiază baze de date și face apel la experți. Al doilea aspect se referă la accesibilitate. Deși abordează o temă complexă din punct de vedere tehnologic și dificilă, la prima vedere, din punct de vedere conceptual și terminologic, cartea se citește ușor și nu necesită cunoștințe de specialitate avansate.

Scopul volumului de față este acela de a informa și de a educa. El prezintă practici ilegale, care profită de disfuncționalități din societate, precum și modalitățile specifice în care infractorii extrag informații. Cititorii pot afla care sunt cele mai bune metode pe care le pot folosi pentru a se proteja. Comportamentul on-line și consecințele acestuia presupun o atitudine activă, nu doar cunoștințe tehnice și actualizări ale programelor informatice, dar și evitarea informațiilor din surse nesigure și accesarea linkurilor dubioase.

Relevanța cărții pentru România este indirectă și privește modul în care societatea românească poate gravita spre componenta infracțională sau spre cea a luptei contra practicilor ilicite. În material, sunt amintite vag rețele infracționale

localizate în estul Europei. Obținerea unor medicamente în România este foarte dificilă, deoarece legislația este imprecisă și instabilă, iar importul este uneori subvenționat. Nu e de mirare că se caută soluții pentru livrarea lor discretă și accesibilă, iar oferta spammerilor se încadrează în această categorie. Mass-media a relatat cazuri de rețele informale care facilitează importul și distribuirea de medicamente, evitând canalele aprobate oficial.

Finalul cărții oferă o imagine dublă și un avertisment. „Războiul farmaceutic" și implicarea autorităților au dus la scăderea globală a spamului. Contextul infracțional cibernetic din Rusia poate servi însă intereselor statului, așa cum se va dovedi după publicarea cărții. Experiența răufăcătorilor cibernetici privați este transformată în programe de subminare a statelor democratice și de finanțare a unor armate de troli pentru a semăna discordie. Infractorii se orientează spre informațiile personale și rețelele sociale, beneficiind de neinformarea și apatia utilizatorilor.

EUGEN GLĂVAN

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.

După sosire, Vrublevski a fost arestat și trimis la Lefortovo, o închisoare de înaltă securitate, ca o fortăreață, construită la Moscova în 1881. Aceasta a devenit faimoasă în timpul Războiului Rece, când a fost folosită de KGB pentru izolarea și interogarea deținuților politici. În 1994, Lefortovo a fost preluată de poliția rusă, iar, ulterior, de FSB, succesoarea KGB.

În închisoare, Vrublevski a recunoscut că a comandat atacul asupra lui Assist, dar, mai târziu, a dezmințit acest lucru. Totuși avocatul său, Stanislav Malțev, angajat al ChronoPay, fostul polițist rus care condusese cândva ancheta în dosarul în care Vrublevski fusese acuzat de afaceri ilegale, a susținut că clientul său ar trebui să rămână în libertate până la proces. Instanța i-a respins cererea și a solicitat ca Vrublevski să fie ținut la Lefortovo șase luni înainte de proces, perioada maximă prevăzută de lege pentru acuzațiile care i se aduceau.

„Riscul principal al eliberării lui nu este că el va fugi, ci că le va face ceva rău martorilor, încercând să-i convingă să nu depună mărturie ori să nu ofere informații despre el", a spus Gusev într-o discuție telefonică.

Este o declarație îndrăzneață pentru un bărbat ale cărui jurnale de chat demonstrează că el și Stupin au plătit 1,5 milioane de dolari pentru a se începe urmărirea penală împotriva lui Vrublevski și 50 000 de dolari pentru urmărirea penală a lui Igor și Dmitri Artimovici, frații care – sub pseudonimul comun „Engel" – se spune ar fi folosit botnetul Festi ca să distribuie spam pentru Rx-Promotion și, ocazional, ca să lanseze atacuri distrugătoare împotriva unor siteuri (inclusiv cel împotriva lui Aeroflot pentru care a fost închis Vrublevski).

Următoarele date provin dintr-o conversație pe chat, care se pare că a avut loc între Gusev și Stupin la 26 septembrie 2010. Cei doi deciseseră deja să închidă SpamIt și se gândeau dacă să procedeze la fel cu GlavMed. Vrublevski este numit aici „Paul" (echivalentul occidental al lui „Pavel").

GUSEV: După părerea mea, tu nu-nțelegi pe deplin ce se-ntâmplă de un an încoace. Paul plănuiește fie să mă arunce în închisoare, fie să mă termine. Intențiile lui sunt absolut clare. Există doar două opțiuni: 1 – nu faci nimic și nu plătești nimănui nimic, iar la sfârșit fie mergi la închisoare, fie continui să te ascunzi până la epuizarea tuturor resurselor; 2 – faci exact ce face și el, în același scop.

Gusev îi spune lui Stupin că „orice război costă bani, resurse și celule nervoase. Nu poți merge la război puțin câte puțin – fie lupți până la capăt, fie nu-l începi deloc. Engel ne va face rău tot timpul… Dacă există vreo posibilitate să-l scoatem din joc, ar trebui s-o folosim. 50 000 de dolari înseamnă foarte puțin față de pierderile pe care le-am avut din cauza atacurilor DDoS și față de pierderile pe care le vom mai suferi dacă ne va ataca din nou".

Conversațiile arată de asemenea că, în aceeași perioadă, Gusev a mers la FSB, fiind ademenit să lucreze cu ei și să ofere informații despre marii jucători din industria farmaceutică ilicită.

„Au multe informații și înțeleg foarte bine cum funcționează totul, de unde vin și unde pleacă banii", i-a spus Gusev lui Stupin în ianuarie 2010. FSB, a zis tot el, „are cu siguranță informații despre felul în care circulă banii. În rezumat: dacă vor să mă bage la închisoare, o vor face. Au întrebat și despre tine. Deocamdată, voiau să lucrez pentru ei și să le ofer informații despre alții. Mi-au promis tot felul de avantaje dacă lucrez pentru ei."

Interesant este că discuțiile de pe chat dintre Gusev și Stupin au fost obținute de anchetatorii FSB care-l arestaseră pe Stupin și făcuseră o copie a hard diskului acestuia. Cumva, Engel – poate datorită mitei plătite de Vrublevski – a obținut o copie a acestor conversații și le-a transmis clandestin câtorva surse, inclusiv autorului acestei cărți.

Conversațiile respective au fost prezentate pe larg în cartea de față, dar una dintre cele mai grăitoare și oneste apare

într-un fir de discuții de pe forumul rusesc master-x.com. Acest fir de discuții este plin de comentarii de la spammeri care au fost excluși din afacere ori au pierdut bani din cauza războiului farma dintre Gusev și Vrublevski. În prezent, el cuprinde peste o sută de pagini.

La începutul discuției de pe master-x.com, aproape toți utilizează pseudonime și, în general, încearcă să-și ascundă identitatea reală, dar, cam pe la jumătatea firului, Gusev începe să facă referiri la propria persoană, care îl identifică în mod clar. În această conversație, Gusev devine neobișnuit de irascibil și se lansează într-o serie de tirade din ce în ce mai ostile la adresa lui Artimovici.

Gusev spune că webmasterii ruși au înțeles că războiul farma dintre el și Vrublevski era doar o întrecere, ca să vadă cine are mai mulți bani și mai multe relații. Gusev îl avertizează de asemenea pe Artimovici că Vrublevski ar putea să-și abată furia asupra lui când va ieși din închisoare. (Recunoscând că Vrublevski l-a angajat să execute atacul DDoS asupra lui Assist, Artimovici a pecetluit în esență soarta lui Pavel.)

> Ține minte că Pașa este un om foarte rău. Și are o memorie de elefant! Faptul că m-am descurcat mai bine ca el după ce am părăsit ChronoPay l-a durut foarte mult timp de 7 ani!!! N-a putut să doarmă și a suferit mult! Asta-i invidia. Distruge omul încet, dar sigur. Acum, imaginează-ți în ce stare de spirit se va afla când va ieși de la închisoare. Flămând, furios, abandonat de toți cei care-l lingușeau, fără afaceri și – lucrul cel mai rău – dându-și seama că nu mă va putea băga la închisoare. Cred că psihicul lui nu va putea suporta o asemenea presiune. Și pentru că pe mine nu mă va putea atinge, se va concentra asupra ta și asupra fratelui tău.

Apoi Gusev spune că, de fapt, *el* s-ar putea răzbuna pe Artimovici înaintea lui Vrublevski.

> Însă toate astea sunt gânduri despre un posibil viitor. Revenind la prezent, cred că, oricum, voi ajunge primul la

tine. Te-am avertizat din timp că, dacă încerci să-mi implici familia în conflictul ăsta, consecințele vor fi foarte dure. Te voi găsi personal, îți voi rupe capul și îți voi pune fundul în locul lui – cel mai probabil, nimeni nu va vedea nicio diferență.

*

Procurorii ruși l-au eliberat pe Vrublevski din închisoarea Lefortovo pe 23 decembrie 2012, cu doar trei zile înainte de ziua lui de naștere. Eliberarea n-a fost nici pe departe un act de milostenie. În conformitate cu legea rusă, șase luni era durata maximă cât putea fi ținut închis cineva în așteptarea procesului.

La câteva ore după întoarcerea sa acasă, Vrublevski posta mesaje pe Twitter și pe blog despre triumfătoarea eliberare. De asemenea, l-a sunat destul de repede pe autorul cărții de față, mai ales pentru a-i povesti despre tratamentul primit și condițiile existente în faimoasa închisoare. Într-o lungă conversație telefonică, Vrublevski a deplâns prezența și discuțiile permanente ale numeroșilor deținuți musulmani care erau închiși cu el la Lefortovo.

„Nu aveam nici măcar apă caldă sau o nenorocită de fereastră, iar becul ardea non-stop, zi și noapte, își amintea Vrublevski. Asta e cea mai strictă închisoare din Rusia și jumătate este plină cu tot felul de teroriști musulmani. Trei luni n-am avut dreptul să comunic cu familia mea… nici apeluri telefonice, nici vizite, nimic. Am auzit doar prostia asta de «Allah, akbar» de cinci ori pe zi!"

Avocatul i-a interzis să discute despre cazul său, dar, ca întotdeauna, el avea o poveste amuzantă de spus despre situația în care se afla. Când un deținut de la Lefortovo urmează să fie eliberat, este informat în mod ceremonios de condamnații mai vechi despre tradiția solemnă de a-și arde ulterior hainele pe care le purta atunci când a ieșit din închisoare. Temându-se că nerespectarea acelei tradiții i-ar putea aduce ghinion, Vrublevski și-a invitat niște prieteni acasă a doua zi după

eliberare pentru a-și arde hainele pe care le purta când a fost închis și eliberat de la Lefortovo.

„Imaginează-ți următoarea scenă, a povestit Pavel, abia stăpânindu-și râsul. Era o vreme închisă, urâtă, iar noi stăteam în spatele casei cu hainele pe care le-am purtat când am ieșit din închisoare. Fumam în fața focului și participam la incinerarea hainelor. Era exact ca-ntr-un film de la Hollywood, nu lipsea decât o muzică dramatică. Vorbeam lucruri serioase, de felul: «Nenică, să nu te-ntorci acolo, bla-bla.» Deodată, nevastă-mea iese în goana mare din casă țipând: «Pavel, nu pantofii ăia trebuie să-i arzi!» Am ars niște pantofi Yamamoto scumpi, nu pe ăia cu care venisem acasă de la închisoare!"

În timpul detenției, Vrublevski a semnat o declarație în care recunoștea că a pus la cale atacul asupra firmei Assist, care procesa plățile cu carduri de credit pentru compania Aeroflot. Potrivit declarației, el îi ceruse unui angajat al ChronoPay – Maksim Permiakov, specialist în securitatea informațiilor – să depună 20 000 de dolari în WebMoney într-un portofel electronic deținut de Igor A. Artimovici, presupusul botmaster al lui Festi și fost angajat al filialei Sun Microsystems în Rusia. Într-adevăr, un lung fir de e-mailuri din arhiva de mesaje scursă de la ChronoPay conține informații detaliate despre acest schimb.

Arestat de Serviciul Federal de Securitate al Federației Ruse (FSB), Artimovici a semnat o declarație similară, afirmând că a fost angajat de ChronoPay să folosească Festi într-un atac împotriva lui Assist. FSB l-a arestat și pe fratele lui Artimovici, Dmitri, programator liber-profesionist.

Toți patru – Vrublevski, Permiakov și frații Artimovici – au fost acuzați de încălcarea a două articole din Codul penal rusesc: articolul 272, care se referă la „accesul ilegal la informații stocate în computer", și articolul 273, care interzice utilizarea și distribuirea de malware. Ambele articole prevăd pedepse cu închisoarea de la trei la șapte ani.

CUPRINS