PREDGOVOR

Kada sam upoznala Jamesa Forshawa, moj posao je u časopisu *Popular Science* iz 2007. godine opisan kao jedan od deset najgorih poslova u oblasti nauke: titula tzv. „Microsoftovih *fizikalaca* za bezbednost" dodeljena je svim članovima centra *Microsoft Security Response Center (MSRC).* Naša radna mesta našla su se na toj listi (proslavljenoj do te mere među nama koji se zlopatimo u Redmondu, država Vašington, da smo napravili i odgovarajuće majice) u istom rangu sa ispitivanjem fekalija kitova, a tek nešto višem od vazektomije slonova. Razlog tome je bila najava čitave gomile izveštaja o bezbednosnim propustima u Microsoftovim proizvodima.

James je moju pažnju prvi put privukao upravo u MSRC-u, kao stručnjak za bezbednosne strategije sa velikim entuzijazmom, kreativnošću i ošrim okom za netipične probleme koje je lako previdеti. James je bio autor najzanimljivijih izveštaja o bezbednosnim propustima – što nije mala stvar, s obzirom na to da u MSRC od istraživača bezbednosti godišnje stiže više od 200.000 izveštaja takve vrste. James je otkrivao ne samo jednostavne programske greške, nego i probleme u platformi .NET

Framework. Greške na nivou osnovne arhitekture teže je rešiti pomoću jednostavnih programskih zakrpa i zato je njihovo otkrivanje više nego dragoceno za Microsoft i njegove klijente.

U junu 2013. godine pokrenula sam prve dodele nagrada za pronađene propuste u kompaniji Microsoft. U prvom paketu nagrada imali smo tri programa, u kojima je istraživačima bezbednosti poput Jamesa trebalo obezbediti novčanu naknadu ako Microsoftu prijave najozbiljnije bezbednosne propuste. Znala sam da ćemo efikasnost tih programa dokazati samo ako se prijave izuzetne bezbednosne greške.

Naravno, pokretanje programa nije nužno značilo da će nalazači grešaka doći kod nas. Borili smo se za najveštije svetske lovce na greške, a bilo je i drugih novčanih nagrada. Osim toga, nisu sva tržišta za za bezbednosne propuste i njihovo iskorišćavanje namenjena odbrani, nego postoje i dobro organizovana nacionalna ili kriminalna napadačka tržišta. Pored toga, Microsoft je računao na one nalazače koji su već dostigli nivo od 200.000 besplatnih godišnjih izveštaja o propustima. Nagrade je trebalo iskoristiti za to da se tim dobronamernim i nesebičnim lovcima na greške skrene pažnja na probleme oko kojih je Microsoftu pomoć bila najpotrebnija.

Zato sam pozvala Jamesa i ostale, verujući da nam mogu isporučiti traženu „robu sa greškom". Prve Microsoftove nagrade žarko smo želeli da dodelimo za ranjivost Internet Explorera 11 beta, naročito za nešto za šta ih nijedan proizvođač softvera nikada nije dodelio: nove metode za iskorišćavanje ranjivosti. Ova poslednja novčana nagrada postala je poznata pod nazivom *Mitigation Bypass Bounty* i iznosila je 100.000 dolara.

Još se sećam kako sam u Londonu uz pivo pokušavala da zagrejem Jamesa za bezbednosne propuste u Internet Exploreru, dok mi je on objašnjavao kako se nije baš previše bavio bezbednošću pregledača i upozorio me da ne očekujem previše.

Na kraju je prijavio četiri jedinstvena izlaza iz karantina za Internet Explorer 11 beta.

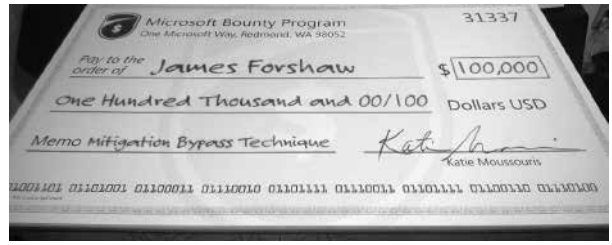
Četiri.

Ti izlazi iz karantina nalazili su se u onim delovima koda Internet Explorera koji su promakli svim našim internim timovima, kao i spoljnim timovima za testiranje neprobojnosti. Izlazi iz karantina su ključni jer pomažu da se na pouzdaniji način iskorišćavaju ostale vrste ranjivosti. James je zaradio nagrade za sve četiri greške, koje mu je isplatio sâm tim Internet Explorera, kao i dodatnih 5000 dolara iz mog budžeta za nagrade – iako mi se sada čini da je zaslužio mnogo više. To zaista nije bio loš rezultat za lovca na greške koji se nikada nije bavio bezbednošću veb-pregledača.

Jednog svežeg jesenjeg dana, samo nekoliko meseci kasnije, pozvala sam Jamesa telefonom i saopštila mu bez daha da je upravo ušao u istoriju. Oduševljena što imam čast da mu prenesem novost, obavestila sam ga da je prihvaćen njegov ulazak u drugi Microsoftov program nagrada za otkrivanje bezbednosnih propusta, *Mitigation Bypass Bounty* za 100.000 dolara. James Forshaw je pronašao nov način da u najnovijem

operativnom sistemu zaobiđe sve odbrane platforme korišćenjem propusta na nivou arhitekture, i tako zasluži Microsoftovu prvu nagradu od 100.000 dolara.

U tom telefonskom razgovoru James mi je rekao da me zamišlja kako mu javno dodeljujem lažni i komično uvećani ček na Microsoftovoj internoj konferenciji *BlueHat*. Odmah posle poziva poslala sam poruku odeljenju za marketing, i tako su James i džinovski ček postali deo istorije Microsofta i interneta.



Ono što će čitaoci sasvim sigurno naći na narednim stranicama ove knjige delići su Jamesove genijalnosti – iste one koju sam uočila pregledajući izveštaje o propustima pre nekoliko godina. Postoji mali broj vrednih istraživača bezbednosti koji mogu da pronađu propuste u jednoj naprednoj tehnologiji, a još je manji broj onih koji mogu jednako dosledno da ih pronađu u više njih. A tu su i ljudi kao što je James Forshaw, koji sa hirurškom preciznošću mogu da se usredsrede na ozbiljnije probleme u arhitekturi. Nadam se da će čitaoci ovu knjigu, kao i svaku buduću koju James bude napisao, posmatrati kao praktičan vodič i izvor inspiracije za svoj budući rad.

Na sastanku povodom dodeljivanja nagrade u Microsoftu, dok su članovi tima Internet Explorera u čudu vrteli glavama, pitajući se kako je moguće da su propustili greške koje je James prijavio, izjavila sam: „James može da vidi i damu u crvenoj haljini i kôd kojim se ona vizuelizuje u filmu *Matriks*." Svi su prihvatili ovo objašnjenje za Jamesov način rada i razmišljanja, jer je reč o čoveku koji snagom uma može da savija kašike. Ako dobro proučite ono što radi i otvorite svoj um, to biste mogli da postignete i vi.

Svima onima koji pronalaze bezbednosne propuste širom sveta: neka ovo postane vaš standard, iako je visok. Svim nebrojenim anonimnim *fizikalcima* za bezbednost softvera: neka svi vaši izveštaji budu dragoceni kao oni koje je napisao jedinstveni i nezamenljivi James Forshaw.

Katie Moussouris,
osnivač i izvršni direktor kompanije Luta Security,
oktobar 2017. godine