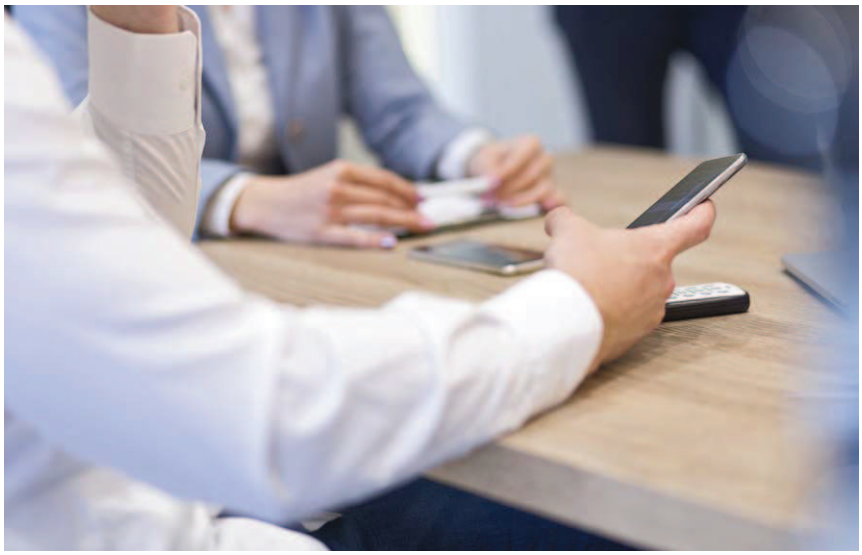
Trendy v bezpečnosti mobilních zařízení

Michael Kupka



Ústřední dějiště pro mnoho činností každodenního života – komunikaci, online transakce, zpracovávání informací o zdravotním stavu, používání biometrie, ovládání IoT zařízení (včetně domácnosti a automobilů), atd. Tak bychom mohli v současné době charakterizovat mobilní zařízení, a to především chytré telefony. Tento výčet každým dnem roste a jak tato zařízení přebírají větší odpovědnost a kontrolu v životě jejich uživatelů, stávají se pro útočníky čím dál lákavějšími.

Kyberbezpečnost je neustálá hra na kočku a na myš – s každým zlepšením v oblasti bezpečnosti přichází ruku v ruce i vývoj nových metod a technik útoků ze strany hackerů. U nich jsou mobilní zařízení v hledáčku již nějakou dobu, ale v poslední době nabývají stále více na významnosti. V praxi se tudíž setkáváme s nárůstem útoků na mobilní platformy. Současně díky tomu, že hacking je dnes prováděn v globálním měřítku a zeměpisné hranice na internetu v podstatě neexistují, můžeme dnešní situaci ohledně kompromitace mobilních zařízení považovat za neúnosnou.

V minulosti bylo nejčastější provedení útoků poměrně jednoduché – vystavování falešných aplikací na webech třetích stran, kde si uživatel v podstatě sám nainstaloval různý malware. Tato situace se ale postupně mění. Hackeři využívají širokou škálu dalších technik, jako jsou útoky na rádiové přenosy (LTE, Wi-Fi, Bluetooth), MDM, využívání zranitelností přímo v operačních systémech (iOS, Android), útoky na backend servery, na kterých jsou aplikace hostovány, a další. Na mobilní aplikace a zařízení tak není útočeno přímo, což většinou znamená, že oběť si takového útoku v dané chvíli ani nevšimne. Následující ilustrace zachycuje nejčastější vektory útoků, tedy jakými způsoby může hacker na zařízení útočit a dopady těchto útoků.

Obr. 1: Vektory (nalevo) a dopady (napravo) útoků na mobilní zařízení

V současnosti můžeme pozorovat několik trendů:

Mobilní Spear phishing

Klasický phishing byl dříve pro hackery spíše záležitostí rozesílání velkého množství e-mailů a čekání na to, jaká oběť se na danou kampaň chytí. Dnes je phishing stále více personalizovaný. Díky veřejným profilům na sociálních sítích a mobilním aplikacím, kterým uživatelé povolují různá dodatečná oprávnění, mohou útočníci v dlouhodobém časovém měřítku sbírat velké množství unikátních informací o svých obětech. To jim umožňuje provést vysoce personalizované a věrohodné útoky, které lze doručit na mobilní zařízení přímo pomocí zpráv nebo aplikacemi pro sociální sítě. Běžné phishingové ochrany založené na spam filtrech a zabezpečení e-mailových schránek jsou proti moderním metodám neúčinné. I přesto, že Google a Apple budou nadále posilovat bezpečnost svých platforem, nejslabším článkem zde bude vždy lidský faktor.

Hrozby týkající se SMS zpráv

Jedním z nejzákeřnějších útoků je tzv. SMS forwarding (přesměrování). Jedná se v podstatě o malware, který odcizí ověřovací kódy doručené prostřednictvím textových zpráv od poskytovatelů platebních služeb. Kódy jsou

útočníky zachyceny a používány k proniknutí do zákaznických účtů nebo k provedení autorizovaných úkonů.

Další hrozba, jejíž obětí se člověk snadno stane, je finanční ztráta spojená s odesíláním SMS zpráv. Škodlivá aplikace v telefonu odesílá textové zprávy na čísla s prémiovou sazbou, aniž by o tom majitel telefonu věděl, dokud na své faktuře od mobilního operátora nezjistí, že platí vysoké poplatky za textové zprávy. Když si uvědomíme, že infikovaných telefonů mohou být například desetitisíce a z každého je odesláno několik SMS zpráv každý týden, je lehké vypočítat, jak velmi rychle se útočníkům vyvíjení takového druhu malware zaplatí a kolik na něm profitují.

Stejně tak je stále závažná a aktuální otázka spamu, a to i prostřednictvím SMS zpráv. Hacker si běžně může pronajmout službu nebo přímo modem, pomocí kterých odešle desítky textových zpráv během jedné minuty. V těchto zprávách pak propaguje různé produkty nebo směřuje uživatele na webové stránky s nebezpečným obsahem.

Útoky na mobilní bankovnictví

Velmi populární je samozřejmě druh malware, který cílí na mobilní bankovnictví. Důvod je jasný, při úspěšné kompromitaci účtu oběti jde o rychlý a velký zisk. Často se lze tedy setkat s malware, které odcizují čísla platebních karet, osobní údaje nebo přímo přihlašovací údaje k bankovním aplikacím.

Příkladem za všechny může být nedávné odhalení aplikace QRecorder, která byla ke stažení oficiálně v obchodu Google Play a cílila na uživatele nejen z České republiky, ale také Polska a Německa. Tato aplikace odcizovala právě přihlašovací údaje do mobilních bankovnictví a několik zákazníků předních českých bank kvůli ní přišlo o peníze. Byla určena pro telefony s operačním systémem Android a sloužila k nahrávání telefonních hovorů. Nyní již aplikace není na Google Play dostupná, stáhnout ji však lze z různých neoficiálních zdrojů.

Aplikace pro úspěšné provedení útoku využívala odsouhlasení několika oprávnění, což je nejčastější chyba, kterou uživatelé při používaní mobilních aplikací dělají. V případě aplikace QRecorder se jednalo o povolení, aby aplikace mohla cokoliv zobrazovat v popředí. To bylo ve své podstatě legitimní oprávnění, protože pokud uživatel telefonoval, zobrazilo se mu „nad“ aplikací telefonu ještě nahrávací tlačítko – aby ho uživatel mohl zmáčknout. Tohoto oprávnění ale lze i v jakékoliv jiné nebezpečné aplikaci využít také tak, že nad mobilním bankovnictvím útočník zobrazí dodatečnou vrstvu. Pokud uživatel zadá přihlašovací údaje, vloží se právě do útočníkem vytvořené vrstvy a ne do pravé bankovní aplikace. S tímto útokem je možné se setkat pod názvem Tapjacking.

QRecorder zároveň do systému nainstaloval vlastní službu pro usnadnění a vyžadoval její povolení. Služba byla příznačně nazvána „Update Service“. V telefonu je možné používat různé služby po usnadnění, které slouží hlavně hendikepovaným lidem a umožňují jim snáze ovládat zařízení. Tyto služby mají mimo jiné přístup k notifikacím, aby například mohly uživatelům přehrát, co jim přišlo za SMS zprávu nebo zprávu na sociálních sítích. Pokud jde tedy o potvrzovací kód k provedené platbě zaslaný prostřednictvím SMS, takto je ho malware schopný zjistit i bez nutnosti odsouhlasení oprávnění ke čtení SMS zpráv.

Infikování přes bezdrátové sítě – budoucnost nebo již realita?

Pokud zůstaneme u stejného tématu, ale zamyslíme se nad dalšími způsoby infekce malwary, můžeme se ohlédnout na práci výzkumníků z Liverpoolské univerzity, která pro někoho může vypadat jako sci-fi. Ti totiž vyvinuli malware, který je schopen se šířit tak, jako se vir přenáší mezi lidmi. Nazvali ho příznačně „Chameleon“. Způsob jeho šíření je pomocí zranitelných a špatně nakonfigurovaných přístupových bodů Wi-Fi. V osídlených oblastech jsou přístupové body Wi-Fi v mnohem vyšší hustotě, což znamená, že například podobně jako chřipka se malware bude šířit mnohem rychleji ve městě.

Když Chameleon napadl přístupový bod, shromáždil různé přístupové údaje všech uživatelů připojených na stejnou Wi-Fi síť. Poté pokračoval v hledání okolních přístupových bodů, které by infikoval. Zajímavé je, že Chameleon unikl detekci různých antivirových řešení, protože ta vyhledávají malware běžně v komunikaci přicházející z internetu nebo na souborovém systému zařízení, ale ne uvnitř přístupového bodu.

Vzhledem k tomu, že Chameleon byl testován pouze v laboratorních podmínkách, můžeme si jen oddychnout, že není vypuštěn mezi veřejnost. Jak dlouho nicméně může trvat, než nějaký hacker vyvine vlastní verzi podobného malware? Zranitelné pak budou především právě mobilní zařízení, protože ta jsou k bezdrátovým sítím připojena nejčastěji a nemusí jít nutně jen o sítě Wi-Fi. Můžeme vzpomenout na rok starý útok BlueBorne využívající Bluetooth. Mimo pozornost by neměly jít ani sítě propojující IoT zařízení ZigBee, Sigfox a další.

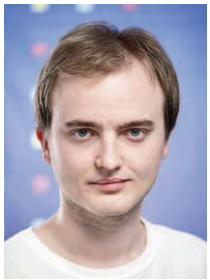
Závěrem

Většina mobilního malware je zaměřena na zařízení s operačním systémem Android. Je to především proto, že architektura je otevřená a jako taková zranitelnější než její konkurent Apple iOS (to však neznamená, že malware na platormě iOS neexistuje). To s sebou samozřejmě nese potřebu tato zařízení dostatečně zabezpečit. Existuje již několik kvalitních bezpečnostních produktů jak pro koncové uživatele, tak i pro firemní sféru – jedná se o anti-malware řešení, systémy pro pokročilou správu aplikací, firewally, MDM nebo systémy pro filtrování obsahu webu a ochranu prohlížeče. Všechny tyto produkty chrání před různými typy útoků a hrozeb a už jen díky tomu, že mobilní výpočetní technika je významnou součástí našich životů, má smysl tato řešení používat. Druhá strana mince je samozřejmě rychlost vývoje těchto produktů a jejich cena ve srovnání s kvalitou.

V případě mobilního bankovnictví z vlastní zkušenosti pozorujeme zlepšení zabezpečení v této oblasti. Banky do jejich vývoje poměrně intenzivně investují a při samotném penetračním testování pozorujeme v kvalitě zabezpečení zvyšující se trend. Za základní formu ochrany se zde považuje především dvoufaktorová autentizace, kde je zapotřebí v rámci bezpečnosti zvážit také uživatelskou přívětivost. Pokud je totiž pro příjem potvrzovacích SMS i pro mobilní bankovnictví používáno totožné zařízení, účinnost tohoto způsobu autentizace se snižuje v případě, že dojde ke kompromitaci daného zařízení.

Jako i v jiných oblastech, v případě zabezpečení mobilních zařízení sehrává hlavní roli lidský faktor. Je to uživatel, kdo by měl sledovat, jaká oprávnění po něm aplikace vyžadují odsouhlasit a jak se chovají. Jakékoliv podezřelé chování aplikací či webových stránek v mobilním prohlížeči, jakožto i celého sytému by mělo být ze strany uživatele důsledně prověřeno. ■

Michael Kupka



Autor článku je Security Specialist společnosti AEC, kde působí v Security Assessment Division.