NOVO DOBA ZLOČINA

Aleksandar Pašagić

Vi ste osoba koja svojoj sigurnosti posvećuje dužnu pažnju. Trudite se biti maksimalno informirani o zbivanjima u vašoj okolini. Vaša kuća opremljena je modernim protuprovalnim vratima, a digitalna kamera pred vašim vratima bilježi svaku aktivnost 24 sata na dan. Pohađate satove neke borilačke vještine ili sistema, i uvijek su vam pri ruci suzavac, elektrošoker ili neko drugo sredstvo za samoobranu. Svjesni ste svoje okoline, uvijek oprezni i budni. Zapravo, uvjereni ste da vas ništa ne može iznenaditi. Onda jednog dana uđete u trgovinu, a prodavač vas informira da je vaš bankovni račun prazan. Upravo ste postali žrtva najmodernijeg oblika kriminala. Dobrodošli u novo doba zločina.

Nova opasnost

Usprkos najboljim naporima uloženim od strane nadležnih državnih službi, „staromodni“ kriminal ne jenjava niti po intenzitetu, niti po učestalosti. Novine svakodnevno izvještavaju o velikom broju kriminalnih aktivnosti prisutnih na svim instancama društva. Nasilniji zločini prirodno plijene veću pažnju javnosti, dok su oni „elegantniji“ poput prijevara i manipulacija zakonom nešto manje atraktivni. No iako je prosječan građanin koji gleda televizijski program ili čita novine i više nego dobro svjestan stope kriminala i potencijalne opasnosti, sve to mu se ipak čini poprilično udaljeno od njega i njegove obitelji. Ukoliko nema izravnih poslovnih ili rodbinskih veza s osobama involviranima u protuzakonite djelatnosti, a također nema niti toliko novaca da bi predstavljao posebno atraktivnu metu zbog onoga što posjeduje, prosječan se čovjek osjeća prilično sigurnim. Malo tko se od nas može zamisliti kao predmet ciljanog atentata, a prirodna je sklonost misliti da se dio nasilja koji je po prirodi odabira žrtve nasumičan uvijek događa „nekom drugome“. Statistički gledano, Hrvatska je još uvijek prilično sigurna zemlja za „običnog“ stanovnika. No u porastu je nova, drugačija vrsta protuzakonite djelatnosti, od koje više nitko nije potpuno siguran, budući da je upravo prosječan čovjek njena najbolja meta.

Kriminalne metode uvijek su držale korak s vremenom i razvojem novih tehnologija. Prije par stotina godina drumski razbojnici pljačkali su koristeći noževe i sablje. Danas pirati opremljeni suvremenim vojnim naoružanjem i poduprijeti sofisticiranom infrastrukturom otimaju cijele prekooceanske tankere. Svaki vid protuzakonite aktivnosti postao je kompleksniji zbog pokušaja kriminalaca da ostanu korak ispred u vječnoj igri lovice koju igraju protiv organa koji sprovode zakon. No usprkos porastu složenosti, sama aktivnost u svojoj je biti ostajala ista od pamtivijeka – ubojstva, pljačke, droga, prostitucija, krijumčarenje i slično. Da biste se bavili nečim takvim, morali ste svjesno odbaciti većinu društvenih i moralnih normi, a na to je bio spreman samo mali broj ljudi. Ali apel novog doba kriminala, računalnog ili cyberkriminala, upravo je suprotan, i glasi – i vi možete zaraditi novac bez muke na ilegalan način, i to iz sigurnosti vlastitog doma; a sve što vam treba jest osobno računalo.

Ciljana populacija

Cyberkriminal (u ovom trenutku) nije pretjerano atraktivna tema, i zato mu se posvećuje relativno malo pažnje u medijima. To dovodi do prevladavajućeg neznanja koje, naravno, izuzetno pogoduje kriminalcima. Kako dolazi do porasta transakcija koje se odvijaju preko računala, tako ta ista računala postaju sve atraktivnija meta. Čak i ako se ne bavite nekim posebnim poslovnim djelatnostima, vrlo je vjerojatno da se u jednom ili drugom

trenutku na vašem računalu može pronaći većina podataka o vama, vašoj obitelji, mjestu stanovanja, vašem poslu i slično. Postoji mnogo načina na koje se te informacije mogu iskoristiti protiv vas, a ipak većina ljudi još uvijek nije svjesna koliko su uistinu izloženi svaki put kada se povežu na Internet, neovisno o svrsi tog povezivanja.

Prvi i osnovni korak koji moramo shvatiti kada govorimo o cyberkriminalu jest da je svatko od nas valjana meta u očima kriminalca. Vaših 1000 kuna vrijedi jednako kao i onih bilo koga drugoga, i samim time isplati ih se uzeti. U fizičkom svijetu, ako ste stara bakica simpatičnog izgleda, džeparoš na ulici mogao bi vas zaobići zbog čistog suosjećanja. Ali kada je vaš cjelokupni identitet samo korisničko ime, iz jednadžbe se uklanja ljudski faktor. U svijetu računalnog kriminala više nema diskriminacije. Štoviše, budući da su korisnici koji raspolažu osjetljivijim informacijama ili većim transakcijama svjesniji rizika, te implementiraju snažnije mjere sigurnosti, običan korisnik Interneta postaje još lakša i atraktivnija meta.

Znanje je najbolje oružje

Iako se svijet računalnog kriminala umnogome razlikuje od svijeta opipljivih zločina, osnovno načelo obrane je identično, a to je svjesnost. Ako želite imati imalo šanse izbjeći da postanete žrtva cyberkriminala, morate posjedovati barem osnovno znanje o načelima u skladu s kojima funkcionira prijetnja kojoj ste izloženi. U fizičkom svijetu, većinu opasnosti prepoznajemo intuitivno. Ne trebamo pročitati nikakav članak da bismo znali kako osobi koja u nas drži uperen pištolj nije na pameti naša dobrobit. Ali budući da smo svijetu računala izloženi tek relativno kratko vrijeme, oslanjati se isključivo na intuiciju kada se radi o sigurnosti u tom okruženju predstavlja veliku grešku. Pogreška je i oslanjanje na zaštitu od strane nekog drugog. Istina je da većina pružatelja Internet usluga daje u svom paketu i određeni stupanj zaštite, ali to je uvijek vrlo daleko od dovoljnoga. Osobna odgovornost je ključna, a ona počinje s upoznavanjem prijetnje. Dakle, što je zapravo cyberkriminal?

Cyberkriminal je, općenito uzevši, zajednički naziv za svaku kriminalnu aktivnost u kojoj je računalo ili računalna mreža izvor, oruđe, cilj ili mjesto zločina. To uključuje protuzakoniti pristup, protuzakonito presretanje informacija, podatkovnu interferenciju (neovlaštene manipulacije računalnim podacima), sistemsku interferenciju (manipulaciju funkcionira nečijeg računalnog sustava), krivotvorenje (krađa identiteta), te razne vrste prijevara. Neki od navedenih napada bit će koncentrirani na organizacije, poduzeća ili ustanove, dok će drugi za cilj imati privatnog korisnika osobnog računala. Podvrsta i specifičnih aktivnosti cyberkriminala je mnoštvo, a kriminalci svakodnevno iznalaze nove načine uporabe računala u protuzakonite svrhe. Opisivanje svih protuzakonitih računalnih aktivnosti daleko nadmašuje opseg ovog članka, čija je namjera povisiti stupanj svjesnosti o specifičnosti ove relativno nove prijetnje. Internet obiluje resursima koji se detaljno bave cyberkriminalom, kao i savjetima kako se nositi s njime. Ali kako bismo ilustrirali opseg same opasnosti i malo dočarali domišljatost cyberkriminalaca, ukratko ćemo se dotaći jedne od najpopularnijih Internet prijevara – tzv. phishinga.

Phishing

Phishing je iskrivljenica engleske riječi fishing (pecanje), a odnosi se upravo na to – skup taktika prevare usmjerenih da se od vas „upecaju“ osobni podaci koji će se kasnije upotrijebiti na korist druge osobe. Osobni podaci mogu uključivati korisnička imena i lozinke, adresu i telefonski broj, brojeve i datume isteka valjanosti kreditnih kartica, PIN-ove i brojeve bankovnih računa. Suvišno je opisivati sve načine na koje poduzetni kriminalac može

iskoristiti takve podatke, ali istovremeno je začuđujuće koliko je prosječni korisnik interneta spreman te podatke učiniti dostupnima kao posljedica needuciranosti ili naivnosti.

Phishing dolazi u raznim oblicima. Mogli biste primiti poruku u vašoj elektronskoj pošti u kojoj vas se traži da potvrdite vaše ime i lozinku, ili provjerite podatke o vašem računu zbog evidencije. Možete dobiti obavijest o tome kako ste sretni dobitnik vrijedne nagrade odabrani nasumičnim izvlačenjem, i sve što trebate jest poslati svoje osobne podatke i broj bankovnog računa. Popularne su i lažne internet stranice koje se predstavljaju kao banke, dobrotvorne organizacije ili web trgovine. Sama činjenica da nešto ima vlastitu profesionalno uređenu web stranicu ne povlači automatski i legitimnost te stranice. Dovoljna je jedna nedovoljno oprezna osoba s čijeg će se bankovnog računa i više nego refundirati trošak izrade i postavljanja te web stranice. Mnogo stranica i mailova u sebi nose tzv. spyware tip računalnih programa koji se automatski instaliraju na vaše računalo i koriste ga za slanje „spam“ poruka, ili bilježe i šalju podatke koje unosite preko tipkovnice. Linkovi na stranice čija adresa izgleda potpuno legitimno mogu voditi na sasvim drugo mjesto. Domišljatost kriminalaca koji koriste phishing kao sredstvo dobivanja vaših osobnih podataka može biti zapanjujuća.

Koje su standarde procedure prevencije tog tipa prevare? Nikada nemojte odgovarati na poruke koje od vas traže vaše osobne podatke preko elektronske pošte; ako vjerujete da je poruka doista poslana od strane vaše banke, nazovite ih telefonom (ne na broj naveden u istoj poruci) ili provjerite situaciju osobno. Nemojte pritiskati veze (linkove) u sumnjivim porukama, niti ih kopirati i zalijepiti u preglednik; upišite vezu ručno. Također, imajte na umu da komunikacija putem komercijalnih pružatelja usluge elektronske pošte ne predstavlja sigurnu komunikaciju, i stoga se nikada ne bi smjela upotrebljavati za slanje osobnih ili osjetljivih podataka. Zaštitite svoje računalo programima za zaštitu od virusa i ostalih zloćudnih programa. Ako za transakcije putem Interneta koristite kreditnu karticu, redovno provjeravajte potvrde i izvještaje vaše banke kako biste se osigurali da iznosi međusobno odgovaraju, a u slučaju bilo kakvih nepravilnosti, što prije kontaktirajte banku.

Budućnost kriminala

Do prije samo nekoliko godina, hakerski napadi, phishing, spam i slične pojave bile su domena nekolicine više razigranih nego zlonamjernih ljudi. No s porastom postotka populacije koja koristi Internet, te gotovo potpunim transferom poslovne komunikacije iz pisanog u elektronski oblik, načini prijevare i kriminala koristeći računala počeli su donositi vrlo opipljivu dobit onima koji su znali iskoristiti slabosti računalnih mreža i sustava. Sam phishing postao je tako unosan posao da u domeni te prijevare trenutno dominira ruska mafija, koja regrutira talentirane programere iz cijelog svijeta. Kako se u cyberkriminalu počinje okretati sve više i više novca, eksperti predviđaju sve značajniji prijelaz izvora internetskih prijevara iz ruku samostalnih „poduzetnika“ u okrilje organiziranog kriminala koji je uvidio mogućnosti novog i još uvijek relativno slabo iskorištenog tržišta s ogromnim potencijalom. U skladu s time, svatko tko koristi računalo za poslovne namjene bilo koje vrste treba posvetiti primjerenu pažnju i vrijeme vlastitoj edukaciji kako bi mogao aktivno doprinijeti suzbijanju širenja te nove vrste kriminala.

.