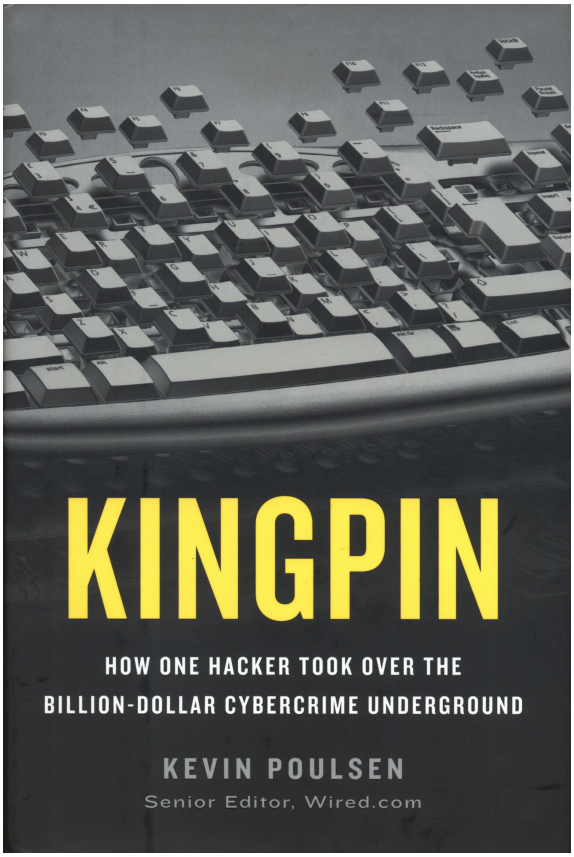
Kevin Poulsen, Kingpin: how one hacker took over the billion-dollar cybercrime underground, Crown Publishers, New York 2011, 266 str.



Knjiga opisuje kariero ameriškega računalniškega strokovnjaka Maxa Butlerja, rojenega leta 1972, ki je kasneje spremenil svoje ime v Max Vision. Njegova formalna izobrazba se je končala po enem letu univerze. Vseeno je postal ekspert za vdore v računalniške sisteme. Poskusi prijateljev, varnostnih služb in podjetij, da bi njegove talente izkoristili v dobre namene, so bili le polovično uspešni, saj mu žilica ni dala, da ne bi ob testiranju računalniške varnosti poskušal narediti še kaka skrivna vratca za nadaljnje vstope in izkoriščanje tujih računalnikov v svoje namene. Že v mladosti je prihajal navzkriž z zakonom, sprva zaradi vandalizma in nasilništva. Ker ni resno jemal opozoril in se ni hotel pogajati z oblastmi, mu je to prineslo več let zapora in konec študija na univerzi. Kasneje je vdrl v računalniške sisteme vojaškega letalstva ZDA. Oblasti so mu bile pripravljene pogledati skozi prste, če bi sodeloval z njimi. Vendar ni hotel sodelovati v lovu na druge hekerje. Svoje so naredila tudi stališča neke liberalne odvetnice. Ta je hekerjem na njihovem srečanju svetovala, naj ne sodelujejo z oblastmi brez pomoči advokata. Tako je bilo sodelovanja s FBI definitivno konec in se je znova znašel v zaporu. Po izpustu so mu kljub vsemu dobri ljudje naročili, naj testira varnostni sistem

nekega podjetja. Po neuspešnem direktnem napadu je vdrl v osebni računalnik nekega uslužbenca in z ukradenimi podatki končno le prišel v sistem. Problem je bil, da je s tem spet presegel svoja pooblastila. Tako je vse teže našel službo in s pomočjo ljudi, ki jih je spoznal v zaporu, je zdrsnil v svet kriminala. Z avtomatiziranim pregledovanjem, z izkoriščanjem lukenj v Internet Explorerju, je našel ranljive računalnike v podjetjih in restavracijah in iz njih pobiral podatke o kreditnih karticah, ki jih je posredoval svojemu kompanjonu. Ta je izdeloval kopije kartic. Delo zločincem olajšuje trmoglavost ameriških bank, ki zaradi enkratnih visokih stroškov nočejo zamenjati zastarelega sistema kreditnih kartic z magnetnim trakom. Podatke z magnetnega traku je mogoče z majhnim skenerjem posneti tudi fizično v nekaj sekundah. Knjiga opisuje, kako je (bilo?) v ZDA mogoče nabaviti vso opremo za ponarejanje kartic.

Samo v eni restavraciji je našel podatke o petdeset tisoč karticah. Delo so mu olajšali nekateri ponudniki informacijskih sistemov, ki so interna omrežja priredili tako, da so za vzdrževanje lahko vanje vstopali na daljavo, te vhode pa so slabo zaščitili. Tudi sicer mnoga podjetja, npr. Amazon, hranijo podatke o kreditnih karticah. To naj bi olajšalo naročanje, pomeni pa tudi tveganje. (Verjetno je to eden od razlogov, da morate recimo pri American Expressu za nakup v Amazonu dobiti poprej odobritev.)

Max Butler se je vključil v ekskluzivne kriminalne forume na omrežju. Tu udeleženci, skriti za psevdonimi, izmenjujejo izkušnje, novosti, kupujejo in prodajajo naslove in številke bančnih računov, kartic, PIN-e, opremo za ponarejanje ipd. Ti forumi ne poznajo meja. Sam je tu prodajal podatke in obenem vdiral v računalnike drugim nepridipravom in jim kradel informacije.

Infiltriral se je v bančne sisteme tako, da je uslužbencem poslal osebna sporočila, v katerih je napisal, da so omenjeni v članku v reviji. Od petsto uslužbencev neke banke jih je četrtina kliknila na povezavo na ta neobstoječi članek in mu s tem odprla vrata. Butler je zelo rad vdiral v računalnike čez Wi-Fi omrežja – s 60 centimetrsko parabolično anteno iz najete sobe v kaki visoki zgradbi.

Podnaslov te knjige omenja enega od njegovih največjih podvigov – so-

vražni prevzem več kriminalnih forumov. To se mu je posrečilo, ker večina teh forumov ni imela varnostnih kopij. Zbrisal je njihovo vsebino, udeležence pa vključil v omrežje, ki ga je sam kontroliral. Dolgo časa je uporabljal strežnik nekega ponudnika informacijskih storitev na Floridi – ne da bi ta za to vedel.

Knjigo je težko odložiti. Uspehi in neuspehi represivnih služb pri zasledovanju glavnega akterja in drugih nepridipravov, vojne in spopadi med zlikovci samimi so zelo napeto branje, (čeprav ni streljanja, divjih zasledovanj in nasilje nastopa le na nekaj straneh.) Eden večjih problemov za predstavnike zakona so bili računalniki s kriptozaščito, ki je, kot vemo, lep primer uporabe teorije števil in algebraične geometrije. Glavni akter knjige je uporabljal izraelski DriveCrypt, ki ga je stal 60 USD. (Podoben program je Pretty Good Privacy.) Prav zaradi tega so leta 2007 v sobo Maxa Butlerja vdrli ob dveh zjutraj, ko je dremal, tako da ni mogel ugasniti računalnikov. Po dveh tednih se je vladnim strokovnjakom v kopiji RAM-a (hitrega spomina) posrečilo najti geslo. Max Vision (Butler) je bil leta 2009 obsojen na 13 let zapora in povrnitev 27 milijonov dolarjev škode (kar ne bo mogel poplačati, saj je bil njegov dobiček le majhen delež te vsote, pa še ta denar je bolj ali manj sproti zapravil). Celotna škoda, ki jo je povzročil, je trikratni znesek te vsote. Menda bi zdaj rad doštudiral matematiko ali fiziko.

Avtor knjige Kevin Poulsen je sam odsedel nekaj časa v zaporu zaradi vdiranja v računalnike. Zato morda glavnega akterja opisuje nekoliko olepšano. Sem in tja najdemo tudi kako nedoslednost. Tako knjiga precejkrat opisuje prenose denarja čez „e-gold“, opis te problematične „računalniške valute“, osnovane na rezervah v zlatu, pa je šele v drugi polovici knjige. Sam vsega tehničnega žargona nisem razumel. Večino stvari bi si gotovo lahko pojasnil s kratkim pogledom v Wikipedijo. Glavni obrisi tehnik vdorov in druge zločinske aktivnosti pa so tako dobro opisani, da človek brez težav preskoči nekatere podrobnosti. Knjigo priporočam tudi kot poučno branje, ki vam morda lahko prihrani kako nevšečnost pri uporabi interneta.

Peter Legiša

http://www.dmfa-zaloznistvo.si/