Jsem Netvor
Tvor, který žije na netu

Pozor, appsťák!

Způsoby, jak někdo může proniknout do našeho zařízení

Webkamery po celém světě už viděly a slyšely docela dost divných věcí. Ať už přes ně ukazujeme cokoliv, chceme to mít pod kontrolou. Představa, že nás prostřednictvím webkamery někdo cizí sleduje, aniž bychom o tom věděli, je totiž dost děsivá. Problém je, že to není tak úplně sci-fi. O tom, jak se nestat nedobrovolným účastníkem reality show vysílané přímo z vašeho pokoje, si můžete přečíst níže.

Jak je možné hacknout naši webkameru nebo mikrofon?

Z technického hlediska je hacknutí webkamery skutečně možné. Možná jste nevěděli, že k tomu hacker nepotřebuje žádné super nástroje. Ať už se jedná o webkameru na notebooku nebo kamerku v mobilu, stačí do našeho zařízení propašovat škodlivý prográmek či aplikaci, které hackerovi umožní vzdálený přístup. A nemusí se jednat jen o webkameru. Z mikrofonu se může stát odposlouchávací zařízení, a sledováním klávesnice je zase možné získat hesla k našim účtům.

Proč má hacker zájem právě o můj mobil nebo počítač?

Možná si teď říkáte, že o váš telefon nebo počítač nemá přece nikdo zájem. Hackeři? Proč?! Máte pravdu, že hackerovi často nejde právě o vás. Většina útoků se podobá spíše rybaření, kdy útočník jednoduše rozhodí sítě

s nástrahami a čeká, kdo se chytí. Jak asi tušíte, zavirovat si nechtěně vlastní mobil není tak složité. Ale co s tím?

Odkud stahovat aplikace?

Mobily, které využíváme prakticky denně, jsou z hlediska bezpečnosti mnohdy zranitelnější než klasické počítače a notebooky. Asi nejzákeřnějším druhem útoku na mobily bývají škodlivé aplikace. Jako uživatelé bychom si tedy měli především stahovat jen aplikace z oficiální distribuce, tzn. obchodů, jako jsou třeba Google Play nebo AppStore. Aplikace, které zde jsou, prochází kontrolou, čímž se zvyšuje naše bezpečí.

Jenže útočníci jsou stále vynalézavější a i přes tuhle kontrolu může projít aplikace, která je škodlivá. Ačkoliv jsou tyhle kontroly relativně úspěšné, stále se do oběhu dostávají statisíce aplikací, které dělají problémy. Z oficiálních obchodů jsou odstraněny teprve ve chvíli, kdy se množí stížnosti uživatelů. Příkladem může být legendární aplikace s názvem „Nejjasnější svítilna zdarma.“ Slouží k tomu, že z displeje, případně blesku fotoaparátu, udělá účinnou svítilnu.

Problém je, že tahle aplikace vyžaduje vysoká oprávnění, která ji dávají nad mobilním telefonem moc, a ta může být obrácena proti nám. Útočník pak může ovládat mikrofon a kameru nebo třeba procházet kontakty a galerie. To vše leckdy dáváme sami k dispozici. Podobně známou aplikací je QRecorder, který umí vzdáleně sdílet displej chytrého mobilního telefonu, takže útočník získá přístup ke zprávám a všemu, co jste si prohlíželi.

Na co si dát pozor při stahování aplikací

Co s tím? Dívat se na hodnocení aplikací a požadavky na oprávnění, které aplikace chce. Chce kalkulačka přístup ke kontaktům? Proč?! U QRecorderu byl navíc zádrhel v tom, že původně se jednalo o aplikaci, která neměla škodlivé úmysly, takže si ji stáhlo hodně lidí. Teprve po aktualizaci se proměnila v trojského koně, který uměl pěkně potrápit. Mimochodem tenhle fígl s aktualizací, která jinak slouží právě k odstranění bezpečnostních problémů, je v neoficiálních obchodech docela běžný.

Ať už budete stahovat jakoukoliv aplikaci, zamyslete se taky nad tím, zda ji skutečně potřebujete. Platí totiž, že čím větší množství aplikací, tím větší pravděpodobnost, že se chytíte do pasti, kterých jsou nastraženy desetitisíce. Podobné trable v sobě ukrývají třeba aplikace pro úpravu fotek, přidání fotofiltrů nebo hry.

K čemu slouží aktualizace?

Dalším typem útoků na mobily je využití zranitelnosti starých a neaktualizovaných verzí mobilních operačních systémů nebo aplikací. Lze tomu přitom docela snadno předcházet a to tím, že mobilnímu telefonu jednoduše dovolíme se čas od času aktualizovat prostřednictvím výzvy k aktualizaci, kterou nám zpravidla dokonce sám nabídne.

Další způsoby, jak se dostane škodlivý program do našeho zařízení

Škodlivý program může být ovšem také součástí odkazu v e-mailu nebo zprávy v messengeru, kde se tváří jako obyčejná příloha ve formě fotky, videa nebo třeba písničky ve formátu mp3. V této podobě si jej koneckonců můžeme stáhnout do zařízení také přímo z internetu. Cest, jak se dostat k našim datům ovšem může být mnohem víc, a na první pohled se nemusí tvářit jako něco nelegálního.

Odposlouchávání mobilu a jiných chytrých zařízení výrobci

Jednou z často diskutovaných otázek je odposlouchávání mobilu a jiných chytrých zařízení přímo samotnými výrobci a vývojáři aplikací. Ve snaze vytvářet stále uživatelsky přívětivější a pohodlnější ovládání digitálních technologií je logickou volbou využívání zvuku a přirozené řeči. Proč bychom měli psát, když můžeme něco říct? Společnost Google se už před pár lety chlubila na své prezentaci hlasovým asistentem, který umí reagovat na nečekané situace a používat v běžné řeči prvky jako je mlasknutí a dokonce i využívat citoslovce. Můžete se tak objednat ke kadeřníkovi, aniž byste si s ním telefonovali. Google Assistent mu zatelefonuje místo vás.

Právě Google Assistent později čelil velkým tlakům kvůli tomu, že ukládá zvukové záznamy a operátoři některé nahrávky analyzují a dále s nimi pracují. I když Google vše zdůvodňoval zlepšováním služeb, tlak byl tak velký, že nastavení aplikace raději změnili a uživatel musí tohle nahrávání a ukládání ručně povolovat. Cílem tohoto sdělení není, abyste žili v obavách, že nás Google, Apple, Amazon, Facebook, Netflix nebo nějaké jiné společnosti tohoto typu odposlouchávají.

Cílem je, abychom si uvědomili, že je to technicky proveditelné, a do budoucna to může znamenat docela velký malér. Afér, kdy nějaká aplikace shromažďovala a odesílala naše data, i když to měla zakázané v nastavení, bylo už poměrně dost. Takže jako uživatelé si nemůžeme být stoprocentně ničím jisti.

Rada na závěr

Každopádně každej netvor ví, že za vším stojí peníze, a data obyčejných uživatelů je umí vydělat. Vyplatí se nestahovat aplikace, které nepotřebujeme, a sledovat, jaká oprávnění jim udělujeme. Protože stačí málo a vysíláme stream, aniž bychom o tom věděli.