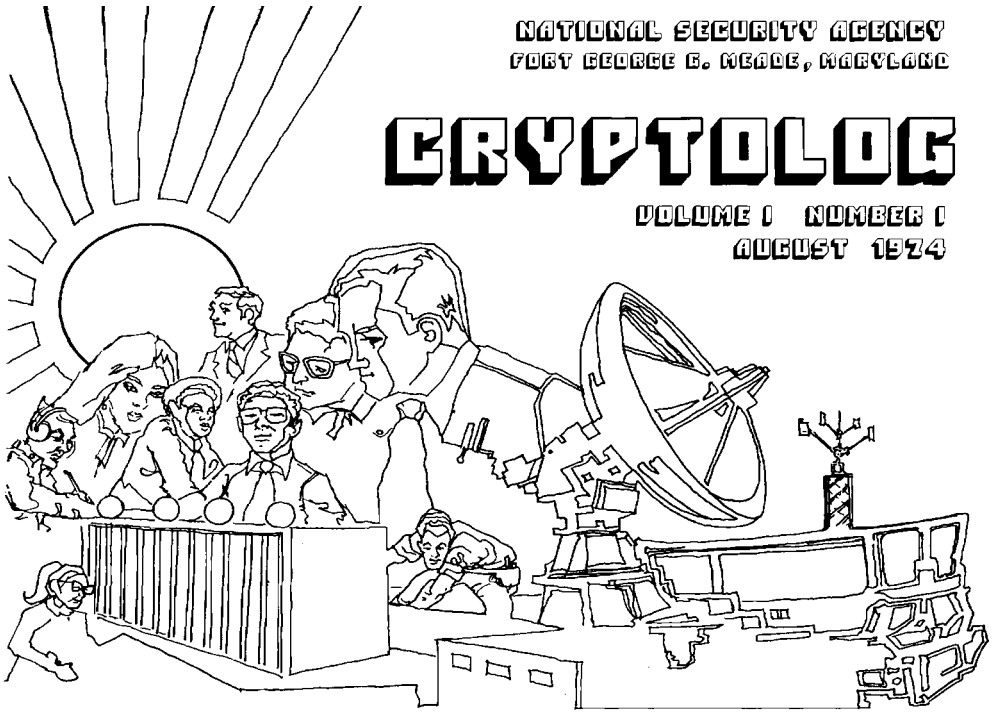
Velký webový test
Kdo provedl březnové DDoS útoky?

Po vlně kybernetických útoků z počátku března má odborná veřejnost víceméně jasno v tom, co se stalo. Pokud jde o otázky, kdo za útoky stojí a proč je provedl, odpovědi zůstávají na rovině spekulací.

ONDŘEJ PROFANT
HONZA ŠÍPEK

Z technického hlediska se jednalo vlastně spíš o drobné polechtání, nicméně s velkým veřejným ohlasem: v pondělí 4. března padla velká internetová média (iDnes.cz, iHNed.cz, Novinky.cz), v úterý pak následoval opravdový šok – nešel Seznam.cz, což pro průměrného českého uživatele v podstatě znamenalo, že nefungoval internet. Ve středu se zhroutil bankovní systém a odborná média vypsala anketu s otázkou, jaký bude další cíl útoků. Vyhráli mobilní operátoři a skutečně: ve čtvrtek přestaly fungovat jejich weby. Komunita počítačových nadšenců tedy správně identifikovala vzorec útoku: cílem jsou známé a často využívané servery, každý den jiná „kategorie". Na pátek komunita předpověděla útoky na servery státní správy, k nimž už nakonec nedošlo.



Obálka prvního čísla nedávno odtajněného časopisu Cryptolog, který vydává pro vlastní potřebu americká Národní bezpečnostní agentura (NSA)

Ve skutečnosti to nebylo tak horké, jak líčily palcové titulky na předních stránkách novin. Seznam nefungoval jen malou chvíli, on-line bankovní služby sice byly ledaskde nedostupné delší dobu (což při jejich zdejší kvalitě není nic neobvyklého), ale bankovní systém se rozhodně nezhroutil.

Přesto takto silný útok český internet zatím nezažil. Vše ukazovalo na techniku DDoS (Distributed Denial of Service), při kterém útočník zahltí zvolený server, na kterém je stránka umístěna, požadavky na přístup. Záludnější varianta takového kyberútoku, SYN Flood, využívá gentlemanský způsob, jímž si počítače mezi sebou „povídají": když server vyzveme ke komunikaci, zdvořile čeká, až komunikovat začneme. Uvedeme-li falešnou zpáteční adresu a uděláme to mnohotisíckrát za sebou, vyčerpáme jeho prostředky. Kvůli podvrženým adresám je navíc obtížné útočníka stopovat a zablokovat. K takovému útoku bývá potřeba tzv. botnet, velká síť počítačů (od desetitisíců po miliony strojů), které útočník ovládá. Počítače a jejich majitelé nevědí, že jsou součástí botnetu – to zařídil virus nebo jiný malware, který obstarává komunikaci (přijímá rozkazy) i samotný útok (vysílá pakety, které v důsledku zahlcují síť).

S překvapujícím zjištěním přišel později CZ.NIC, správce domény .cz. V době probíhajících útoků vyrobil jejich simulátor, jakýsi cvičný kybernetický kanón na testování vlastní infrastruktury. Překvapivě k provedení několikrát silnějšího útoku nebyl botnet zapotřebí, stačilo menší množství počítačů připojených do sítě dostatečně silným připojením. Dá se jen spekulovat, kdo všechno může mít podobnou „kyberzbraň" připravenou v záloze.

Možná vysvětlení

Nejdůležitější a nejzajímavější otázky – kdo útočil a proč? – zůstávají nezodpovězeny. Mezi nejdiskutovanější odpovědi patří šest následujících:

Varianta, že za vším stojí talentovaný „osamělý střelec", který si stvořil vlastní botnet, působí poněkud fantasknè. Podobné případy alespoň krátkodobého znefunkčnění některých systémů se ale už staly. Vyloučit nelze ani šikovného gymnazistu, který se vytahuje před svou holkou.

Širokou pozornost získaly hacktivistické skupiny Anonymous či LulzSec (viz článek Hactivismus na vzestupu v A2 č. 3/2012), které prostředky pro provedení takového útoku nejspíš mají. Ale k čemu by byla politickým aktivistům prospěšná akce bez příslušné politické deklarace? Chyběl totiž pamflet, prohlášení, požadavky – zpráva, která se má šířit médii spolu s informacemi o útoku. Ani zákulisní informace „z prostředí" nenasvědčují tomu, že by útočili čeští Anonymous.

Kyberútoky se samozřejmě využívají i v rámci konkurenčního komerčního boje, avšak této eventualitě odporuje příliš široké zaměření útoku. Kromě toho, že je těžko myslitelný konkurent společný všem napadeným subjektům, je tu i příliš velké riziko odhalení.

V odborných kruzích se v souvislosti s útoky nejčastěji probírá teorie komerční prezentace: majitel botnetu prezentuje jeho sílu – takový Seznam opravdu není bezbranný outsider a vyřadit ho i na pár minut je výkon vzbuzující respekt. Toto vysvětlení má ale zásadní trhlinu: útok takového rozsahu a koncentrace vyvolá reakce a po očekávatelném odhalení viru bude botnet do jisté míry vyřazen ze hry.

Politický tlak?

Poněkud paranoidní je teorie politického tlaku. Mnozí upozorňují na souvislost se založením českého Národního centra kybernetické bezpečnosti, které bylo odborným i laickým médiím představeno krátce před útoky. Národní bezpečnostní úřad, jenž bedlivě prověřuje mimo jiné adepty na práci s tajnými informacemi, převzal předloni kybernetickobezpečnostní agendu od ministerstva vnitra a chystá nový zákon o kybernetické bezpečnosti. Lze očekávat, že v okamžiku schvalování zákona budou panovat obavy o ohrožení svobody internetu. Strach z opakování útoků a volání po větším zabezpečení před nimi může pomoci odpor veřejnosti otupit. Nasvědčovalo by tomu snad i nedávné vyjádření NBÚ, že viníky je těžké vypátrat a že bude zapotřebí „drobná úprava návrhu zákona o kybernetické bezpečnosti, případně novelizace zákona o elektronických komunikacích".

Samotný věcný záměr zákona byl zpočátku hodně divoký a terminologicky nejasný. V připomínkovém řízení ale prošel velkými změnami, mimo jiné i díky úsilí České pirátské strany, a současná podoba je odbornou veřejností vnímána jako schůdná a vlastně i potřebná. O co v zákoně jde? Především o to, aby se státní správa o bezpečnost vůbec starala a definovala, kdo je za ni odpovědný. Dále potom o stanovení způsobu, jakým budou postižené strany komunikovat s centrem kybernetické bezpečnosti a jaké informace mu budou povinny poskytovat. Centrum by pak mělo koordinovat obranu. V případě „kybernetického nebezpečí" (toto rozhodnutí musí schválit vláda a každých sedm dní ho znovupotvrdit) budou mít povinnost zavádět opatření nařízená NBÚ i poskytovatelé internetu.

A zde je právě možný kámen úrazu: nemůže státní dozor nařídit například odstřižení celých webů? Je to sice nejfašističtější výklad jinak potřebného zákona, ale zákon sám proti němu nenabízí žádnou pojistku. A scénář, kdy dojde například k pouličním nepokojům a DDoS útokům na vládu, ta vyhlásí kybernetické nebezpečí a NBÚ nařídí providerům blokovat třeba Twitter, přes nějž se útoky organizují, je v extrémním výkladu možný. Zákon by měl cenzuru webu explicitně zakazovat.

„Pouhé" cvičení

Posledním vysvětlením je, že šlo pouze o cvičení. Útok byl sice masivní, pokud jde o razanci, ale netrval dlouho a v důsledku se dohromady nic nestalo. Cvičný útok provozovatele serverů přesvědčil o nutnosti zabezpečení proti tomuto typu útoků a může pomoci opevnit infrastrukturu dříve, než „půjde do tuhého" a budeme čelit skutečné kyberválce. Podobnou pozitivní roli měli hackeři i jejich útoky v ekosystému internetu odedávna. Útočit lze jen tam, kde je špatné zabezpečení. Když server banky nebo tajné služby „hacknou" vtipálci, kteří jen „přemalují" titulní stránku, je to lepší, než když zaútočí někdo se skutečně zlým úmyslem. A výsledná ostuda (někdy) donutí správce systémů chytnout se za nos a napříště se ochránit lépe. Je to jako očkování: tělu se vpíchnou oslabené bakterie a to si na ně samo vybuduje protilátky. Koneckonců, velké společnosti si k simulovaným hackerským útokům samy najímají „penetrační testery". Některé zranitelnosti březnový „test" skutečně odhalil, například to, že na webu závisejí platební terminály České spořitelny nebo SMS jízdenky MHD. Neměly by.

Pozoruhodnou zkušenost s cvičením NATO v listopadu 2012 popisuje český informační publicista Jiří Peterka. Součástí kybernetického armádního cvičení byla i práce s vybranými novináři, kterým byly dávkovány informace ze simulovaných útoků a vyhodnocovány jejich (neveřejné) články. Schopnost komunikace s médii a zvládání jejich reakcí je tedy součástí vojenských plánů. O tom, co se o útocích ze začátku března podařilo zjistit, i o detailech jejich zvládání jsme se dozvídali z médií celkem podrobně. I to by mohlo být – v lehce paranoidním uvažování – součástí „velkého testu".

Autoři jsou uživatelé internetu.