ELEKTROTEHNIŠKI VESTNIK 83(3): 144-147, 2016
STROKOVNI ČLANEK

Varna uporaba mobilnih naprav v kibernetskem prostoru

Simon Vrhovec

Univerza v Mariboru, Fakulteta za varnostne vede, Kotnikova 8, 1000 Ljubljana, Slovenija
E-pošta: simon.vrhovec@fvv.uni-mb.si

Povzetek. Število uporabnikov mobilnih naprav hitro narašča in se širi na nove skupine uporabnikov, kot so upokojenci in otroci. Kljub široko dostopnim varnostnim mehanizmom so uporabniki mobilnih naprav v kibernetskem prostoru čedalje bolj ranljivi. To zbuja skrb, saj uporabniki po navadi shranjujejo občutljive podatke na svojih mobilnih napravah, ki so v kibernetski prostor povezane tako rekoč dan in noč, kar jih nenehno izpostavlja potencialnim kibernetskim napadalcem. Izdelovalci mobilnih naprav si prizadevajo uporabnikom ponuditi naprave, ki so preproste za uporabo in ki ne zahtevajo dolge učne krivulje. To delno dosežejo s tem, da izklopijo nekatere varnostne mehanizme, ki zahtevajo preveč napora za njihovo učinkovito uporabo. Poleg tega se uporabniki mobilnih naprav pogosto ne zavedajo varnostnih groženj, ki pretijo nanje v kibernetskem prostoru, kar bistveno znižuje njihovo motivacijo za učenje, kako učinkovito uporabljati obstoječe varnostne mehanizme. V tem članku predstavljamo pregled ključnih varnostnih groženj v kibernetskem prostoru in varnostnih mehanizmov, ki lahko uporabnikom pomagajo učinkovito soočanje z njimi.

Ključne besede: mobilne naprave, kibernetski prostor, informacijska varnost

Safe mobile-device use in the cyberspace

The number of the mobile-device users is rapidly growing and expanding to new populations, such as seniors and kids. Despite a wide availability of the security measures, the mobile-device users are more and more vulnerable in the cyberspace. This is worrying as the users usually keep sensitive information on their mobile devices that are connected to the cyberspace day and night continuously exposing them to potential cyber attackers. The tendency of the mobile-device manufacturers is to offer the users the mobile devices that are easy to use and do not require a lengthy learning curve. This is partially achieved by disabling some security measures necessitating too much effort for their effective use. Additionally, the users are often unaware of the security threats in the cyberspace which significantly lowers their motivation to learn how to efficiently use the existing security measures. In this paper we review the key security threats in the cyberspace and security measures that can help the mobile-device users to tackle them.

Keywords: mobile devices, cyberspace, information security

1 UVOD

Sodobne mobilne tehnologije omogočajo stalno povezanost uporabnikov v kibernetski prostor, ki ga najpogosteje povezujemo ali kar enačimo z internetom. Razvoj različnih mobilnih naprav, predvsem pametnih telefonov in tablic, je približal kibernetski prostor širokemu spektru uporabnikov, od osnovnošolske mladine do upokojencev. Mobilne naprave sicer omogočajo ustrezno varovanje uporabnikov, a izdelovalci mobilnih naprav kljub temu težijo k najpreprostejšim varnostnim nastavitvam, s čimer je uporaba mobilnih naprav mogoča tako rekoč brez razumevanja vidika varnosti. S tem so mobilne naprave takoj, brez usposabljanja ali izobraževanja, uporabne za tako rekoč ves spekter uporabnikov. Toda hkrati take nastavitve puščajo neizkoriščene oz. izklopljene obstoječe varnostne mehanizme. Uporaba le-teh je tako prepuščena uporabnikom in njihovemu znanju, ki ga večina uporabnikov nima dovolj, mobilne naprave pa tako večinoma ostajajo povsem nezaščitene in izpostavljene zlorabam. Uporabniki se poleg tega veliko nevarnosti kibernetskega sveta tudi ne zavedajo in zato temu niti ne namenjajo potrebne pozornosti. Zaradi nepoznavanja nevarnosti kibernetskega sveta se uporabniki tako ne obremenjujejo z naprednejšimi varnostnimi mehanizmi, ki marsikateremu uporabniku ostanejo povsem tuji tudi po večletni uporabi mobilne naprave [1].

Poznavanje nevarnosti kibernetskega prostora je pogoj za ustrezno zaščito pred njimi. Namen tega članka je ozaveščanje uporabnikov mobilnih naprav o varnem delu v kibernetskem prostoru. Članek daje uporabnikom mobilnih naprav pregled nad nevarnostmi, ki prežijo nanje v kibernetskem prostoru, in jim ponuja različne rešitve, s katerimi se lahko pred temi nevarnostmi zavarujejo. Čeprav obstaja zajetna množica tehničnih rešitev oz. varnostnih nastavitev mobilnih naprav, pa je glavno vodilo varnega dela v kibernetskem prostoru t. i. zdrava kmečka pamet.

Prejet 18. januar, 2016
Odobren 19. april, 2016

2 VARNOSTNE GROŽNJE V KIBERNETSKEM PROSTORU

V nadaljevanju so v podpoglavjih predstavljene varnostne grožnje, ki pretijo uporabnikom mobilnih naprav v kibernetskem prostoru.

2.1 Zlonamerne aplikacije

Med mobilnimi aplikacijami, vključno s tistimi, ki jih namestimo prek uradnih trgovin (Google Play, Apple Store, Windows Store), je mogoče najti tudi zlonamerne aplikacije. To so tiste aplikacije, ki želijo npr. pridobiti podatke, do katerih sicer niso upravičeni (npr. fotografije, stiki, zapiski), ali neupravičeno uporabljati storitve mobilne naprave (npr. sledenje prek GPS). Nekatere trgovine zagotavljajo določeno stopnjo preverjanja mobilnih aplikacij, zato je med njimi delež zlonamernih aplikacij manjši. Bistveno višjo stopnjo tveganja pa pomenijo aplikacije, ki jih namestimo iz nepreverjenih virov, saj jih pred namestitvijo ne preverja nihče.

2.2 Škodljiva programska oprema

Škodljive programske opreme (angl. *malware*) za mobilne naprave je bistveno manj kot za osebne računalnike, a je ta kljub temu velik problem. Poznamo več vrst škodljive programske opreme, ki mobilno napravo ogrožajo na več načinov. Parazitski oglaševalski programi (angl. *adware*) prikazujejo različna oglasna sporočila in zbirajo podatke o uporabniku ter njegovi spletni aktivnosti. Parazitski vohunski programi (angl. *spyware*) omogočajo nadzorovanje uporabnika mobilne naprave brez njegove vednosti [2]. Izsiljevalska programska oprema (angl. *ransomware*) šifrira podatke na mobilni napravi in zahteva plačilo za njeno dešifriranje [2]. Strašilna programska oprema (angl. *scareware*) obvešča uporabnika mobilne naprave o lažni težavi in ponudi tudi (lažno) rešitev zanjo, npr. nakazilo denarja na določen bančni račun [2]. Škodljiva programska oprema lahko na napravo namesti stranska vrata (angl. *backdoor*), prek katerih lahko napadalec neopazno upravlja obilno napravo. Škodljiva programska oprema lahko mobilno napravo spremeni tudi v robotsko napravo (angl. *bot*) in jo vključi v omrežje robotskih naprav (angl. *botnet*) [3]. Robotske naprave je mogoče upravljati na daljavo, omrežja robotskih naprav pa se po navadi uporabljajo za napade na spletne strežnike, pošiljanje nezaželene pošte, širjenje škodljive programske opreme ipd. Bolj »klasična« škodljiva programska oprema lahko izbriše podatke iz mobilne naprave ali onemogoči dostop do njih, npr. s formatiranjem spominske kartice, s sesuvanjem operacijskega sistema ali brisanjem nameščenih aplikacij. Pogosto škodljiva programska oprema poveča porabo virov mobilne naprave (npr. večja obremenitev procesorja ali zasedenost delovnega pomnilnika RAM) in posledično upočasni delovanje mobilne naprave ter skrajša trajanje baterije. Nazadnje lahko škodljiva programska oprema brez vednosti uporabnika uporablja storitve mobilnega operaterja, npr. pošilja kratka sporočila SMS in opravlja klice na plačljive številke.

Svojo mobilno napravo lahko uporabnik zelo hitro okuži nevede. Mobilna naprava se lahko okuži že z obiskom napačne spletne strani, ki prikrito namesti škodljivo programsko opremo v ozadju (angl. *drive by download*). Uporabniki lahko svojo mobilno napravo okužijo tudi z namestitvijo predelanih legitimnih aplikacij (npr. brezplačne verzije sicer plačljive aplikacije). Podobno kot pri osebnih računalnikih se lahko mobilne naprave okužijo tudi na bolj »klasične« načine, kot so npr. priponke v elektronskih sporočilih ali kar s fizično namestitvijo napadalca.

2.3 Socialni inženiring

Socialni inženiring je napad, pri katerem napadalec s prevaro prelisiči uporabnika mobilne naprave in ga tako pripravi k temu, da npr. sam izda zasebne podatke ali namesti škodljivo programsko opremo na svojo mobilno napravo. Področje socialnega inženiringa je izjemno obsežno, omenjamo pa tiste tipe, ki so za mobilne naprave najbolj aktualni. Spletno ribarjenje (angl. *phishing*) je napad, ki se izvede prek svetovnega spleta in izkorišča predvsem nepozornost uporabnikov mobilnih naprav. Pri elektronskih sporočilih gre za povezave na spletne naslove, ki so podobni uradnim (npr. http://accaunts.g00gle.com/), pri brezžičnih omrežjih gre za lažne dostopne točke s kredibilnim imenom (npr. Ljubljana WiFi FREE) ipd. Z nastavljanjem vabe (angl. *baiting*) napadalci izkoriščajo človeško radovednost. Uporabnik mobilne naprave lahko svojo napravo okuži zgolj z vstavljanjem najdene spominske kartice vanjo. Ribarjenje prek kratkih sporočil SMS (angl. *smishing* / *SMS phishing*) in telefonskih klicev (angl. *vishing* / *VOIP phishing*) je sorodno spletnemu ribarjenju, saj prav tako izkorišča človekovo nepozornost in zbuja občutek, da je nujno razrešiti nastalo situacijo. Podobno lahko pod socialni inženiring štejemo tudi strašilno programsko opremo (angl. *scareware*), ki pri uporabniku mobilne naprave zbuja občutek strahu in panike. Med najpreprostejše tehnike štejemo tudi t. i. vohunjenje čez ramo (angl. *shoulder surfing*), pri katerem napadalec neposredno ali prek kamere opazuje zaslon uporabnika mobilne naprave, s čimer pridobi geslo, PIN-kodo ali druge podatke o uporabniku oz. njegovi mobilni napravi.

2.4 Fizično upravljanje mobilne naprave

Fizično upravljanje mobilne naprave se nanaša na uporabo mobilne naprave med njenim držanjem v roki. Mobilno napravo najpogosteje uporablja njen lastnik, lahko pa jo v uporabo posodi tudi osebam, ki jim zaupa. Problemi nastanejo tedaj, ko dobijo mobilno napravo v roke nepooblaščene osebe. Situacije se lahko med seboj zelo razlikujejo. Med klepetanjem v restavraciji si lahko mobilno napravo na mizi neopazno izposodijo prijatelji

in na neko družbeno omrežje objavijo kakšno smešno izjavo. Taki primeri so pravzaprav zelo pogosti in največkrat nimajo hujših posledic, saj niso zlonamerni. Toda v drugih primerih, kot so npr. zdravstvene ustanove, so lahko posledice veliko hujše. Z vsako mobilno napravo je namreč mogoče dostopati do občutljivih zdravstvenih podatkov o pacientih. Če se pri tem spremeni količina predpisanega zdravila za nekega pacienta, to lahko močno poslabša njegovo zdravljenje.

2.5 Družbena omrežja

Družbena omrežja (angl. *social networks*) so spletne strani, pogosto globalne, namenjene medsebojnemu druženju posameznikov. Uporabnikom omogočajo, da si ustvarijo lasten profil, prek katerega komunicirajo s prijatelji, objavljajo svoje misli, slike in videoposnetke idr. Pri družbenih omrežjih je težava v tem, da se na njih namerno ali nenamerno objavlja velika količina zasebnih podatkov (npr. kontaktnih podatkov, informacij o trenutni lokaciji uporabnikov, slik in videoposnetkov, iz katerih je mogoče razbrati zasebne informacije idr.), ki jih je mogoče zlorabiti, in sicer za ustvarjanje lažnih profilov, načrtovanje vlomov v stanovanja, prevare s socialnim inženiringom, izsiljevanje itd.

2.6 Predhodno nameščena programska oprema

Ob nakupu nove mobilne naprave je pogosto poleg operacijskega sistema nameščena tudi programska oprema izdelovalca mobilne naprave. Poleg izdelovalca lahko svoje aplikacije namesti tudi ponudnik telekomunikacijskih storitev oz. mobilni operater. Vse te aplikacije imenujemo predhodno nameščena programska oprema (angl. *bloatware*). Predhodno nameščena programska oprema naj bi uporabniku poenostavila uporabo mobilne naprave s posebnimi aplikacijami za upravljanje mobilne naprave (za pošiljanje sporočil, opravljanje klicev, upravljanje galerije, predvajanje glasbe idr.) ter omogočila lažjo interakcijo oz. sinhronizacijo s svetovnim spletom. Toda predhodno nameščena programska oprema dodatno obremenjuje mobilno napravo (večja obremenitev procesorja, zasedenost delovnega pomnilnika RAM in posledično krajše trajanje baterije). Hkrati ta programska oprema zbira podatke o uporabniku mobilne naprave in jih posreduje izdelovalcem mobilne naprave in mobilnim operaterjem. Zato se uporabniki mobilnih naprav pogosto odločajo za odstranitev te programske opreme, kar pa ima lahko tudi negativne posledice, npr. slabša stabilnost operacijskega sistema ali nastanek varnostnih lukenj. Odstranitev te programske opreme ima lahko tudi druge posledice, npr. razveljavitev garancije.

2.7 Vsiljena elektronska pošta

Vsiljena elektronska pošta (angl. *spam* / *junk e-mail*) je vsako sporočilo, ki je poslano z namenom vsiljevanja določenih vsebin, in je globalno vseprisoten problem, saj jo prejemamo vsi. Vsiljena elektronska pošta je problematična z več vidikov. V sporočilih se pogosto zavajajo prejemniki ali ponujajo malovredne stvari. Poleg tega lahko pošiljatelji oglašujejo tudi ilegalne proizvode in proizvode, ki so nevarni za zdravje (npr. steroidi in farmacevtski izdelki sumljivega izvora). Ne nazadnje pa je vsiljena elektronska pošta tudi nadloga za prejemnike, ki jih vsebina sporočil ne zanima [4], [5].

2.8 Izguba in kraja mobilne naprave

Včasih se zgodi, da uporabniku mobilno napravo ukradejo ali pa jo kje pozabi ali izgubi. Pri tem uporabnik mobilne naprave poleg same naprave izgubi tudi dostop do vseh podatkov na njej. Najditelj ali tat mobilne naprave lahko, če ta ni ustrezno zaščitena, dostopa do podatkov na njej, z njo dostopa do elektronskih računov (Google, Facebook, Instagram, Snapchat idr.) in jo uporabi za plačevanje storitev in izdelkov (npr. Moneta).

2.9 Poškodovanje in uničenje mobilne naprave

Mobilno napravo njeni uporabniki najpogosteje poškodujejo, ko to najmanj pričakujejo. Padec v vodo ali na tla sta samo dva od pogostejših primerov. Ob tem lahko uporabniki poleg izgube vrednosti mobilne naprave izgubijo tudi dostop do podatkov na njej ali pa se podatki oz. nosilci podatkov uničijo.

2.10 Povezave kratkega dosega

Bluetooth in NFC (angl. *near field communication*) sta tehnologiji brezžičnega povezovanja naprav, ki omogočata prenos podatkov med dvema ali več napravami na kratkih razdaljah. Zloraba povezav Bluetooth in NFC je mogoča samo, če je povezava vklopljena. Uporabniki mobilnih naprav povezavo kratkega dosega pogosto pozabijo izklopiti, jo imajo nenehno vklopljeno zaradi uporabe brezžičnih naprav (npr. Bluetooth slušalke) ali pa sploh ne vedo, kako povezavo izklopiti oz. preveriti, ali je po uporabi še vedno vklopljena. Prek povezav kratkega dosega lahko napadalec dostopa tako rekoč do vseh podatkov, ki so shranjeni na mobilni napravi (kontakti, sporočila, uporabniški računi, slike itd.). Ker mora biti napadalec v času napada v bližini mobilne naprave, so mobilne naprave ogrožene na lokacijah, kjer se na manjšem prostoru zbira več ljudi, npr. v učilnici, na avtobusu ali v restavraciji.

2.11 Wi-Fi omrežje

Uporabniki se velikokrat povezujejo do svetovnega spleta prek različnih omrežij Wi-Fi, saj je le-ta pogosto brezplačen in omogoča hitrejše brskanje po spletu, kot prek mobilnega omrežja. Povezovanje na omrežja Wi-Fi omogoča relativno preprosto prestrezanje in zbiranje podatkov, npr. o tem, do katerih spletnih strani uporabnik mobilne naprave dostopa. Na nezavarovanih omrežjih Wi-Fi lahko celotnemu spletnemu prometu na dostopni točki prisluškuje kdorkoli, ki je v njenem

dosegu in ki ima ustrezno prisluškovalno programsko opremo. Podobno je pravzaprav tudi na omrežjih Wi-Fi, ki so zavarovana z gesli, saj zgolj omrežja, ki uporabljajo zaščito WPA2-Enterprise, veljajo za varna. Ta omrežja zahtevajo, da ima vsak uporabnik svoje lastno geslo, s čimer se prepreči prestrezanje. Omeniti velja, da to ne pomeni, da prek omrežij Wi-Fi ni mogoče varno brskati po svetovnem spletu, a je za to treba poskrbeti na druge načine, npr. z uporabo šifriranega dostopa do spleta prek protokola HTTPS.

2.12 Kompromitiran operacijski sistem

Operacijski sistem je kompromitiran, če mu uporabnik omogoči večje pravice za dostop, kot to omogočajo privzete nastavitve (eskalacija privilegijev). Med različnimi operacijskimi sistemi so razlike v stopnji posega v operacijski sistem, ki jo zahteva kompromitiranje. Na operacijskem sistemu Android dostop do korenskega imenika (angl. *rooting*) uporabniku omogoča poln nadzor nad operacijskim sistemom in posledično tudi nad aplikacijami, preostalo programsko opremo in strojno opremo. Na operacijskem sistemu iOS se z razbitjem »ječe« oz. operacijskega sistema (angl. *jailbreaking*) odstrani vzpostavljena varnostna zaščita strojne opreme. S tem uporabnik pridobi dostop do korenskega imenika in sistemskih datotek, kar omogoča namestitev aplikacij, razširitev in tem, ki niso na voljo v uradni trgovini. Z razbitjem uporabnik krši uporabniško licenco in razveljavi garancijo. Na operacijskem sistemu Windows se mobilna naprava odklene (angl. *unlock*) s poseganjem v register operacijskega sistema. Uporabnik lahko po odklepanju namesti ali zažene aplikacije, ki niso na voljo prek uradne trgovine. Ločimo tri ravni odklepa, in sicer odklepanje za razvijalce (angl. *developer unlock*), odklepanje za izdelovalce strojne opreme (angl. *interop unlock* / *OEM developer unlock*) in polno odklepanje naprave (angl. *full unlock*). Pridobivanje dostopa do korenskega imenika, razbitje ječe in odklepanje mobilne naprave omogočajo obhod varnostnih mehanizmov, zaradi česar lahko mobilne aplikacije delujejo zunaj predvidenih okvirov. Zato taki posegi v operacijski sistem zmanjšujejo varnost mobilne naprave [6].

3 SKLEP

V članku je predstavljen pregled nad nevarnostmi, ki v kibernetskem prostoru prežijo na uporabnike mobilnih naprav. Čeprav sta že poznavanje nevarnosti in uporaba zdrave pameti v marsikaterem primeru dovolj za zaščito pred njimi, pa so uporabnikom poleg tega na voljo tudi rešitve, s katerimi se lahko pred temi nevarnostmi učinkovito zavarujejo.

LITERATURA

[1] Markelj, B., & Bernik, I. "Safe use of mobile devices arises from knowing the threats", *Journal of Information Security and Applications*, 20, str. 84–89, 2015.

[2] McGuire, C. F. "TIM Lecture Series The Expanding Cybersecurity Threat", *Technology Innovation Management Review*, 5(3), str. 46–48, 2015.

[3] Hamon, V. "Android botnets for multi-targeted attacks", *Journal in Computer Virology and Hacking Techniques*, 11(4), str. 193–202, 2015.

[4] Lee, T., Cho, H., Park, H., & Kwak, J. "Detection of Malware Propagation in Sensor Node and Botnet Group Clustering based on Email Spam Analysis", *International Journal of Distributed Sensor Networks*, članek št. 530250, 2015.

[5] Kojić, A., Hovelja, T., & Vavpotič, D. "Ogrodje za izboljšanje procesov razvoja informacijskih sistemov z uporabo hevristik za izboljšave splošnih poslovnih procesov", *Elektrotehniški vestnik*, 83(1–2), str. 47–53, 2016.

[6] Shao, Y., Luo, X., & Qian, C. "RootGuard: Protecting rooted android phones", *Computer*, 47(6), str. 32–40, 2014.

Simon Vrhovec je zaposlen na Fakulteti za varnostne vede Univerze v Mariboru. Doktoriral je leta 2015 na Fakulteti za računalništvo in informatiko Univerze v Ljubljani. Njegova glavna raziskovalna področja so vodenje projektov, odpor deležnikov do sprememb, agilne metode, globalni razvoj programske opreme, informacijska varnost in digitalna forenzika.